CYBERSURE

Hack Prevention Tips Handbook

Simple | Convenient | Easy

YOU CAN BE SURE

canSURE

cyber@cansure.com

www.cansure.com

Form B013.1 | Apr 2017

CYBERSURE
HACK PREVENTION TIPS

Material reproduced with permission from US-CERT (Computer Emergency Readiness Team) and the Software Engineering Institute (SEI) at Carnegie Mellon University

Table of Contents 

Attacks and Threats

Email and Communication

General Information

General Security

Mobile Devices

Privacy

Attacks and Threats

Handling Destructive Malware

Destructive malware will utilize popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from web sites, and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy.

Overview

Presents a direct threat to an organization's daily operations, directly impacting the availability of critical assets and data. Organizations should increase vigilance and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event. This publication is focused on the threat of enterprise-scale distributed propagation methods for malware and provides recommended guidance and considerations for an organization to address as part of their network architecture, security baseline, continuous monitoring, and Incident Response practices.

While specific indicators and modules related to destructive malware may evolve over time, it is critical that an organization assess their capability to actively prepare for and respond to such an event.

Potential Distribution Vectors

Destructive malware has the capability to target a large scope of systems, and can potentially execute across multiple systems throughout a network. As a result, it is important for an organization to assess their environment for atypical channels for potential malware delivery and/or propagation throughout their systems. Systems to assess include:

- Enterprise Applications – particularly those which have the capability to directly interface with and impact multiple hosts and endpoints. Common examples include
  - Patch Management Systems,
  - Asset Management Systems,
  - Remote Assistance software (typically utilized by the corporate Help Desk),
  - Anti-Virus,
  - Systems assigned to system and network administrative personnel,
  - Centralized Backup Servers, and
  - Centralized File Shares.

While not applicable to malware specifically, threat actors could compromise additional resources to impact the availability of critical data and applications. Common examples include:

- Centralized storage devices
  - Potential Risk – direct access to partitions and data warehouses;
- Network devices
  - Potential Risk – capability to inject false routes within the routing table, delete specific routes from the routing table, or remove/modify configuration attributes - which could isolate or degrade availability of critical network resources.

Best Practices and Planning Strategies

Common strategies can be followed to strengthen an organization's resilience against destructive malware. Targeted assessment and enforcement of best practices should be employed for enterprise components susceptible to destructive malware.

Communication Flow

- Ensure proper network segmentation.
- Ensure that network-based access-control lists (ACLs) are configured to permit server-to-host and host-to-host connectivity via the minimum scope of ports and protocols – and that directional flows for connectivity are represented appropriately.
  - Communication flow paths should be fully defined, documented, and authorized.
- Increase awareness of systems which can be utilized as a gateway to pivot (lateral movement) or directly connect to additional endpoints throughout the enterprise.
  - Ensure that these systems are contained within restrictive VLANs, with additional segmentation and network access-controls.
- Ensure that centralized network and storage devices' management interfaces are resident on restrictive VLANs.
  - Layered access-control, and
  - Device-level access-control enforcement – restricting access from only pre-defined VLANs and trusted IP ranges.

Access Control

- For Enterprise systems which can directly interface with multiple endpoints:
  - Require two factor authentication for interactive logons.
  - Ensure that authorized users are mapped to a specific subset of enterprise personnel.
- If possible, the "Everyone", "Domain Users" or the "Authenticated Users" groups should not be permitted the capability to directly access or authenticate to these systems.
  - Ensure that unique domain accounts are utilized and documented for each Enterprise application service.
- Context of permissions assigned to these accounts should be fully documented and configured based upon the concept of least privilege.
- Provides an enterprise with the capability to track and monitor specific actions correlating to an application's assigned service account.
  - If possible, do not grant a service account with local or interactive logon permissions.
- Service accounts should be explicitly denied permissions to access network shares and critical data locations.
  - Accounts which are utilized to authenticate to centralized enterprise application servers or devices should not contain elevated permissions on downstream systems and resources throughout the enterprise.
- Continuously review centralized file share access-control lists and assigned permissions.
  - Restrict Write/Modify/Full Control permissions when possible.

Monitoring

- Audit and review security logs for anomalous references to enterprise-level administrative (privileged) and service accounts.
  - Failed logon attempts,
  - File share access, and
  - Interactive logons via a remote session.
- Review network flow data for signs of anomalous activity.
  - Connections utilizing ports which do not correlate to the standard communication flow associated with an application,
  - Activity correlating to port scanning or enumeration, and
  - Repeated connections utilizing ports which can be utilized for command and control purposes.
- Ensure that network devices log and audit all configuration changes.
  - Continually review network device configurations and rule sets, to ensure that communication flows are restricted to the authorized subset of rules.

File Distribution

- When deploying patches or AV signatures throughout an enterprise, stage the distributions to include a specific grouping of systems (staggered over a pre-defined time period).
  - This action can minimize the overall impact in the event that an enterprise patch management or AV system is leveraged as a distribution vector for a malicious payload.
- Monitor and assess the integrity of patches and AV signatures which are distributed throughout the enterprise.
  - Ensure updates are received only from trusted sources,
  - Perform file and data integrity checks, and
  - Monitor and audit – as related to the data that is distributed from an enterprise application.

System and Application Hardening

- Ensure that the underlying Operating System (OS) and dependencies (ex: IIS, Apache, SQL) supporting an application are configured and hardened based upon industry-standard best practice recommendations. Implement application-level security controls based upon best practice guidance provided by the vendor. Common recommendations include:
  - Utilize role-based access control,
  - Prevent end-user capabilities to bypass application-level security controls,
- Example – disabling Antivirus on a local workstation
  - Disable un-necessary or un-utilized features or packages, and
  - Implement robust application logging and auditing
- Thoroughly test and implement vendor patches in a timely manner.

Recovery and Reconstitution Planning

A Business Impact Analysis (BIA) is a key component of contingency planning and preparation. The overall output of a BIA will provide an organization with two key components (as related to critical mission/business operations):

- Characterization and classification of system components, and
- Interdependencies.

Based upon the identification of an organization's mission critical assets (and their associated interdependencies), in the event that an organization is impacted by a potentially destructive condition, recovery and reconstitution efforts should be considered. To plan for this scenario, an organization should address the availability and accessibility for the following resources (and should include the scope of these items within Incident Response exercises and scenarios):

- Comprehensive inventory of all mission critical systems and applications:
  - Versioning information,
  - System / application dependencies,

    - System partitioning/ storage configuration and connectivity, and
    - Asset Owners / Points of Contact.
- Comprehensive inventory of all mission critical systems and applications:
    - Versioning information,
    - System / application dependencies,
    - System partitioning/ storage configuration and connectivity, and
    - Asset Owners / Points of Contact.
- Contact information for all essential personnel within the organization,
- Secure communications channel for recovery teams,
- Contact information for external organizational-dependent resources:
    - Communication Providers,
    - Vendors (hardware / software), and
    - Outreach partners / External Stakeholders
- Service Contract Numbers - for engaging vendor support,
- Organizational Procurement Points of Contact,
- ISO / image files for baseline restoration of critical systems and applications:
    - Operating System installation media,
    - Service Packs / Patches,
    - Firmware, and
    - Application software installation packages.
- Licensing/activation keys for Operating Systems (OS) and dependent applications,
- Enterprise Network Topology and Architecture diagrams,
- System and application documentation,
- Hard copies of operational checklists and playbooks,
- System and application configuration backup files,
- Data backup files (full/differential),
- System and application security baseline and hardening checklists/guidelines, and
- System and application integrity test and acceptance checklists.

Containment

In the event that an organization observes a large-scale outbreak that may be reflective of a destructive malware attack, in accordance with Incident Response best practices, the immediate focus should be to contain the outbreak, and reduce the scope of additional systems which could be further impacted. Strategies for containment include:

- Determining a vector common to all systems experiencing anomalous behavior (or having been rendered unavailable) – from which a malicious payload could have been delivered:
    - Centralized Enterprise Application,
    - Centralized File Share (for which the identified systems were mapped or had access),
    - Privileged User Account common to the identified systems,
    - Network Segment or Boundary, and
    - Common DNS Server for name resolution.
- Based upon the determination of a likely distribution vector, additional mitigation controls can be enforced to further minimize impact:
    - Implement network-based access-control lists to deny the identified application(s) the capability to directly communicate with additional systems,
- Provides an immediate capability to isolate and sandbox specific systems or resources
    - Implement null network routes for specific IP addresses (or IP ranges) – from which the payload may be distributed,
- An organization's internal DNS can also be leveraged for this task – as a null pointer record could be added within a DNS zone for an identified server or application
    - Readily disable access for suspected user or service account(s), and
    - For suspect file shares (which may be hosting the infection vector), remove access or disable the share path from being accessed by additional systems.

As related to incident response and incident handling, organizations are reminded to:
- Report the incident to US-CERT and/or ICS-CERT for tracking and correlation purposes, and
- Preserve forensic data for use in internal investigation of the incident or for possible law enforcement purposes.

Understanding Hidden Threats: Rootkits and Botnets

Attackers are continually finding new ways to access computer systems. The use of hidden methods such as rootkits and botnets has increased, and you may be a victim without even realizing it.

What are rootkits and botnets?

A rootkit is a piece of software that can be installed and hidden on your computer without your knowledge. It may be included in a larger software package or installed by an attacker who has been able to take advantage of a vulnerability on your computer or has convinced you to download it (see Avoiding Social Engineering and Phishing Attacks for more information). Rootkits are not necessarily malicious, but they may hide malicious activities. Attackers may be able to access information, monitor your actions, modify programs, or perform other functions on your computer without being detected.

Botnet is a term derived from the idea of bot networks. In its most basic form, a bot is simply an automated computer program, or robot. In the context of botnets, bots refer to computers that are able to be controlled by one, or many, outside sources. An attacker usually gains control by infecting the computers with a virus or other malicious code that gives the attacker access. Your computer may be part of a botnet even though it appears to be operating normally. Botnets are often used to conduct a range of activities, from distributing spam and viruses to conducting denial-of-service attacks (see Understanding Denial-of-Service Attacks for more information).

Why are they considered threats?

The main problem with both rootkits and botnets is that they are hidden. Although botnets are not hidden the same way rootkits are, they may be undetected unless you are specifically looking for certain activity. If a rootkit has been installed, you may not be aware that your computer has been compromised, and traditional anti-virus software may not be able to detect the malicious programs. Attackers are also creating more sophisticated programs that update themselves so that they are even harder to detect.

Attackers can use rootkits and botnets to access and modify personal information, attack other computers, and commit other crimes, all while remaining undetected. By using multiple computers, attackers increase the range and impact of their crimes. Because each computer in a botnet can be programmed to execute the same command, an attacker can have each of them scanning multiple computers for vulnerabilities, monitoring online activity, or collecting the information entered in online forms.

What can you do to protect yourself?

If you practice good security habits, you may reduce the risk that your computer will be compromised:

- **Use and maintain anti-virus software** - Anti-virus software recognizes and protects your computer against most known viruses, so you may be able to detect and remove the virus before it can do any damage (see Understanding Anti-Virus Software for more information). Because attackers are continually writing new viruses, it is important to keep your definitions up to date. Some anti-virus vendors also offer anti-rootkit software.
- **Install a firewall** - Firewalls may be able to prevent some types of infection by blocking malicious traffic before it can enter your computer and limiting the traffic you send (see Understanding Firewalls for more information). Some operating systems actually include a firewall, but you need to make sure it is enabled.
- **Use good passwords** - Select passwords that will be difficult for attackers to guess, and use different passwords for different programs and devices (see Choosing and Protecting Passwords for more information). Do not choose options that allow your computer to remember your passwords.
- **Keep software up to date** - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Follow good security practices** - Take appropriate precautions when using email and web browsers to reduce the risk that your actions will trigger an infection (see other US-CERT security tips for more information).

Unfortunately, if there is a rootkit on your computer or an attacker is using your computer in a botnet, you may not know it. Even if you do discover that you are a victim, it is difficult for the average user to effectively recover. The attacker may have modified files on your computer, so simply removing the malicious files may not solve the problem, and you may not be able to safely trust a prior version of a file. If you believe that you are a victim, consider contacting a trained system administrator.

As an alternative, some vendors are developing products and tools that may remove a rootkit from your computer. If the software cannot locate and remove the infection, you may need to reinstall your operating system, usually with a system restore disk that is often supplied with a new computer. Note that reinstalling or restoring the operating system typically erases all of your files and any additional software that you have installed on your computer. Also, the infection may be located at such a deep level that it cannot be removed by simply reinstalling or restoring the operating system.

Browsing Safely: Understanding Active Content and Cookies

What is active content?

To increase functionality or add design embellishments, web sites often rely on scripts that execute programs within the web browser. This active content can be used to create "splash pages" or options like drop-down menus. Unfortunately, these scripts are often a way for attackers to download or execute malicious code on a user's computer.

- JavaScript - JavaScript is just one of many web scripts (other examples are VBScript, ECMAScript, and JScript) and is probably the most recognized. Used on almost every web site now, JavaScript and other scripts are popular because users expect the functionality and "look" that it provides, and it's easy to incorporate (many common software programs for building web sites have the capability to add JavaScript features with little effort or knowledge required of the user).
- However, because of these reasons, attackers can manipulate it to their own purposes. A popular type of attack that relies on JavaScript involves redirecting users from a legitimate web site to a malicious one that may download viruses or collect personal information.
- Java and ActiveX controls - Different from JavaScript, Java and ActiveX controls are actual programs that reside on your computer or can be downloaded over the network into your browser. If executed by attackers, untrustworthy ActiveX controls may be able to do anything on your computer that you can do (such as running spyware and collecting personal information, connecting to other computers, and potentially doing other damage). Java applets usually run in a more restricted environment, but if that environment isn't secure, then malicious Java applets may create opportunities for attack as well.

JavaScript and other forms of active content are not always dangerous, but they are common tools for attackers. You can prevent active content from running in most browsers, but realize that the added security may limit functionality and break features of some sites you visit. Before clicking on a link to a web site that you are not familiar with or do not trust, take the precaution of disabling active content.

These same risks may also apply to the email program you use. Many email clients use the same programs as web browsers to display HTML, so vulnerabilities that affect active content like JavaScript and ActiveX often apply to email. Viewing messages as plain text may resolve this problem.

What are cookies?

When you browse the Internet, information about your computer may be collected and stored. This information might be general information about your computer (such as IP address, the domain you used to connect (e.g., .edu, .com, .net), and the type of browser you used). It might also be more specific information about your browsing habits (such as the last time you visited a particular web site or your personal preferences for viewing that site).

Cookies can be saved for varying lengths of time:

- Session cookies - Session cookies store information only as long as you're using the browser; once you close the browser, the information is erased. The primary purpose of session cookies is to help with navigation, such as by indicating whether or not you've already visited a particular page and retaining information about your preferences once you've visited a page.
- Persistent cookies - Persistent cookies are stored on your computer so that your personal preferences can be retained. In most browsers, you can adjust the length of time that persistent cookies are stored. It is because of these cookies that your email address appears by default when you open your Yahoo! or Hotmail email account, or your personalized home page appears when you visit your favorite online merchant. If an attacker gains access to your computer, he or she may be able to gather personal information about you through these files.

To increase your level of security, consider adjusting your privacy and security settings to block or limit cookies in your web browser. To make sure that other sites are not collecting personal information about you without your knowledge, choose to only allow cookies for the web site you are visiting; block or limit cookies from a third-party. If you are using a public computer, you should make sure that cookies are disabled to prevent other people from accessing or using your personal information.

Understanding Hidden Threats: Corrupted Software Files

Malicious code is not always hidden in web page scripts or unusual file formats. Attackers may corrupt types of files that you would recognize and typically consider safe, so you should take precautions when opening files from other people.

What types of files can attackers corrupt?

An attacker may be able to insert malicious code into any file, including common file types that you would normally consider safe. These files may include documents created with word processing software, spreadsheets, or image files. After corrupting the file, an attacker may distribute it through email or post it to a website. Depending on the type of malicious code, you may infect your computer by just opening the file.

When corrupting files, attackers often take advantage of vulnerabilities that they discover in the software that is used to create or open the file. These vulnerabilities may allow attackers to insert and execute malicious scripts or code, and they are not always detected. Sometimes the vulnerability involves a combination of certain files (such as a particular piece of software running on a particular operating system) or only affects certain versions of a software program.

What problems can malicious files cause?

There are various types of malicious code, including viruses, worms, and Trojan horses (see Why is Cyber Security a Problem? for more information). However, the range of consequences varies even within these categories. The malicious code may be designed to perform one or more functions, including

- interfering with your computer's ability to process information by consuming memory or bandwidth (causing your computer to become significantly slower or even "freeze")
- installing, altering, or deleting files on your computer
- giving the attacker access to your computer
- using your computer to attack other computers (see Understanding Denial-of-Service Attacks for more information)

How can you protect yourself?

- **Use and maintain anti-virus software** - Anti-virus software can often recognize and protect your computer against most known viruses, so you may be able to detect and remove the virus before it can do any damage (see Understanding Anti-Virus Software for more information). Because attackers are continually writing new viruses, it is important to keep your definitions up to date.
- **Use caution with email attachments** - Do not open email attachments that you were not expecting, especially if they are from people you do not know. If you decide to open an email attachment, scan it for viruses first (see Using Caution with Email Attachments for more information). Not only is it possible for attackers to "spoof" the source of an email message, but your legitimate contacts may unknowingly send you an infected file. If your email program automatically downloads and opens attachments, check your settings to see if you can disable this feature.
- **Be wary of downloadable files on websites** - Avoid downloading files from sites that you do not trust. If you are getting the files from a supposedly secure site, look for a website certificate (see Understanding Web Site Certificates for more information). If you do download a file from a website, consider saving it to your computer and manually scanning it for viruses before opening it.
- **Keep software up to date** - Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Take advantage of security settings** - Check the security settings of your email client and your web browser. Apply the highest level of security available that still gives you the functionality you need.

Recognizing Fake Antiviruses

Fake antivirus is malicious software (malware) designed to steal information from unsuspecting users by mimicking legitimate security software. It's important to protect your computer from fake antivirus infection and to be able to recognize when an infection has occurred.

What is fake antivirus?

Fake antivirus is malicious software (malware) designed to steal information from unsuspecting users by mimicking legitimate security software. The malware makes numerous system modifications making it extremely difficult to terminate unauthorized activities and remove the program. It also causes realistic, interactive security warnings to be displayed to the computer user.

How can my computer become infected with fake antivirus?

Criminals distribute this type of malware using search engines, emails, social networking sites, internet advertisements and other malware. They leverage advanced social engineering methodologies and popular technologies to maximize number of infected computers.

How will I know if I am infected?

The presence of pop-ups displaying unusual security warnings and asking for credit card or personal information is the most obvious method of identifying a fake antivirus infection.

What can I do to protect myself?

- Be cautious when visiting web links or opening attachments from unknown senders. See Using Caution with Email Attachments for more information.
- Keep software patched and updated.
- To purchase or renew software subscriptions, visit the vendor sites directly.
- Monitor your credit cards for unauthorized activity.
- To report Internet crime or fraud, contact the Internet Crime Complaint Center (https://www.ic3.gov).

Recognizing and Avoiding Spyware

Because of its popularity, the internet has become an ideal target for advertising. As a result, spyware, or adware, has become increasingly prevalent. When troubleshooting problems with your computer, you may discover that the source of the problem is spyware software that has been installed on your machine without your knowledge.

What is spyware?

Despite its name, the term "spyware" doesn't refer to something used by undercover operatives, but rather by the advertising industry. In fact, spyware is also known as "adware." It refers to a category of software that, when installed on your computer, may send you pop-up ads, redirect your browser to certain web sites, or monitor the web sites that you visit. Some extreme, invasive versions of spyware may track exactly what keys you type. Attackers may also use spyware for malicious purposes.
Because of the extra processing, spyware may cause your computer to become slow or sluggish. There are also privacy implications:

- What information is being gathered?
- Who is receiving it?
- How is it being used?

How do you know if there is spyware on your computer?

The following symptoms *may* indicate that spyware is installed on your computer:

- you are subjected to endless pop-up windows
- you are redirected to web sites other than the one you typed into your browser
- new, unexpected toolbars appear in your web browser
- new, unexpected icons appear in the task tray at the bottom of your screen
- your browser's home page suddenly changed
- the search engine your browser opens when you click "search" has been changed
- certain keys fail to work in your browser (e.g., the tab key doesn't work when you are moving to the next field within a form)
- random Windows error messages begin to appear
- your computer suddenly seems very slow when opening programs or processing tasks (saving files, etc.)

How can you prevent spyware from installing on your computer?

To avoid unintentionally installing it yourself, follow these good security practices:

- **Don't click on links within pop-up windows** - Because pop-up windows are often a product of spyware, clicking on the window may install spyware software on your computer. To close the pop-up window, click on the "X" icon in the titlebar instead of a "close" link within the window.
- **Choose "no" when asked unexpected questions** - Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. Always select "no" or "cancel," or close the dialog box by clicking the "X" icon in the titlebar.
- **Be wary of free downloadable software** - There are many sites that offer customized toolbars or other features that appeal to users. Don't download programs from sites you don't trust, and realize that you may be exposing your computer to spyware by downloading some of these programs.
- **Don't follow email links claiming to offer anti-spyware software** - Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating.

As an additional good security practice, especially if you are concerned that you might have spyware on your machine and want to minimize the impact, consider taking the following action:

- **Adjust your browser preferences to limit pop-up windows and cookies** - Pop-up windows are often generated by some kind of scripting or active content. Adjusting the settings within your browser to reduce or prevent scripting or active content may reduce the number of pop-up windows that appear. Some browsers offer a specific option to block or limit pop-up windows. Certain types of cookies are sometimes considered spyware because they reveal what web pages you have visited. You can adjust your privacy settings to only allow cookies for the web site you are visiting (see Browsing Safely: Understanding Active Content and Cookies).

How do you remove spyware?

- **Run a full scan on your computer with your anti-virus software** - Some anti-virus software will find and remove spyware, but it may not find the spyware when it is monitoring your computer in real time. Set your anti-virus software to prompt you to run a full scan periodically (see Understanding Anti-Virus Software for more information).
- **Run a legitimate product specifically designed to remove spyware** - Many vendors offer products that will scan your computer for spyware and remove any spyware software. Popular products include Lavasoft's Ad-Aware, Microsoft's Window Defender, Webroot's SpySweeper, and Spybot Search and Destroy.

Make sure that your anti-virus and anti-spyware software are compatible - Take a phased approach to installing the software to ensure that you don't unintentionally introduce problems (see Coordinating Virus and Spyware Defense for more information).

Understanding Denial-of-Service Attacks

You may have heard of denial-of-service attacks launched against websites, but you can also be a victim of these attacks. Denial-of-service attacks can be difficult to distinguish from common network activity, but there are some indications that an attack is in progress.

What is a denial-of-service (DoS) attack?

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular website into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.

An attacker can use spam email messages to launch a similar attack on your email account. Whether you have an email account supplied by your employer or one available through a free service such as Yahoo or Hotmail, you are assigned a specific quota, which limits the amount of data you can have in your account at any given time. By sending many, or large, email messages to the account, an attacker can consume your quota, preventing you from receiving legitimate messages.

What is a distributed denial-of-service (DDoS) attack?

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

How do you avoid being part of the problem?

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- Install and maintain anti-virus software (see Understanding Anti-Virus Software for more information).
- Install a firewall, and configure it to restrict traffic coming into and leaving your computer (see Understanding Firewalls for more information).
- Follow good security practices for distributing your email address (see Reducing Spam for more information). Applying email filters may help you manage unwanted traffic.

How do you know if an attack is happening?

Not all disruptions to service are the result of a denial-of-service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the following symptoms *could* indicate a DoS or DDoS attack:

- unusually slow network performance (opening files or accessing websites)
- unavailability of a particular website
- inability to access any website
- dramatic increase in the amount of spam you receive in your account

What do you do if you think you are experiencing an attack?

Even if you do correctly identify a DoS or DDoS attack, it is unlikely that you will be able to determine the actual target or source of the attack. Contact the appropriate technical professionals for assistance.

- If you notice that you cannot access your own files or reach any external websites from your work computer, contact your network administrators. This may indicate that your computer or your organization's network is being attacked.

If you are having a similar experience on your home computer, consider contacting your internet service provider (ISP). If there is a problem, the ISP might be able to advise you of an appropriate course of action.

Avoiding Social Engineering and Phishing Attacks

Do not give sensitive information to others unless you are sure that they are indeed who they claim to be and that they should have access to the information.

What is a social engineering attack?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security. (See Protecting Your Privacy for more information.)
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. (See Understanding Firewalls, Understanding Anti-Virus Software, and Reducing Spam for more information.)
- Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft. (See Preventing and Responding to Identity Theft for more information.)

Consider reporting the attack to the police, and file a report with the Federal Trade Commission.

Preventing and Responding to Identity Theft

Is identity theft just a problem for people who submit information online?

You can be a victim of identity theft even if you never use a computer. Malicious people may be able to obtain personal information (such as credit card numbers, phone numbers, account numbers, and addresses) by stealing your wallet, overhearing a phone conversation, rummaging through your trash (a practice known as dumpster diving), or picking up a receipt at a restaurant that has your account number on it. If a thief has enough information, he or she may be able to impersonate you to purchase items, open new accounts, or apply for loans.

The Internet has made it easier for thieves to obtain personal and financial data. Most companies and other institutions store information about their clients in databases; if a thief can access that database, he or she can obtain information about many people at once rather than focus on one person at a time. The Internet has also made it easier for thieves to sell or trade the information, making it more difficult for law enforcement to identify and apprehend the criminals.

How are victims of online identity theft chosen?

Identity theft is usually a crime of opportunity, so you may be victimized simply because your information is available. Thieves may target customers of certain companies for a variety of reasons; for example, a company database is easily accessible, the demographics of the customers are appealing, or there is a market for specific information. If your information is stored in a database that is compromised, you may become a victim of identity theft.

Are there ways to avoid being a victim?

Unfortunately, there is no way to guarantee that you will not be a victim of online identity theft. However, there are ways to minimize your risk:

- **Do business with reputable companies** – Before providing any personal or financial information, make sure that you are interacting with a reputable, established company. Some attackers may try to trick you by creating malicious web sites that appear to be legitimate, so you should verify the legitimacy before supplying any information. (See Avoiding Social Engineering and Phishing Attacks for more information.)
- **Take advantage of security features** – Passwords and other security features add layers of protection if used appropriately. (See Choosing and Protecting Passwords and Supplementing Passwords for more information.)
- **Check privacy policies** – Take precautions when providing information, and make sure to check published privacy policies to see how a company will use or distribute your information. (See Protecting Your Privacy and How Anonymous Are You? for more information.) Many companies allow customers to request that their information not be shared with other companies; you should be able to locate the details in your account literature or by contacting the company directly.
- **Be careful what information you publicize** – Attackers may be able to piece together information from a variety of sources. Avoid posting personal data in public forums. (See Guidelines for Publishing Information Online for more information.)
- **Use and maintain anti-virus software and a firewall** – Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall. (See Understanding Anti-Virus Software and Understanding Firewalls for more information.) Make sure to keep your virus definitions up to date.
- **Be aware of your account activity** – Pay attention to your statements, and check your credit report yearly. You are entitled to a free copy of your credit report from each of the main credit reporting companies once every twelve months. (See AnnualCreditReport.com (link is external) for more information.)

How do you know if your identity has been stolen?

Companies have different policies for notifying customers when they discover that someone has accessed a customer database. However, you should be aware of changes in your normal account activity. The following are examples of changes that could indicate that someone has accessed your information:

- unusual or unexplainable charges on your bills
- phone calls or bills for accounts, products, or services that you do not have
- failure to receive regular bills or mail
- new, strange accounts appearing on your credit report
- unexpected denial of your credit card

What can you do if you suspect or know that your identity has been stolen?

Recovering from identity theft can be a long, stressful, and potentially costly process. Many credit card companies have adopted policies that try to minimize the amount of money you are liable for, but the implications can extend beyond your existing accounts. To minimize the extent of the damage, take action as soon as possible:

- **Start by visiting IdentityTheft.gov –** This is a trusted, one-stop resource to help you report and recover from identity theft. Information provided here includes checklists, sample letters, and links to other resources.
- **Possible next steps in the process –** You may need to contact credit reporting agencies or companies where you have accounts, file police or other official reports, and consider other information that may have been compromised.

Other sites that offer information and guidance for recovering from identity theft are:

- Federal Trade Commission – https://www.consumer.ftc.gov
- United States Department of Justice – https://www.usdoj.gov/criminal/fraud/websites/idtheft.html
- Social Security Administration – https://www.ssa.gov/pubs/EN-05-10064.pdf

Recovering from Viruses, Worms, and Trojan Horses

Unfortunately, many users are victims of viruses, worms, or Trojan horses. If your computer gets infected with malicious code, there are steps you can take to recover.

How do you know your computer is infected?

Unfortunately, there is no particular way to identify that your computer has been infected with malicious code. Some infections may completely destroy files and shut down your computer, while others may only subtly affect your computer's normal operations. Be aware of any unusual or unexpected behaviors. If you are running anti-virus software, it may alert you that it has found malicious code on your computer. The anti-virus software may be able to clean the malicious code automatically, but if it can't, you will need to take additional steps.

What can you do if you are infected?

- **Minimize the damage** - If you are at work and have access to an IT department, contact them immediately. The sooner they can investigate and clean your computer, the less damage to your computer and other computers on the network. If you are on your home computer or a laptop, disconnect your computer from the internet. By removing the internet connection, you prevent an attacker or virus from being able to access your computer and perform tasks such as locating personal data, manipulating or deleting files, or using your computer to attack other computers.
- **Remove the malicious code** - If you have anti-virus software installed on your computer, update the virus definitions (if possible), and perform a manual scan of your entire system. If you do not have anti-virus software, you can purchase it at a local computer store (see Understanding Anti-Virus Software for more information). If the software can't locate and remove the infection, you may need to reinstall your operating system, usually with a system restore disk that is often supplied with a new computer. Note that reinstalling or restoring the operating system typically erases all of your files and any additional software that you have installed on your computer. After reinstalling the operating system and any other software, install all of the appropriate patches to fix known vulnerabilities.

How can you reduce the risk of another infection?

Dealing with the presence of malicious code on your computer can be a frustrating experience that can cost you time, money, and data. The following recommendations will build your defense against future infections:

- **use and maintain anti-virus software** - Anti-virus software recognizes and protects your computer against most known viruses. However, attackers are continually writing new viruses, so it is important to keep your anti-virus software current (see Understanding Anti-Virus Software for more information).
- **change your passwords** - Your original passwords may have been compromised during the infection, so you should change them. This includes passwords for web sites that may have been cached in your browser. Make the passwords difficult for attackers to guess (see Choosing and Protecting Passwords for more information).
- **keep software up to date** - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **install or enable a firewall** - Firewalls may be able to prevent some types of infection by blocking malicious traffic before it can enter your computer (see Understanding Firewalls for more information). Some operating systems actually include a firewall, but you need to make sure it is enabled.
- **use anti-spyware tools** - Spyware is a common source of viruses, but you can minimize the number of infections by using a legitimate program that identifies and removes spyware (see Recognizing and Avoiding Spyware for more information).
- **follow good security practices** - Take appropriate precautions when using email and web browsers so that you reduce the risk that your actions will trigger an infection (see other US-CERT security tips for more information).

As a precaution, maintain backups of your files on CDs or DVDs so that you have saved copies if you do get infected again.

Email and Communication

Staying Safe on Social Networking Sites

What are social networking sites?

Social networking sites, sometimes referred to as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

Although the features of social networking sites differ, they all allow you to provide information about yourself and offer some type of communication mechanism (forums, chat rooms, email, instant messenger) that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be "introduced" to new people through a connection you share. Many of the sites have communities or subgroups that may be based on a particular interest.

What security implications do these sites present?

Social networking sites rely on connections and communication, so they encourage you to provide a certain amount of personal information. When deciding how much information to reveal, people may not exercise the same amount of caution as they would when meeting someone in person because

- the Internet provides a sense of anonymity
- the lack of physical interaction provides a false sense of security
- they tailor the information for their friends to read, forgetting that others may see it
- they want to offer insights to impress potential friends or associates

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available. The more information malicious people have about you, the easier it is for them to take advantage of you. Predators may form relationships online and then convince unsuspecting individuals to meet them in person. That could lead to a dangerous situation. The personal information can also be used to conduct a social engineering attack. (See Avoiding Social Engineering and Phishing Attacks for more information.) Using information that you provide about your location, hobbies, interests, and friends, a malicious person could impersonate a trusted friend or convince you that they have the authority to access other personal or financial data.

Additionally, because of the popularity of these sites, attackers may use them to distribute malicious code. Sites that offer applications developed by third parties are particularly susceptible. Attackers may be able to create customized applications that appear to be innocent while infecting your computer or sharing your information without your knowledge.

How can you protect yourself?

- **Limit the amount of personal information you post** - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.
- **Remember that the Internet is a public resource** - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines. (See Guidelines for Publishing Information Online.)
- **Be wary of strangers** - The Internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.
- **Be skeptical** - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.
- **Evaluate your settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.
- **Be wary of third-party applications** - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.

- **Use strong passwords** - Protect your account with passwords that cannot easily be guessed. (See Choosing and Protecting Passwords.) If your password is compromised, someone else may be able to access your account and pretend to be you.
- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. (See Reducing Spam.) Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.
- **Keep software, particularly your web browser, up to date** - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Use and maintain anti-virus software** - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. (See Understanding Anti-Virus Software.) Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

Children are especially susceptible to the threats that social networking sites present. Although many of these sites have age restrictions, children may misrepresent their ages so that they can join. By teaching children about Internet safety, being aware of their online habits, and guiding them to appropriate sites, parents can make sure that the children become safe and responsible users.

Understanding Your Computer: Email Clients

The main difference between email clients is the user interface. Regardless of which software you decide to use, follow good security practices when reading or sending email.

How do email clients work?

Every email address has two basic parts: the user name and the domain name. When you are sending email to someone else, your domain's server has to communicate with your recipient's domain server.

For example, let's assume that your email address is *johndoe@example.com*, and the person you are contacting is at *janesmith@anotherexample.org*. In very basic terms, after you hit **send**, the server hosting your domain (example.com) looks at the email address and then contacts the server hosting the recipient's domain (anotherexample.org) to let it know that it has a message for someone at that domain. Once the connection has been established, the server hosting the recipient's domain (anotherexample.org) then looks at the user name of the email address and routes the message to that account.

How many email clients are there?

There are many different email clients and services, each with its own interface. Some are web-based applications, some are stand-alone applications installed directly on your computer, and some are text-based applications. There are also variations of many of these email clients that have been designed specifically for mobile devices such as cell phones.

How do you choose an email client?

There is usually an email client included with the installation of your operating system, but many other alternatives are available. Be wary of "home-brewed" software, because it may not be as secure or reliable as software that is tested and actively maintained. Some of the factors to consider when deciding which email client best suits your needs include:

- **security** - Do you feel that your email program offers you the level of security you want for sending, receiving, and reading email messages? How does it handle attachments (see Using Caution with Email Attachments for more information)? If you are dealing with sensitive information, do you have the option of sending and receiving signed and/or encrypted messages (see Understanding Digital Signatures and Understanding Encryption for more information)?
- **privacy** - If you are using a web-based service, have you read its privacy policy (see Protecting Your Privacy for more information)? Do you know what information is being collected and who has access to it? Are there options for filtering spam (see Reducing Spam for more information)?
- **functionality** - Does the software send, receive, and interpret email messages appropriately?
- **reliability** - For web-based services, is the server reliable, or is your email frequently unavailable due to maintenance, security problems, a high volume of users, or other reasons?
- **availability** - Do you need to be able to access your account from any computer?
- **ease of use** - Are the menus and options easy to understand and use?
- **visual appeal** - Do you find the interface appealing?

Each email client may have a different way of organizing drafted, sent, saved, and deleted mail. Familiarize yourself with the software so that you can find and store messages easily, and so that you don't unintentionally lose messages. Once you have chosen the software you want to use for your email, protect yourself and your contacts by following good security practices (see US-CERT Tips for more information).

Can you have use more than one email client?

You can have more than one email client, although you may have issues with compatibility. Some email accounts, such as those issued through your internet service provider (ISP) or place of employment, are only accessible from a computer that has appropriate privileges and settings for you to access that account. You can use any stand-alone email client to read those messages, but if you have more than one client installed on your machine, you should choose one as your default. When you click an email link in a browser or email message, your computer will open that default email client that you chose.

Most vendors give you the option to download their email software directly from their websites. Make sure to verify the authenticity of the site before downloading any files, and follow other good security practices, like using a firewall and keeping anti-virus software up to date, to further minimize risk (see Understanding Firewalls, Understanding Anti-Virus Software, and other US-CERT Tips for more information).

You can also maintain free email accounts through browser-based email clients (e.g., Yahoo!, Hotmail, Gmail) that you can access from any computer. Because these accounts are maintained directly on the vendors' servers, they don't interfere with other email accounts.

Understanding Digital Signatures

Digital signatures are a way to verify that an email message is really from the person who supposedly sent it and that it hasn't been changed.

What is a digital signature?

There are different types of digital signatures; this tip focuses on digital signatures for email messages. You may have received emails that have a block of letters and numbers at the bottom of the message. Although it may look like useless text or some kind of error, this information is actually a digital signature. To generate a signature, a mathematical algorithm is used to combine the information in a key with the information in the message. The result is a random-looking string of letters and numbers.

Why would you use one?

Because it is so easy for attackers and viruses to "spoof" email addresses (see Using Caution with Email Attachments for more information), it is sometimes difficult to identify legitimate messages. Authenticity may be especially important for business correspondence—if you are relying on someone to provide or verify information; you want to be sure that the information is coming from the correct source. A signed message also indicates that changes have not been made to the content since it was sent; any changes would cause the signature to break.

How does it work?

Before you can understand how a digital signature works, there are some terms you should know:

- Keys - Keys are used to create digital signatures. For every signature, there is a public key and a private key.
  - Private key - The private key is the portion of the key you use to actually sign an email message. The private key is protected by a password, and you should never give your private key to anyone.
  - Public key - The public key is the portion of the key that is available to other people. Whether you upload it to a public key ring or send it to someone, this is the key other people can use to check your signature. A list of other people who have signed your key is also included with your public key. You will only be able to see their identities if you already have their public keys on your key ring.
- Key ring - A key ring contains public keys. You have a key ring that contains the keys of people who have sent you their keys or whose keys you have gotten from a public key server. A public key server contains keys of people who have chosen to upload their keys.
- Fingerprint - When confirming a key, you will actually be confirming the unique series of letters and numbers that comprise the fingerprint of the key. The fingerprint is a different series of letters and numbers than the chunk of information that appears at the bottom of a signed email message.
- Key certificates - When you select a key on a key ring, you will usually see the key certificate, which contains information about the key, such as the key owner, the date the key was created, and the date the key will expire.
- "Web of trust" - When someone signs your key, they are confirming that the key actually belongs to you. The more signatures you collect, the stronger your key becomes. If someone sees that your key has been signed by other people that he or she trusts, he or she is more inclined to trust your key. **Note:** Just because someone else has trusted a key or you find it on a public key ring does not mean you should automatically trust it. You should always verify the fingerprint yourself.

The process for creating, obtaining, and using keys is fairly straightforward:

- Generate a key using software such as PGP, which stands for Pretty Good Privacy, or GnuPG, which stands for GNU Privacy Guard.

- Increase the authenticity of your key by having your key signed by co-workers or other associates who also have keys. In the process of signing your key, they will confirm that the fingerprint on the key you sent them belongs to you. By doing this, they verify your identity and indicate trust in your key.
- Upload your signed key to a public key ring so that if someone gets a message with your signature, they can verify the digital signature.
- Digitally sign your outgoing email messages. Most email clients have a feature to easily add your digital signature to your message.

There are a variety of mechanisms for creating digital signatures, and these mechanisms may operate differently. For example, S/MIME does not add a visible block of letters and numbers within the message, and its digital signatures are verified *indirectly* using a certificate authority instead of *directly* with other users in a web of trust. You may just see an icon or note on the message that the signature has been verified. If you get an error about a digital signature, try to contact the sender through a phone call or a separate email address that you know is valid to verify the authenticity of the message.

Using Caution with Email Attachments

While email attachments are a popular and convenient way to send documents, they are also a common source of viruses. Use caution when opening attachments, even if they appear to have been sent by someone you know.

Why can email attachments be dangerous?

Some of the characteristics that make email attachments convenient and popular are also the ones that make them a common tool for attackers:

- Email is easily circulated - Forwarding email is so simple that viruses can quickly infect many machines. Most viruses don't even require users to forward the email—they scan a users' computer for email addresses and automatically send the infected message to all of the addresses they find. Attackers take advantage of the reality that most users will automatically trust and open any message that comes from someone they know.
- Email programs try to address all users' needs - Almost any type of file can be attached to an email message, so attackers have more freedom with the types of viruses they can send.
- Email programs offer many "user-friendly" features - Some email programs have the option to automatically download email attachments, which immediately exposes your computer to any viruses within the attachments.

What steps can you take to protect yourself and others in your address book?

- **Be wary of unsolicited attachments, even from people you know** - Just because an email message looks like it came from your mom, grandma, or boss doesn't mean that it did. Many viruses can "spoof" the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This includes email messages that appear to be from your ISP or software vendor and claim to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.
- **Keep software up to date** - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Trust your instincts** - If an email or email attachment seems suspicious, don't open it, even if your anti-virus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the anti-virus software might not have the signature. At the very least, contact the person who supposedly sent the message to make sure it's legitimate before you open the attachment. However, especially in the case of forwards, even messages sent by a legitimate sender might contain a virus. If something about the email or the attachment makes you uncomfortable, there may be a good reason. Don't let your curiosity put your computer at risk.
- **Save and scan any attachments before opening them** - If you have to open an attachment before you can verify the source, take the following steps:
  - Be sure the signatures in your anti-virus software are up to date (see Understanding Anti-Virus Software for more information).
  - Save the file to your computer or a disk.
  - Manually scan the file using your anti-virus software.
  - If the file is clean and doesn't seem suspicious, go ahead and open it.
- **Turn off the option to automatically download attachments** - To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it.
- **Consider creating separate accounts on your computer** - Most operating systems give you the option of creating multiple user accounts with different privileges. Consider reading your email on an account with restricted privileges. Some viruses need "administrator" privileges to infect a computer.
- **Apply additional security practices** - You may be able to filter certain types of attachments through your email software (see Reducing Spam) or a firewall (see Understanding Firewalls).

Both the National Cyber Security Alliance and US-CERT have identified this topic as one of the top tips for home users.

Benefits of BCC

Although in many situations it may be appropriate to list email recipients in the To: or CC: fields, sometimes using the BCC: field may be the most desirable option.

What is BCC?

BCC, which stands for blind carbon copy, allows you to hide recipients in email messages. Addresses in the **To:** field and the **CC:** (carbon copy) field appear in messages, but users cannot see addresses of anyone you included in the **BCC:** field.

Why would you want to use BCC?

There are a few main reasons for using BCC:

- **Privacy** - Sometimes it's beneficial, even necessary, for you to let recipients know who else is receiving your email message. However, there may be instances when you want to send the same message to multiple recipients without letting them know who else is receiving the message. If you are sending email on behalf of a business or organization, it may be especially important to keep lists of clients, members, or associates confidential. You may also want to avoid listing an internal email address on a message being sent to external recipients .Another point to remember is that if any of the recipients use the "reply to all" feature to reply to your messages, all of the recipients listed in the **To:** and **CC:** fields will receive the reply. If there is potential for a response that is not appropriate for all recipients, consider using BCC.
- **Tracking** - Maybe you want to access or archive the email message you are sending at another email account. Or maybe you want to make someone, such as a supervisor or team member, aware of the email without actually involving them in the exchange. BCC allows you to accomplish these goals without advertising that you are doing it.

- **Respect for your recipients** - People often forward email messages without removing the addresses of previous recipients. As a result, messages that are repeatedly sent to many recipients may contain long lists of email addresses. Spammers and email-borne viruses may collect and target those addresses. To reduce the risk, encourage people who forward messages to you to use BCC so that your email address is less likely to appear in other people's inboxes and be susceptible to being harvested. To avoid becoming part of the problem, in addition to using BCC if you forward messages, take time to remove all existing email addresses within the message. The additional benefit is that the people you're sending the message to will appreciate not having to scroll through large sections of irrelevant information to get to the actual message.

How do you BCC an email message?

Most email clients have the option to BCC listed a few lines below the **To:** field. However, sometimes it is a separate option that is not listed by default. If you cannot locate it, check the help menu or the software's documentation.

If you want to BCC all recipients and your email client will not send a message without something in the **To:** field, consider using your own email address in that field. In addition to hiding the identity of other recipients, this option will enable you to confirm that the message was sent successfully.

Reducing Spam

Spam is a common, and often frustrating, side effect to having an email account. Although you will probably not be able to eliminate it, there are ways to reduce it.

What is spam?

Spam is the electronic version of “junk mail.” The term spam refers to unsolicited, often unwanted, email messages. Spam does not necessarily contain viruses—valid messages from legitimate sources could fall into this category.

How can you reduce the amount of spam?

- **Be careful about releasing your email address** – Think twice before you respond to any request for your email address, on the web, verbally, or on paper. Spammers can harvest any email address posted on a website. If you give your email address to a company, that information is often entered into a database so that customer information and preferences can be tracked. If these email databases are sold to or shared with other companies, you can receive email that you didn’t request.
- **Check privacy policies** – Before submitting your email address online, look for a privacy policy. Most reputable sites will have a link to their privacy policy from any form where you’re asked to submit personal data. You should read this policy before submitting your email address or any other personal information so that you know what the owners of the site plan to do with the information (see Protecting Your Privacy for more information).
- **Be aware of options selected by default** – When you sign up for some online accounts or services, there may be a section that provides you with the option to receive email about other products and services. Sometimes there are options selected by default, so if you do not deselect them, you could begin to receive email from those lists as well.

- **Use filters or spam tagging** – Many email programs offer filtering capabilities that allow you to block certain addresses or to allow only email from addresses on your contact list. Many ISPs also offer spam tagging services that allow the user the option to review suspected spam messages before they are deleted. Spam tagging can be useful in conjunction with filtering capabilities provided by many email programs.
- **Report messages as spam** – Most email clients offer an option to report a message as spam or junk. If your email client has that option, take advantage of it. Reporting messages as spam or junk helps to train the mail filter so that the messages aren't delivered to your inbox. However, check your junk or spam folders occasionally to look for legitimate messages that were incorrectly classified as spam.
- **Don't follow links in spam messages** – Some spam relies on generators that try variations of email addresses at certain domains. If you click a link within an email message or reply to a certain address, you are just confirming that your email address is valid. Unwanted messages that offer an "unsubscribe" option are particularly tempting, but this is often just a method for collecting valid addresses that are then targeted for other spam.
- **Disable the automatic downloading of graphics in HTML mail** – Many spammers send HTML mail with a linked graphic file that is then used to track who opens the mail message. When your mail client downloads the graphic from their web server, the spammers know you've opened the message. Disabling HTML mail entirely and viewing messages in plain text also prevents this problem.
- **Consider opening an additional email account** – Many domains offer free email accounts. If you frequently submit your email address (for online shopping, signing up for services, or including it on something like a comment card), you may want to have a secondary email account to protect your primary email account from any spam that could be generated. You could also use this secondary account when posting to public mailing lists, social networking sites, blogs, and web forums. If the account start to fill up with spam, you can get rid of it and open a different one.
- **Use privacy settings on social networking sites** – Social networking sites typically allow you to choose who has access to see your email address. Consider hiding your email account or changing the settings so that only a small group of people that you trust are able to see your address. Know that when you use applications on these sites, you may be granting permission for them to access your personal information. So, be cautious about which applications you choose to use.

Don't spam other people – Be a responsible and considerate user. Some people consider email forwards a type of spam, so be selective with the messages you redistribute. Don't forward every message to everyone in your address book, and if recipients ask that you not forward messages to them, respect their requests. In Canada, this could be seen as a Violation of CASL (Canadian Anti-Spam Legislation) and you can be faced with fines. http://crtc.gc.ca/eng/internet/anti.htm

General Information

Understanding ISPs

ISPs offer services like email and internet access. In addition to availability, you may want to consider other factors so that you find an ISP that supports all of your needs.

What is an ISP?

An ISP, or internet service provider, is a company that provides its customers access to the internet and other web services. In addition to maintaining a direct line to the internet, the company usually maintains web servers. By supplying necessary software, a password-protected user account, and a way to connect to the internet (e.g., modem), ISPs offer their customers the capability to browse the web and exchange email with other people. Some ISPs also offer additional services. With the development of smart phones, many cell phone providers are also ISPs.

ISPs can vary in size—some are operated by one individual, while others are large corporations. They may also vary in scope—some only support users in a particular city, while others have regional or national capabilities.

What services do ISPs provide?

Almost all ISPs offer email and web browsing capabilities. They also offer varying degrees of user support, usually in the form of an email address or customer support hotline. Most ISPs also offer web hosting capabilities, allowing users to create and maintain personal web pages; and some may even offer the service of developing the pages for you. Some ISPs bundle internet service with other services, such as television and telephone service. Many ISPs offer a wireless modem as part of their service so that customers can use devices equipped with Wi-Fi.

As part of normal operation, most ISPs perform backups of email and web files. If the ability to recover email and web files is important to you, check with your ISP to see if they back up the data; it might not be advertised as a service. Additionally, most ISPs implement firewalls to block some portion of incoming traffic, although you should consider this a supplement to your own security precautions, not a replacement (see Understanding Firewalls for more information).

How do you choose an ISP?

Traditional, broadband ISPs typically offer internet access through cable, DSL, or fiber optic options. The availability of these options may depend where you live. In addition to the type of access, there are other factors that you may want to consider:

- security - Do you feel that the ISP is concerned about security? Does it use encryption and SSL (see Protecting Your Privacy for more information) to protect any information you submit (e.g., user name, password)? If the ISP provides a wireless modem, what wireless security standards does it support, and are those standards compatible with your existing devices?
- privacy - Does the ISP have a published privacy policy? Are you comfortable with who has access to your information and how it is being handled and used?
- services - Does your ISP offer the services you want? Do they meet your requirements? Is there adequate support for the services? If the ISP provides a wireless modem, are its wireless standards compatible with your existing devices?
- cost - Are the ISP's costs affordable? Are they reasonable for the number of services you receive, as well as the level of those services? Are you sacrificing quality and security to get the lowest price?
- reliability - Are the services your ISP provides reliable, or are they frequently unavailable due to maintenance, security problems, a high volume of users, or other reasons? If the ISP knows that services will be unavailable for a particular reason, does it adequately communicate that information?
- user support - Are there published methods for contacting customer support? Do you receive prompt and friendly service? Do their hours of availability accommodate your needs? Do the consultants have the appropriate level of knowledge?
- speed - How fast is your ISP's connection? Is it sufficient for accessing your email or navigating the internet?
- recommendations - Have you heard or seen positive reviews about the ISP? Were they from trusted sources? Does the ISP serve your geographic area? If you've uncovered negative points, are they factors you are concerned about?

Why is it important to remember that the Internet is public?

Because the Internet is so accessible and contains a wealth of information, it has become a popular resource for communicating, for researching topics, and for finding information about people. It may seem less intimidating than actually interacting with other people because there is a sense of anonymity. However, you are not really anonymous when you are online, and it is just as easy for people to find information about you as it is for you to find information about them. Unfortunately, many people have become so familiar and comfortable with the Internet that they may adopt practices that make them vulnerable. For example, although people are typically wary of sharing personal information with strangers they meet on the street, they may not hesitate to post that same information online. Once it is online, it can be accessed by a world of strangers, and you have no idea what they might do with that information.

What guidelines can you follow when publishing information on the Internet?

- **View the Internet as a novel, not a diary** – Make sure you are comfortable with anyone seeing the information you put online. Expect that people you have never met will find your page; even if you are keeping an online journal or blog, write it with the expectation that it is available for public consumption. Some sites may use passwords or other security restrictions to protect the information, but these methods are not usually used for most websites. If you want the information to be private or restricted to a small, select group of people, the Internet is probably not the best forum.
- **Be careful what you advertise** – In the past, it was difficult to find information about people other than their phone numbers or address. Now, an increasing amount of personal information is available online, especially because people are creating personal web pages with information about themselves. When deciding how much information to reveal, realize that you are broadcasting it to the world. Supplying your email address may increase the amount of spam you receive (see Reducing Spam for more information). Providing details about your hobbies, your job, your family and friends, and your past may give attackers enough information to perform a successful social engineering attack (see Avoiding Social Engineering and Phishing Attacks for more information).
- **Realize that you can't take it back** – Once you publish something online, it is available to other people and to search engines. You can change or remove information after something has been published, but it is possible that someone has already seen the original version. Even if you try to remove the page(s) from the Internet, someone may have saved a copy of the page or used excerpts in another source. Some search engines "cache" copies of web pages; these cached copies may be available after a web page has been deleted or altered. Some web browsers may also maintain a cache of the web pages a user has visited, so the original version may be stored in a temporary file on the user's computer. Think about these implications before publishing information—once something is out there, you can't guarantee that you can completely remove it.

As a general practice, let your common sense guide your decisions about what to post online. Before you publish something on the Internet, determine what value it provides and consider the implications of having the information available to the public. Identity theft is an increasing problem, and the more information an attacker can gather about you, the easier it is to pretend to be you. Behave online the way you would behave in your daily life, especially when it involves taking precautions to protect yourself.

Why is Cyber Security a Problem?

You've heard the news stories about credit card numbers being stolen and email viruses spreading. Maybe you've even been a victim yourself. One of the best defenses is understanding the risks, what some of the basic terms mean, and what you can do to protect yourself against them.

What is cyber security?

It seems that everything relies on computers and the internet now — communication (email, cellphones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system?

Cyber security involves protecting that information by preventing, detecting, and responding to attacks.

What are the risks?

There are many risks, some more serious than others. Among these dangers are viruses erasing your entire system, someone breaking into your system and altering files, someone using your computer to attack others, or someone stealing your credit card information and making unauthorized purchases. Unfortunately, there's no 100% guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances.

What can you do?

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.

- Hacker, attacker, or intruder - These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting. The results can range from mere mischief (creating a virus with no intentionally negative impact) to malicious activity (stealing or altering information).
- Malicious code - Malicious code, sometimes called malware, is a broad category that includes any code that could be used to attack your computer. Malicious code can have the following characteristics:
  - It might require you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.
  - Some forms propagate without user intervention and typically start by exploiting a software vulnerability. Once the victim computer has been infected, the malicious code will attempt to find and infect other computers. This code can also propagate via email, websites, or network-based software.
  - Some malicious code claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.
- Viruses and worms are examples of malicious code.
- Vulnerability - In most cases, vulnerabilities are caused by programming errors in software. Attackers might be able to take advantage of these errors to infect your computer, so it is important to apply updates or patches that address known vulnerabilities.

This series of cyber security tips will give you more information about how to recognize and protect yourself from attacks.

Guidelines for Publishing Information Online

Remember that the Internet is a public resource. Avoid putting anything online that you don't want the public to see or that you may want to retract.

Why is it important to remember that the Internet is public?

Because the Internet is so accessible and contains a wealth of information, it has become a popular resource for communicating, for researching topics, and for finding information about people. It may seem less intimidating than actually interacting with other people because there is a sense of anonymity. However, you are not really anonymous when you are online, and it is just as easy for people to find information about you as it is for you to find information about them. Unfortunately, many people have become so familiar and comfortable with the Internet that they may adopt practices that make them vulnerable. For example, although people are typically wary of sharing personal information with strangers they meet on the street, they may not hesitate to post that same information online. Once it is online, it can be accessed by a world of strangers, and you have no idea what they might do with that information.

What guidelines can you follow when publishing information on the Internet?

- **View the Internet as a novel, not a diary** – Make sure you are comfortable with anyone seeing the information you put online. Expect that people you have never met will find your page; even if you are keeping an online journal or blog, write it with the expectation that it is available for public consumption. Some sites may use passwords or other security restrictions to protect the information, but these methods are not usually used for most websites. If you want the information to be private or restricted to a small, select group of people, the Internet is probably not the best forum.
- **Be careful what you advertise** – In the past, it was difficult to find information about people other than their phone numbers or address. Now, an increasing amount of personal information is available online, especially because people are creating personal web pages with information about themselves. When deciding how much information to reveal, realize that you are broadcasting it to the world. Supplying your email address may increase the amount of spam you receive (see Reducing Spam for more information). Providing details about your hobbies, your job, your family and friends, and your past may give attackers enough information to perform a successful social engineering attack (see Avoiding Social Engineering and Phishing Attacks for more information).
- **Realize that you can't take it back** – Once you publish something online, it is available to other people and to search engines. You can change or remove information after something has been published, but it is possible that someone has already seen the original version. Even if you try to remove the page(s) from the Internet, someone may have saved a copy of the page or used excerpts in another source. Some search engines "cache" copies of web pages; these cached copies may be available after a web page has been deleted or altered. Some web browsers may also maintain a cache of the web pages a user has visited, so the original version may be stored in a temporary file on the user's computer. Think about these implications before publishing information—once something is out there, you can't guarantee that you can completely remove it.

As a general practice, let your common sense guide your decisions about what to post online. Before you publish something on the Internet, determine what value it provides and consider the implications of having the information available to the public. Identity theft is an increasing problem, and the more information an attacker can gather about you, the easier it is to pretend to be you. Behave online the way you would behave in your daily life, especially when it involves taking precautions to protect yourself.

General Security

Before You Connect a New Computer to the Internet

Computers are an important part of everyday life. To keep your computer and information secure, it is important to properly set up your computer before connecting to the Internet.

Why Should I Care About Computer Security?

Computers help us maintain our financial, social, and professional relationships. We use them for banking and bill paying, online shopping, connecting with our friends and family through email and social networking sites, researching data posted on the Internet, and so much more. We rely heavily on our computers to provide these services, yet we sometimes overlook our need to secure them. Because our computers play such critical roles in our lives, and we input and view so much personally identifiable information (PII) on them, it’s imperative to maintain computer security that ensures the safe processing and storage of our information.

How Do I Improve the Security of My Home Computer?

Following are important steps you should consider to make your home computer more secure. While no individual step will eliminate your risk, together these defense-in-depth practices will make your home computer’s defense stronger and minimize the threat of malicious exploit.

Connect to a Secure Network

- Once your computer is connected to the Internet, it’s also connected to millions of other computers, which could allow attackers access to your computer. Information flows from the Internet to your home network by first coming into your modem, then into your router and finally into your computer. Although cable modem, digital subscriber line (DSL), and internet service providers (ISP) purport some level of security monitoring, it’s crucial to secure your router—the first securable device that receives information from the Internet. Be sure to secure it *before* you connect to the Internet to improve your computer’s security.

Enable and Configure a Firewall

- A firewall is a device that controls the flow of information between your computer and the Internet, similar to a router. Most modern operating systems include a software firewall. In addition to the operating system’s firewall, the majority of home routers have a firewall built in. Refer to your user’s guide for instructions on how to enable your firewall. Once your firewall is enabled, consult the user’s guide to learn how to configure the security settings and set a strong password to protect it against unwanted changes. (See Understanding Firewalls for more information.)

Install and Use Antivirus and Antispyware Software

- Installing an antivirus and antispyware software program and keeping it up to date is a critical step in protecting your computer. Many types of antivirus and antispyware software can detect the possible presence of malware by looking for patterns in the files or memory of your computer. This software uses virus signatures provided by software vendors to look for malware. Antivirus vendors frequently create new signatures to keep their software effective against newly discovered malware. Many antivirus and antispyware programs offer automatic updating. Enable that feature so your software always has the most current signatures. If automatic updates aren't offered, be sure to install the software from a reputable source, like the vendor's website or a CD from the vendor. (See Understanding Anti-Virus Software.)

Remove Unnecessary Software

- Intruders can attack your computer by exploiting software vulnerabilities (that is, flaws or weaknesses), so the less software you have installed, the fewer avenues for potential attack. Check the software installed on your computer. If you don't know what a software program does and don't use it, research it to determine whether it's necessary. Remove any software you feel isn't necessary after confirming it's safe to remove the software.
- Back up important files and data before removing unnecessary software in case you accidentally remove software essential to the operating system. If possible, locate the installation media for the software in case you need to reinstall it.

Modify Unnecessary Default Features

- Like removing unnecessary software and disabling nonessential services, modifying unnecessary default features eliminates opportunities for attack. Review the features that came enabled by default on your computer and disable or customize those you don't need or plan on using. As with nonessential services, be sure to research these features before disabling or modifying them.

Operate Under the Principle of Least Privilege

- In most instances of a malware infection, the malware can operate only under the rights of the logged-in user. To minimize the impact the malware can have if it successfully infects a computer, consider using a standard or restricted user account for day-to-day activities and only logging in with the administrator account (which has full operating privileges on the system) when you need to install or remove software or change system settings from the computer.

Secure Your Web Browser

- Web browsers installed on new computers usually don't have secure default settings. Securing your browser is another critical step in improving your computer's security because an increasing number of attacks take advantage of web browsers.

Apply Software Updates and Enable Future Automatic Updates

- Most software vendors release updates to patch or fix vulnerabilities, flaws, and weaknesses (bugs) in their software. Because intruders can exploit these bugs to attack your computer, keeping your software updated is important to help prevent infection.
- When you set up a new computer (and after you have completed the previous practices), go to your software vendors' websites to check for and install all available updates. Enable automatic updates if your vendors offer it; that will ensure your software is always updated, and you won't have to remember to do it yourself. Many operating systems and software have options for automatic updates. As you're setting up your new computer, be sure to enable these options if offered. Be cautious, however, because intruders can set up malicious websites that look nearly identical to legitimate sites. Only download software updates directly from a vendor's website, from a reputable source, or through automatic updating.

Use Good Security Practices

You can do some simple things to improve your computer's security. Some of the most important are:

- **Use caution with email attachments and untrusted links.** Malware is commonly spread by people clicking on an email attachment or a link that launches the malware. Don't open attachments or click on links unless you're certain they're safe, even if they come from a person you know. Some malware sends itself through an infected computer. While the email may appear to come from someone you know, it really came from a compromised computer. Be especially wary of attachments with sensational names, emails that contain misspellings, or emails that try to entice you into clicking on a link or attachment (for example, an email with a subject like that reads, "Hey, you won't believe this picture of you I saw on the Internet!"). (See Using Caution with Email Attachments.)

- **Use caution when providing sensitive information.** Some email or web pages that appear to come from a legitimate source may actually be the work of an attacker. An example is an email claiming to be sent from a system administrator requesting your password or other sensitive information or directing you to a website requesting that information. While Internet service providers may request that you change your password, they will never specify what you should change it to or ask you what it is. (See Avoiding Social Engineering and Phishing Attacks.)

Create strong passwords. Passwords that have eight or more characters, use a variety of uppercase and lowercase letters, and contain at least one symbol and number are best. Don't use passwords that people can easily guess like your birthday or your child's name. Password detection software can conduct dictionary attacks to try common words that may be used as passwords or conduct brute-force attacks where the login screen is pummeled with random attempts until it succeeds. The longer and more complex a password is, the harder these tools have to work to crack it. Also, when setting security verification questions, choose questions for which it is unlikely that an Internet search would yield the correct answer. (See Choosing and Protecting Passwords.)

International Mobile Safety Tips

Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.

October 29, 2013 marks the 4th Annual Asia Pacific Economic Cooperation Cyber Security Awareness Day. To recognize this occasion and in observance of the 10th year of National Cyber Security Awareness Month in the United States, US-CERT, along with its international partners from Asia and Europe, is promoting a set of International Mobile Safety Tips that were developed by the National Cyber Security Alliance, InfollutionZero, the Cyber Security Awareness Alliance in Singapore, and the iZ HERO Project.

The goal of the campaign is to use harmonized messaging to reach out to children, families, and schools across the world, and to provide them with core principles and simple tips that can help people of all ages enjoy safer and more secure use of digital devices and the Internet.

US-CERT encourages users and administrators to view the International Mobile Safety Tips at the following link and share them with their respective communities.

https://stopthinkconnect.org/campaigns/details/?id=442

The guidelines below provide core principles and recommendations for more secure use of digital devices and the Internet.

- Keep software updated. Running the most recent versions of your mobile operating system, security software, apps and Web browsers is among the best defenses against malware, viruses and other online threats.
- Keep your device secure by using a strong password to lock your smartphone or tablet.

- Enable two-step authentication when offered, and change passwords to any accounts you accessed while connected to an unfamiliar network.
- Before downloading an application (app), make sure you understand what information (i.e., location, your contacts, social networking profiles, etc.) the app would access and share before you download it. Download apps from trusted sources.
- Back up your contacts, photos, videos and other mobile device data with another device or cloud service on a weekly basis.
- When using a public or unsecured wireless connection, avoid using sites and apps that require personal information like log-ins.
- Automatically connecting to networks can create vulnerabilities exploitable by hackers and others. Switch off your Wi-Fi and Bluetooth connections when not in use.
- Delete any online communications (i.e., texts, emails, social media posts) that look suspicious, even if you think you know the source.
- When banking or shopping online, use only trusted apps or websites that begin with https://.
- The Golden Rule. Be respectful on your device. Treat others as you would like to be treated when texting, calling or using social networks.
- Share with care. Be a true friend when taking and sharing photos and videos with your smartphone. Get permission from friends before you share them via text or social networks.
- Be Web wise. Stay informed of the latest updates to your device and apps. Know what to do if something goes wrong.

Related Topics:
- Safety and Security for the Business Professional Traveling Abroad http://www.fbi.gov/about-us/investigate/counterintelligence/business-brochure
- (ST05-017) Cybersecurity for Electronic Devices http://www.us-cert.gov/ncas/tips/ST05-017
- (ST04-017) Protecting Physical Devices: Physical Security https://www.us-cert.gov/ncas/tips/ST04-017

Understanding Anti-Virus Software

Anti-virus software can identify and block many viruses before they can infect your computer. Once you install anti-virus software, it is important to keep it up to date.

What does anti-virus software do?

Although details may vary between packages, anti-virus software scans files or your computer's memory for certain patterns that may indicate the presence of malicious software (i.e., malware). Anti-virus software (sometimes more broadly referred to as anti-malware software) looks for patterns based on the signatures or definitions of known malware. Anti-virus vendors find new and updated malware daily, so it is important that you have the latest updates installed on your computer.

Once you have installed an anti-virus package, you should scan your entire computer periodically.

- **Automatic scans** – Most anti-virus software can be configured to automatically scan specific files or directories in real time and prompt you at set intervals to perform complete scans.
- **Manual scans** – If your anti-virus software does not automatically scan new files, you should manually scan files and media you receive from an outside source before opening them. This process includes:
  - Saving and scanning email attachments or web downloads rather than opening them directly from the source.
  - Scanning media, including CDs and DVDs, for malware before opening files.

How will the software respond when it finds malware?

Sometimes the software will produce a dialog box alerting you that it has found malware and ask whether you want it to "clean" the file (to remove the malware). In other cases, the software may attempt to remove the malware without asking you first. When you select an anti-virus package, familiarize yourself with its features so you know what to expect.

Which software should you use?

There are many vendors who produce anti-virus software, and deciding which one to choose can be confusing. Anti-virus software typically performs the same types of functions, so your decision may be driven by recommendations, particular features, availability, or price. Regardless of which package you choose, installing any anti-virus software will increase your level of protection.

How do you get the current malware information?

This process may differ depending on what product you choose, so find out what your anti-virus software requires. Many anti-virus packages include an option to automatically receive updated malware definitions. Because new information is added frequently, it is a good idea to take advantage of this option. Resist believing alarmist emails claiming that the "worst virus in history" or the "most dangerous malware ever" has been detected and will destroy your computer's hard drive. These emails are usually hoaxes. You can confirm malware information through your anti-virus vendor or through resources offered by other anti-virus vendors.

While installing anti-virus software is one of the easiest and most effective ways to protect your computer, it has its limitations. Because it relies on signatures, anti-virus software can only detect malware that has known characteristics. It is important to keep these signatures up-to-date. You will still be susceptible to malware that circulates before the anti-virus vendors add their signatures, so continue to take other safety precautions as well.

Understanding Firewalls

When anyone or anything can access your computer at any time, your computer is more susceptible to being attacked. You can restrict outside access to your computer and the information on it with a firewall.

What do firewalls do?

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network. Firewalls can be configured to block data from certain locations or applications while allowing relevant and necessary data through. (See Understanding Denial-of-Service Attacks and Understanding Hidden Threats: Rootkits and Botnets for more information.)

What type of firewall is best?

There are various types of firewalls with differences in where they are located and what types of activity they control. Firewalls may be broadly categorized as hardware or software. While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type you use.

- **Hardware** – Typically called network firewalls, these external devices are positioned between your computer and the Internet (or other network connection). Many vendors and some Internet service providers (ISPs) offer integrated small office / home office (SOHO) routers that also include firewall features. Hardware-based firewalls are particularly useful for protecting multiple computers and control the network activity that attempts to pass through them. The advantage of hardware-based firewalls is that they are separate devices running their own operating systems, so they provide an additional line of defense against attacks when compared to system or host-level protections.

- **Software** – Most operating systems include a built-in firewall feature that should be enabled for added protection even if you have an external firewall. Firewall software can also be obtained as separate software from your local computer store, software vendor, or ISP. If you download firewall software from the Internet, make sure it is from a reputable source (i.e., an established software vendor or service provider) and offered via a secure site. (See Understanding Web Site Certificates for more information.) The advantage of software firewalls is their ability to control the specific network behavior of individual applications on a system. Relying on a software firewall alone does provide some protection. However, realize that having the firewall on the same computer as the information you're trying to protect may hinder the firewall's ability to detect and stop malicious activity. This is especially true if your computer is already compromised by malware.

How do you know what configuration settings to apply?

Most commercially available firewall products, both hardware- and software-based, come pre-configured and ready to use. Since each firewall is different, you'll need to read and understand the documentation that comes with it to determine whether the default settings on your firewall are sufficient for your needs. Additional assistance may be available from your firewall vendor or your ISP. Also, alerts about current malicious activity (such as US-CERT's Cyber Security Alerts) sometimes include information about restrictions you can implement through your firewall.

Unfortunately, while properly configured firewalls may be effective at blocking some attacks, don't be lulled into a false sense of security. Firewalls do not guarantee that your computer will not be attacked. Firewalls primarily help protect against malicious traffic, not against malicious programs (malware), and may not protect you if you accidentally install malware on your computer. However, using a firewall in conjunction with other protective measures (such as anti-virus software and safe computing practices) will strengthen your resistance to attacks. (See Understanding Anti-Virus Software and other security tips for more information.)

Both the National Cyber Security Alliance and US-CERT have identified this topic as one of the top tips for home users.

Coordinating Virus and Spyware Defense

Software is an important part of cyber security. But in an attempt to protect yourself, you may unintentionally cause problems.

Isn't it better to have more protection?

Spyware and viruses can interfere with your computer's ability to process information or can modify or destroy data. You may feel that the more anti-virus and anti-spyware programs you install on your computer, the safer you will be. It is true that not all programs are equally effective, and they will not all detect the same malicious code. However, by installing multiple programs in an attempt to catch everything, you may introduce problems.

How can anti-virus or anti-spyware software cause problems?

It is important to use anti-virus and anti-spyware software (see Understanding Anti-Virus Software and Recognizing and Avoiding Spyware for more information). But too much or the wrong kind can affect the performance of your computer and the effectiveness of the software itself.

Scanning your computer for viruses and spyware uses some of the available memory on your computer. If you have multiple programs trying to scan at the same time, you may limit the amount of resources left to perform your tasks. Essentially, you have created a denial of service against yourself (see Understanding Denial-of-Service Attacks for more information). It is also possible that in the process of scanning for viruses and spyware, anti-virus or anti-spyware software may misinterpret the virus definitions of other programs. Instead of recognizing them as definitions, the software may interpret the definitions as actual malicious code. Not only could this result in false positives for the presence of viruses or spyware, but the anti-virus or anti-spyware software may actually quarantine or delete the other software.

How can you avoid these problems?

- **Investigate your options in advance** – Research available anti-virus and anti-spyware software to determine the best choice for you. Consider the amount of malicious code the software recognizes, and try to find out how frequently the virus definitions are updated. Also check for known compatibility issues with other software you may be running on your computer.
- **Limit the number of programs you install** – Many vendors are now releasing packages that incorporate both anti-virus and anti-spyware capabilities together. However, if you decide to choose separate programs, you really only need one anti-virus program and one anti-spyware program. If you install more, you increase your risk for problems.
- **Install the software in phases** – Install the anti-virus software first and test it for a few days before installing anti-spyware software. If problems develop, you have a better chance at isolating the source and then determining if it is an issue with the software itself or with compatibility.

Watch for problems – If your computer starts processing requests more slowly, you are seeing error messages when updating your virus definitions, your software does not seem to be recognizing malicious code, or other issues develop that cannot be easily explained, check your anti-virus and anti-spyware software.

Safeguarding Your Data

It is especially important to take extra security precautions when multiple people use your computer—or when you store sensitive personal and work-related data on your computer.

Why isn't "more" better?

Maybe there is an extra software program included with a program you bought. Or perhaps you found a free download online. You may be tempted to install the programs just because you can, or because you think you might use them later. However, even if the source and the software are legitimate, there may be hidden risks. And if other people use your computer, there are additional risks.

These risks become especially important if you use your computer to manage your personal finances (banking, taxes, online bill payment, etc.), store sensitive personal data, or perform work-related activities away from the office. However, there are steps you can take to protect yourself.

How can you protect both your personal and work-related data?

- **Use and maintain anti-virus software and a firewall** – Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall. (See Understanding Anti-Virus Software and Understanding Firewalls for more information.) Make sure to keep your virus definitions up to date.
- **Regularly scan your computer for spyware** – Spyware or adware hidden in software programs may affect the performance of your computer and give attackers access to your data. Use a legitimate anti-spyware program to scan your computer and remove any of these files. (See Recognizing and Avoiding Spyware for more information.) Many anti-virus products have incorporated spyware detection.
- **Keep software up to date** – Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should turn it on.
- **Evaluate your software's settings** – The default settings of most software enable all available functionality. However, attackers may be able to take advantage of this functionality to access your computer. It is especially important to check the settings for software that connects to the internet (browsers, email clients, etc.). Apply the highest level of security available that still gives you the functionality you need.
- **Avoid unused software programs** – Do not clutter your computer with unnecessary software programs. If you have programs on your computer that you do not use, consider uninstalling them. In addition to consuming system resources, these programs may contain vulnerabilities that, if not patched, may allow an attacker to access your computer.
- **Consider creating separate user accounts** – If there are other people using your computer, you may be worried that someone else may accidentally access, modify, and/or delete your files. Most operating systems (including Windows XP and Vista, Mac OS X, and Linux) give you the option of creating a different user account for each user, and you can set the amount of access and privileges for each account. You may also choose to have separate accounts for your work and personal purposes. While this approach will not completely isolate each area, it does offer some additional protection. However, it will not protect your computer against vulnerabilities that give an attacker administrative privileges. Ideally, you will have separate computers for work and personal use; this will offer a different type of protection.
- **Establish guidelines for computer use** – If there are multiple people using your computer, especially children, make sure they understand how to use the computer and internet safely. Setting boundaries and guidelines will help to protect your data.
- **Use passwords and encrypt sensitive files** – Passwords and other security features add layers of protection if used appropriately. (See Choosing and Protecting Passwords and Supplementing Passwords for more information.) By encrypting files, you ensure that unauthorized people can't view data even if they can physically access it. You may also want to consider options for full disk encryption, which prevents a thief from even starting your laptop without a passphrase. When you use encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.
- **Follow corporate policies for handling and storing work-related information** – If you use your computer for work-related purposes, make sure to follow any corporate policies for handling and storing the information. These policies were likely established to protect proprietary information and customer data, as well as to protect you and the company from liability. Even if it is not explicitly stated in your corporate policy, you should avoid allowing other people, including family members, to use a computer that contains corporate data.
- **Dispose of sensitive information properly** – Simply deleting a file does not completely erase it. To ensure that an attacker cannot access these files, make sure that you adequately erase sensitive files. (See Effectively Erasing Files for more information.)

Follow good security habits – Review other security tips for ways to protect yourself and your data.

Understanding Web Site Certificates

You may have been exposed to web site, or host, certificates if you have ever clicked on the padlock in your browser or, when visiting a web site, have been presented with a dialog box claiming that there is an error with the name or date on the certificate. Understanding what these certificates are may help you protect your privacy.

What are web site certificates?

If an organization wants to have a secure web site that uses encryption, it needs to obtain a site, or host, certificate. There are two elements that indicate that a site uses encryption (see Protecting Your Privacy for more information):

- a closed padlock, which, depending on your browser, may be located in the status bar at the bottom of your browser window or at the top of the browser window between the address and search fields
- a URL that begins with "https:" rather than "http:"

By making sure a web site encrypts your information and has a valid certificate, you can help protect yourself against attackers who create malicious sites to gather your information. You want to make sure you know where your information is going before you submit anything (see Avoiding Social Engineering and Phishing Attacks for more information).

If a web site has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organization. When you type a URL or follow a link to a secure web site, your browser will check the certificate for the following characteristics:

1. the web site address matches the address on the certificate
2. the certificate is signed by a certificate authority that the browser recognizes as a "trusted" authority

If the browser senses a problem, it may present you with a dialog box that claims that there is an error with the site certificate. This may happen if the name the certificate is registered to does not match the site name, if you have chosen not to trust the company who issued the certificate, or if the certificate has expired. You will usually be presented with the option to examine the certificate, after which you can accept the certificate forever, accept it only for that particular visit, or choose not to accept it. The confusion is sometimes easy to resolve (perhaps the certificate was issued to a particular department within the organization rather than the name on file). If you are unsure whether the certificate is valid or question the security of the site, do not submit personal information. Even if the information is encrypted, make sure to read the organization's privacy policy first so that you know what is being done with that information (see Protecting Your Privacy for more information).

Can you trust a certificate?

The level of trust you put in a certificate is connected to how much you trust the organization and the certificate authority. If the web address matches the address on the certificate, the certificate is signed by a trusted certificate authority, and the date is valid, you can be more confident that the site you want to visit is actually the site that you are visiting. However, unless you personally verify that certificate's unique fingerprint by calling the organization directly, there is no way to be absolutely sure.

When you trust a certificate you are, essentially, trusting the certificate authority to verify the organization's identity for you. However, it is important to realize that certificate authorities vary in how strict they are about validating all of the information in the requests and about making sure that their data is secure. By default, your browser contains a list of more than 100 trusted certificate authorities. That means that, by extension, you are trusting all of those certificate authorities to properly verify and validate the information. Before submitting any personal information, you may want to look at the certificate.

How do you check a certificate?

There are two ways to verify a web site's certificate in Internet Explorer or Firefox. One option is to click on the padlock icon. However, your browser settings may not be configured to display the status bar that contains the icon. Also, attackers may be able to create malicious web sites that fake a padlock icon and display a false dialog window if you click that icon. A more secure way to find information about the certificate is to look for the certificate feature in the menu options. This information may be under the file properties or the security option within the page information. You will get a dialog box with information about the certificate, including the following:

- who issued the certificate - You should make sure that the issuer is a legitimate, trusted certificate authority (you may see names like VeriSign, thawte, or Entrust). Some organizations also have their own certificate authorities that they use to issue certificates to internal sites such as intranets.
- who the certificate is issued to - The certificate should be issued to the organization who owns the web site. Do not trust the certificate if the name on the certificate does not match the name of the organization or person you expect.
- expiration date - Most certificates are issued for one or two years. One exception is the certificate for the certificate authority itself, which, because of the amount of involvement necessary to distribute the information to all of the organizations who hold its certificates, may be ten years. Be wary of organizations with certificates that are valid for longer than two years or with certificates that have expired.

Good Security Habits

There are some simple habits you can adopt that, if performed consistently, may dramatically reduce the chances that the information on your computer will be lost or corrupted.

How can you minimize the access other people have to your information?

You may be able to easily identify people who could, legitimately or not, gain *physical* access to your computer—family members, roommates, co-workers, members of a cleaning crew, and maybe others. Identifying the people who could gain *remote* access to your computer becomes much more difficult. As long as you have a computer and connect it to a network, you are vulnerable to someone or something else accessing or corrupting your information; however, you can develop habits that make it more difficult.

- **Lock your computer when you are away from it.** Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.
- **Disconnect your computer from the Internet when you aren't using it.** The development of technologies such as DSL and cable modems have made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the Internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. When you are connected, make sure that you have a firewall enabled (see Understanding Firewalls for more information).
- **Evaluate your security settings.** Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of the software, or if you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate (see Understanding Patches, Safeguarding Your Data, and Evaluating Your Web Browser's Security Settings for more information).

What other steps can you take?

Sometimes the threats to your information aren't from other people but from natural or technological causes. Although there is no way to control or prevent these problems, you can prepare for them and try to minimize the damage.

- **Protect your computer against power surges and brief outages.** Aside from providing outlets to plug in your computer and all of its peripherals, some power strips protect your computer against power surges. Many power strips now advertise compensation if they do not effectively protect your computer. Power strips alone will not protect you from power outages, but there are products that do offer an uninterruptible power supply when there are power surges or outages. During a lightning storm or construction work that increases the odds of power surges, consider shutting your computer down and unplugging it from all power sources.
- **Back up all of your data.** Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. You have probably already experienced this at least once— losing one or more files due to an accident, a virus or worm, a natural event, or a problem with your equipment. Regularly backing up your data on a CD or network reduces the stress and other negative consequences that result from losing important information. Determining how often to back up your data is a personal decision. If you are constantly adding or changing data, you may find weekly backups to be the best alternative; if your content rarely changes, you may decide that your backups do not need to be as frequent. You don't need to back up software that you own on CD-ROM or DVD-ROM—you can reinstall the software from the original media if necessary.

Both the National Cyber Security Alliance and US-CERT have identified this topic as one of the top tips for home users.

Mobile Devices

Protecting Portable Devices: Physical Security

Many computer users, especially those who travel for business, rely on laptops and personal internet-enabled devices like smartphones and tablets because they are small and easily transported. But while these characteristics make them popular and convenient, they also make them an ideal target for thieves. Make sure to secure your mobile devices to protect both the machine and the information they contain.

What is at risk?

Only you can determine what is actually at risk. If a thief steals your laptop or mobile device, the most obvious loss is the machine itself. However, if the thief is able to access the information on the computer or mobile device, all of the information stored on the device is at risk, as well as any additional information that could be accessed as a result of the data stored on the device itself.

Sensitive corporate information or customer account information should not be accessed by unauthorized people. You've probably heard news stories about organizations panicking because laptops with confidential information on them have been lost or stolen. But even if there isn't any sensitive corporate information on your laptop or mobile device, think of the other information at risk: information about appointments, passwords, email addresses and other contact information, personal information for online accounts, etc.

How can you protect your laptop or internet-enabled device?

- **Password-protect your computer** - Make sure that you have to enter a password to log in to your computer or mobile device (see Choosing and Protecting Passwords for more information).
- **Keep your valuables with you at all times** - When traveling, keep your device with you. Meal times are optimum times for thieves to check hotel rooms for unattended laptops. If you are attending a conference or trade show, be especially wary—these venues offer thieves a wider selection of devices that are likely to contain sensitive information, and the conference sessions offer more opportunities for thieves to access guest rooms.
- **Downplay your laptop or mobile device** - There is no need to advertise to thieves that you have a laptop or mobile device. Avoid using your device in public areas, and consider non-traditional bags for carrying your laptop.
- **Be aware of your surroundings** - If you do use your laptop or mobile device in a public area, pay attention to people around you. Take precautions to shield yourself from "shoulder surfers"—make sure that no one can see you type your passwords or see any sensitive information on your screen.
- **Consider an alarm or lock** - Many companies sell alarms or locks that you can use to protect or secure your laptop. If you travel often or will be in a heavily populated area, you may want to consider investing in an alarm for your laptop bag or a lock to secure your laptop to a piece of furniture.
- **Back up your files** - If your mobile device is stolen, it's bad enough that someone else may be able to access your information. To avoid losing all of the information, make backups of important information and store the backups in a separate location (see Good Security Habits for more information). Not only will you still be able to access the information, but you'll be able to identify and report exactly what information is at risk.

What can you do if your laptop or mobile device is lost or stolen?

Report the loss or theft to the appropriate authorities. These parties may include representatives from law enforcement agencies, as well as hotel or conference staff. If your device contained sensitive corporate or customer account information, immediately report the loss or theft to your organization so that they can act quickly.

Cybersecurity for Electronic Devices

When you think about cybersecurity, remember that electronics such as smartphones and other internet-enabled devices may also be vulnerable to attack. Take appropriate precautions to limit your risk.

Why does cybersecurity extend beyond computers?

Actually, the issue is not that cybersecurity extends beyond computers; it is that computers extend beyond traditional laptops and desktops. Many electronic devices are computers—from cell phones and tablets to video games and car navigation systems. While computers provide increased features and functionality, they also introduce new risks. Attackers may be able to take advantage of these technological advancements to target devices previously considered "safe." For example, an attacker may be able to infect your cell phone with a virus, steal your phone or wireless service, or access the data on your device. Not only do these activities have implications for your personal information, but they could also have serious consequences if you store corporate information on the device.

What types of electronics are vulnerable?

Any piece of electronic equipment that uses some kind of computerized component is vulnerable to software imperfections and vulnerabilities. The risks increase if the device is connected to the internet or a network that an attacker may be able to access. Remember that a wireless connection also introduces these risks (see Securing Wireless Networks for more information). The outside connection provides a way for an attacker to send information to or extract information from your device.

How can you protect yourself?

- **Remember physical security** - Having physical access to a device makes it easier for an attacker to extract or corrupt information. Do not leave your device unattended in public or easily accessible areas (see Protecting Portable Devices: Physical Security for more information).

- **Keep software up to date** - If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities.
- **Use good passwords** - Choose devices that allow you to protect your information with passwords. Select passwords that will be difficult for thieves to guess, and use different passwords for different programs and devices (see Choosing and Protecting Passwords for more information). Do not choose options that allow your computer to remember your passwords.
- **Disable remote connectivity** - Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use.
- **Encrypt files** - If you are storing personal or corporate information, see if your device offers the option to encrypt the files. By encrypting files, you ensure that unauthorized people can't view data even if they can physically access it. When you use encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.
- **Be cautious of public Wi-Fi networks** - Before you connect to any public wireless hotspot – like on an airplane or in an airport, hotel, train/bus station or café:
  - Be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.
  - Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network.

Only use sites that begin with “https://” when online shopping or banking. Using your mobile network connection is generally more secure than using a public wireless network.

Using Caution with USB Drives

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks.

What security risks are associated with USB drives?

Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

One option is for attackers to use your USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware, that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on their computers.

Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive. Victims may not even realize that their computers were attacked.

The most obvious security risk for USB drives, though, is that they are easily lost or stolen (see Protecting Portable Devices: Physical Security for more information). If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

How can you protect your data?

There are steps you can take to protect the data on your USB drive and on any computer that you might plug the drive into:

- **Take advantage of security features** - Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost (see Protecting Portable Devices: Data Security for more information).
- **Keep personal and business USB drives separate** - Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.
- **Use and maintain security software, and keep all software up to date** - Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions current (see Understanding Firewalls, Understanding Anti-Virus Software, and Recognizing and Avoiding Spyware for more information). Also, keep the software on your computer up to date by applying any necessary patches.
- **Do not plug an unknown USB drive into your computer** - If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into your computer to view the contents or to try to identify the owner.

Disable Autorun - The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically. In How to disable the Autorun functionality in Windows (link is external) , Microsoft has provided a wizard to disable Autorun. In the "More Information" section, look for the Microsoft® Fix it icon under the heading "How to disable or enable all Autorun features in Windows 7 and other operating systems."

Securing Wireless Networks

How do wireless networks work?

As the name suggests, wireless networks, sometimes called WiFi, allow you to connect to the internet without relying on wires. If your home, office, airport, or even local coffee shop has a wireless connection, you can access the network from anywhere that is within that wireless area.

Wireless networks rely on radio waves rather than wires to connect computers to the internet. A transmitter, known as a wireless access point or gateway, is wired into an internet connection. This provides a "hotspot" that transmits the connectivity over radio waves. Hotspots have identifying information, including an item called an SSID (service set identifier), that allow computers to locate them. Computers that have a wireless card and have permission to access the wireless frequency can take advantage of the network connection. Some computers may automatically identify open wireless networks in a given area, while others may require that you locate and manually enter information such as the SSID.

What security threats are associated with wireless networks?

Because wireless networks do not require a wire between a computer and the internet connection, it is possible for attackers who are within range to hijack or intercept an unprotected connection. A practice known as war driving involves individuals equipped with a computer, a wireless card, and a GPS device driving through areas in search of wireless networks and identifying the specific coordinates of a network location. This information is then usually posted online. Some individuals who participate in or take advantage of war driving have malicious intent and could use this information to hijack your home wireless network or intercept the connection between your computer and a particular hotspot.

What can you do to minimize the risks to your wireless network?

- **Change default passwords** - Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily found online, so they don't provide any protection. Changing default passwords makes it harder for attackers to take control of the device (see Choosing and Protecting Passwords for more information).
- **Restrict access** - Only allow authorized users to access your network. Each piece of hardware connected to a network has a MAC (media access control) address. You can restrict or allow access to your network by filtering MAC addresses. Consult your user documentation to get specific information about enabling these features. There are also several technologies available that require wireless users to authenticate before accessing the network.
- **Encrypt the data on your network** - WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) both encrypt information on wireless devices. However, WEP has a number of security issues that make it less effective than WPA, so you should specifically look for gear that supports encryption via WPA. Encrypting the data would prevent anyone who might be able to access your network from viewing your data (see Understanding Encryption for more information).
- **Protect your SSID** - To avoid outsiders easily accessing your network, avoid publicizing your SSID. Consult your user documentation to see if you can change the default SSID to make it more difficult to guess.
- **Install a firewall** - While it is a good security practice to install a firewall on your network, you should also install a firewall directly on your wireless devices (a host-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer (see Understanding Firewalls for more information).

Maintain anti-virus software - You can reduce the damage attackers may be able to inflict on your network and wireless computer by installing anti-virus software and keeping your virus definitions up to date (see Understanding Anti-Virus Software for more information). Many of these programs also have additional features that may protect against or detect spyware and Trojan horses (see Recognizing and Avoiding Spyware and Why is Cyber Security a Problem? for more information).

Protecting Portable Devices: Data Security

In addition to taking precautions to protect your portable devices, it is important to add another layer of security by protecting the data itself.

Why do you need another layer of protection?

Although there are ways to physically protect your laptop, PDA, or other portable device (see Protecting Portable Devices: Physical Security for more information), there is no guarantee that it won't be stolen. After all, as the name suggests, portable devices are designed to be easily transported. The theft itself is, at the very least, frustrating, inconvenient, and unnerving, but the exposure of information on the device could have serious consequences. Also, remember that any devices that are connected to the internet, especially if it is a wireless connection, are also susceptible to network attacks (see Securing Wireless Networks for more information).

What can you do?

- **Use passwords correctly** - In the process of getting to the information on your portable device, you probably encounter multiple prompts for passwords. Take advantage of this security. Don't choose options that allow your computer to remember passwords, don't choose passwords that thieves could easily guess, use different passwords for different programs, and take advantage of additional authentication methods (see Choosing and Protecting Passwords and Supplementing Passwords for more information).
- **Consider storing important data separately** - There are many forms of storage media, including CDs, DVDs, and removable flash drives (also known as USB drives or thumb drives). By saving your data on removable media and keeping it in a different location (e.g., in your suitcase instead of your laptop bag), you can protect your data even if your laptop is stolen. You should make sure to secure the location where you keep your data to prevent easy access. It may be helpful to carry storage media with other valuables that you keep with you at all times and that you naturally protect, such as a wallet or keys.
- **Encrypt files** - By encrypting files, you ensure that unauthorized people can't view data even if they can physically access it. You may also want to consider options for full disk encryption, which prevents a thief from even starting your laptop without a passphrase. When you use encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.
- **Install and maintain anti-virus software** - Protect laptops and PDAs from viruses the same way you protect your desktop computer. Make sure to keep your virus definitions up to date (see Understanding Anti-Virus Software for more information). If your anti-virus software doesn't include anti-spyware software, consider installing separate software to protect against that threat (see Recognizing and Avoiding Spyware and Coordinating Virus and Spyware Defense for more information).
- **Install and maintain a firewall** - While always important for restricting traffic coming into and leaving your computer, firewalls are especially important if you are traveling and using different networks. Firewalls can help prevent outsiders from gaining unwanted access (see Understanding Firewalls for more information).

Back up your data - Make sure to back up any data you have on your computer onto a CD-ROM, DVD-ROM, or network (see Good Security Habits) Not only will this ensure that you will still have access to the information if your device is stolen, but it could help you identify exactly which information a thief may be able to access. You may be able to take measures to reduce the amount of damage that exposure could cause.

Defending Cell Phones and PDAs Against Attack

As cell phones and PDAs become more technologically advanced, attackers are finding new ways to target victims. By using text messaging or email, an attacker could lure you to a malicious site or convince you to install malicious code on your portable device.

What unique risks do cell phones and PDAs present?

Most current cell phones have the ability to send and receive text messages. Some cell phones and PDAs also offer the ability to connect to the internet. Although these are features that you might find useful and convenient, attackers may try to take advantage of them. As a result, an attacker may be able to accomplish the following:

- **abuse your service** - Most cell phone plans limit the number of text messages you can send and receive. If an attacker spams you with text messages, you may be charged additional fees. An attacker may also be able to infect your phone or PDA with malicious code that will allow them to use your service. Because the contract is in your name, you will be responsible for the charges.
- **lure you to a malicious web site** - While PDAs and cell phones that give you access to email are targets for standard phishing attacks, attackers are now sending text messages to cell phones. These messages, supposedly from a legitimate company, may try to convince you to visit a malicious site by claiming that there is a problem with your account or stating that you have been subscribed to a service. Once you visit the site, you may be lured into providing personal information or downloading a malicious file (see Avoiding Social Engineering and Phishing Attacks for more information).
- **use your cell phone or PDA in an attack** - Attackers who can gain control of your service may use your cell phone or PDA to attack others. Not only does this hide the real attacker's identity, it allows the attacker to increase the number of targets (see Understanding Denial-of-Service Attacks for more information).
- **gain access to account information** - In some areas, cell phones are becoming capable of performing certain transactions (from paying for parking or groceries to conducting larger financial transactions). An attacker who can gain access to a phone that is used for these types of transactions may be able to discover your account information and use or sell it.

What can you do to protect yourself?

- **Follow general guidelines for protecting portable devices** - Take precautions to secure your cell phone and PDA the same way you should secure your computer (see Cybersecurity for Electronic Devices and Protecting Portable Devices: Data Security for more information).
- **Be careful about posting your cell phone number and email address** - Attackers often use software that browses web sites for email addresses. These addresses then become targets for attacks and spam (see Reducing Spam for more information). Cell phone numbers can be collected automatically, too. By limiting the number of people who have access to your information, you limit your risk of becoming a victim.
- **Do not follow links sent in email or text messages** - Be suspicious of URLs sent in unsolicited email or text messages. While the links may appear to be legitimate, they may actually direct you to a malicious web site.
- **Be wary of downloadable software** - There are many sites that offer games and other software you can download onto your cell phone or PDA. This software could include malicious code. Avoid downloading files from sites that you do not trust. If you are getting the files from a supposedly secure site, look for a web site certificate (see Understanding Web Site Certificates for more information). If you do download a file from a web site, consider saving it to your computer and manually scanning it for viruses before opening it.

Evaluate your security settings - Make sure that you take advantage of the security features offered on your device. Attackers may take advantage of Bluetooth connections to access or download information on your device. Disable Bluetooth when you are not using it to avoid unauthorized access.

Privacy

Supplementing Passwords

Passwords are a common form of protecting information, but passwords alone may not provide adequate security. For the best protection, look for sites that have additional ways to verify your identity.

Why aren't passwords sufficient?

Passwords are a good first layer of protection, but attackers can guess or intercept passwords. Additional security measures can protect you even if an attacker does obtain your password. You can strengthen that first layer of protection by avoiding passwords based on personal information or words found in the dictionary; building passwords from combinations of numbers, special characters, and lowercase and capital letters; and not sharing your passwords with anyone else. (See Choosing and Protecting Passwords for more information.)

What additional levels of security are available?

Multi-factor authentication, simultaneously using multiple pieces of information to verify your identity, is becoming more common. (You may see multi-factor authentication (MFA) advertised as two-factor authentication.) Even if an attacker obtains your password, he may not be able to access your account if it's protected by MFA. The theory behind this approach is similar to requiring two or more forms of identification or two keys to open a safe deposit box. You should turn on MFA where it's available. Authentication categories include **something you know** (e.g., answers to secret questions or passwords); **something you have** (e.g., a token or other item in your possession); and **something you are** (e.g., a biometric measure such as a fingerprint).

Something you know – This includes passwords or pre-established answers to questions. (See tips below for setting up good answers to these "secret questions.")

Something you have – This could be a small physical token such as a smart card, a special key fob, or USB drive. You might use this token in conjunction with a password to log into an account. However, software-based tokens are also common. These software-based tokens can generate a single-use login personal identification number (PIN). Other variations include SMS messages, phone calls, or emails sent to the user with a verification PIN. These token PINs can often be used only once and are voided immediately after use. So, even if an attacker intercepts the exchange, the attacker will not be able to use the information again to access your account.

Something you are – Biometric identification can include scanning of eyes (retinas or irises) or fingerprints, other facial recognition, voice recognition, or authentication through signatures or keystroke movements. A common example of biometric identification is the fingerprint scanner used to sign in users on many modern smartphones.

Another form of verification is the use of **personal web certificates.** Unlike certificates used to identify web sites (see Understanding Web Site Certificates), personal web certificates are used to identify individual users. A website using personal web certificates relies on these certificates and the authentication process of the corresponding public/private keys to verify that you are who you claim to be. (See Understanding Digital Signatures and Understanding Encryption). Because information identifying you is embedded within the certificate, an additional password is unnecessary. However, you should have a password to protect your private key so that attackers can't gain access to your key and represent themselves as you. This process is similar to MFA, but it differs in this way: the password protecting your private key is used to decrypt the information on your computer and is never sent over the network.

What if you lose your password or certificate?

Perhaps you've forgotten your password or you've reformatted your computer and lost your personal web certificate. Most organizations have procedures for giving you access to your information in these situations. For the best security, keep information on your account up to date. This includes alternate email addresses or phone numbers that can help verify your identity if you forget your password.

In the case of certificates, you may need to request that the organization issue you a new one. In the case of passwords, you may just need a reminder. No matter what happened, the organization needs a way to verify your identity. To do this, many organizations rely on ***secret questions***.

When you open a new account (e.g. email, credit card), some organizations will prompt you to provide them with the answer to a question. They may ask you this question if you forget your password or request information about your account over the phone. If your answer matches the answer they have on file, they will assume that they are actually communicating with you. In theory, secret questions and answers can protect your information. However, common secret questions ask for mother's maiden name, social security number, date of birth, or your pet's name. Because so much personal information is now available online or through other public sources, attackers may be able to discover the answers to these questions.

Realize that the secret question is really just an additional password. When establishing the answer, you don't have to supply real information. In fact, if you're asked to provide a pre-established answer, dishonesty may be the best policy. Choose your answer as you would choose any other good password, store it in a secure location (e.g., in a password manager), and don't share it with other people.

While additional security practices offer you more protection than a password alone, they should not be considered completely effective. Increasing the level of security only makes it more difficult for attackers to access your information. Be aware of MFA and other security practices when choosing a bank, credit card company, or other organization that will have access to your personal information. Don't be afraid to ask what kind of security practices the organization uses.

Effectively Erasing Files

Before selling or discarding an old computer, or throwing away a CD or DVD, you naturally make sure that you've copied all of the files you need. You've probably also attempted to delete your personal files so that other people aren't able to access them. However, unless you have taken the proper steps to make sure the hard drive, CD, or DVD is erased, people may still be able to resurrect those files.

Where do deleted files go?

When you delete a file, depending on your operating system and your settings, it may be transferred to your trash or recycle bin. This "holding area" essentially protects you from yourself—if you accidentally delete a file, you can easily restore it. However, you may have experienced the panic that results from emptying the trash bin prematurely or having a file seem to disappear on its own. The good news is that even though it may be difficult to locate, the file is probably still somewhere on your machine. The bad news is that even though you think you've deleted a file, an attacker or other unauthorized person may be able to retrieve it.

What are the risks?

Think of the information you have saved on your computer. Is there banking or credit card account information? Tax returns? Passwords? Medical or other personal data? Personal photos? Sensitive corporate information? How much would someone be able to find out about you or your company by looking through your computer files?

Depending on what kind of information an attacker can find, he or she may be able to use it maliciously. You may become a victim of identity theft. Another possibility is that the information could be used in a social engineering attack. Attackers may use information they find about you or an organization you're affiliated with to appear to be legitimate and gain access to sensitive data (see Avoiding Social Engineering and Phishing Attacks for more information).

Can you erase files by reformatting?

Reformatting your hard drive, CD, or DVD may superficially delete the files, but the information is still buried somewhere. Unless those areas of the disk are effectively overwritten with new content, it is still possible that knowledgeable attackers may be able to access the information.

How can you be sure that your information is completely erased?

Some people use extreme measures to make sure their information is destroyed, but these measures can be dangerous and may not be completely successful. Your best option is to investigate software programs and hardware devices that claim to erase your hard drive, CD, or DVD. Even so, these programs and devices have varying levels of effectiveness. When choosing a software program to perform this task, look for the following characteristics:

- **"Secure Erase" is performed** - Secure Erase is a standard in modern hard drives. If you select a program that runs the Secure Erase command, it will erase data by overwriting all areas of the hard drive, even areas that are not being used.
- **data is written multiple times** - It is important to make sure that not only is the information erased, but new data is written over it. By adding multiple layers of data, the program makes it difficult for an attacker to "peel away" the new layer. Three to seven passes is fairly standard and should be sufficient.
- **random data is used** - Using random data instead of easily identifiable patterns makes it harder for attackers to determine the pattern and discover the original information underneath.
- **zeros are used in the final layer** - Regardless of how many times the program overwrites the data, look for programs that use all zeros in the last layer. This adds an additional level of security.

While many of these programs assume that you want to erase an entire disk, there are programs that give you the option to erase and overwrite individual files.

An effective way to ruin a CD or DVD is to wrap it in a paper towel and shatter it. However, there are also hardware devices that erase CDs or DVDs by destroying their surface. Some of these devices actually shred the media itself, while others puncture the writable surface with a pattern of holes. Many paper shredders will also shred CDs and DVDs. If you decide to use one of these devices, compare the various features and prices to determine which option best suits your needs.

How Anonymous Are You?

You may think that you are anonymous as you browse websites, but pieces of information about you are always left behind. You can reduce the amount of information revealed about you by visiting legitimate sites, checking privacy policies, and minimizing the amount of personal information you provide.

What information is collected?

When you visit a website, a certain amount of information is automatically sent to the site. This information may include the following:

- **IP address** - Each computer on the internet is assigned a specific, unique IP (internet protocol) address. Your computer may have a static IP address or a dynamic IP address. If you have a static IP address, it never changes. However, some ISPs own a block of addresses and assign an open one each time you connect to the internet—this is a dynamic IP address. You can determine your computer's IP address at any given time by visiting www.showmyip.com (link is external) .
- **domain name** - The internet is divided into domains, and every user's account is associated with one of those domains. You can identify the domain by looking at the end of URL; for example, .edu indicates an educational institution, .gov indicates a US government agency, .org refers to organization, and .com is for commercial use. Many countries also have specific domain names. The list of active domain names is available from the Internet Assigned Numbers Authority (IANA).
- **software details** - It may be possible for an organization to determine which browser, including the version, that you used to access its site. The organization may also be able to determine what operating system your computer is running.
- **page visits** - Information about which pages you visited, how long you stayed on a given page, and whether you came to the site from a search engine is often available to the organization operating the website.

If a website uses cookies, the organization may be able to collect even more information, such as your browsing patterns, which include other sites you've visited. If the site you're visiting is malicious, files on your computer, as well as passwords stored in the temporary memory, may be at risk.

How is this information used?

Generally, organizations use the information that is gathered automatically for legitimate purposes, such as generating statistics about their sites. By analyzing the statistics, the organizations can better understand the popularity of the site and which areas of content are being accessed the most. They may be able to use this information to modify the site to better support the behavior of the people visiting it.

Another way to apply information gathered about users is marketing. If the site uses cookies to determine other sites or pages you have visited, it may use this information to advertise certain products. The products may be on the same site or may be offered by partner sites.

However, some sites may collect your information for malicious purposes. If attackers are able to access files, passwords, or personal information on your computer, they may be able to use this data to their advantage. The attackers may be able to steal your identity, using and abusing your personal information for financial gain. A common practice is for attackers to use this type of information once or twice, then sell or trade it to other people. The attackers profit from the sale or trade, and increasing the number of transactions makes it more difficult to trace any activity back to them. The attackers may also alter the security settings on your computer so that they can access and use your computer for other malicious activity.

Are you exposing any other personal information?

While using cookies may be one method for gathering information, the easiest way for attackers to get access to personal information is to ask for it. By representing a malicious site as a legitimate one, attackers may be able to convince you to give them your address, credit card information, social security number, or other personal data (see Avoiding Social Engineering and Phishing Attacks for more information).

How can you limit the amount of information collected about you?

- **Be careful supplying personal information** - Unless you trust a site, don't give your address, password, or credit card information. Look for indications that the site uses SSL to encrypt your information (see Protecting Your Privacy for more information). Although some sites require you to supply your social security number (e.g., sites associated with financial transactions such as loans or credit cards), be especially wary of providing this information online.
- **Limit cookies** - If an attacker can access your computer, he or she may be able to find personal data stored in cookies. You may not realize the extent of the information stored on your computer until it is too late. However, you can limit the use of cookies (see Browsing Safely: Understanding Active Content and Cookies for more information).
- **Browse safely** - Be careful which websites you visit; if it seems suspicious, leave the site. Also make sure to take precautions by increasing your security settings (see Evaluating Your Web Browser's Security Settings for more information), keeping your virus definitions up to date (see Understanding Anti-Virus Software for more information), and scanning your computer for spyware (see Recognizing and Avoiding Spyware for more information).

Additional information

Securing Your Web Browser

Understanding Encryption

Encrypting data is a good way to protect sensitive information. It ensures that the data can only be read by the person who is authorized to have access to it.

What is encryption?

In very basic terms, encryption is a way to send a message in code. The only person who can decode the message is the person with the correct key; to anyone else, the message looks like a random series of letters, numbers, and characters.
Encryption is especially important if you are trying to send sensitive information that other people should not be able to access. Because email messages are sent over the internet and might be intercepted by an attacker, it is important to add an additional layer of security to sensitive information.

How is it different from digital signatures?

Like digital signatures, public-key encryption utilizes software such as PGP, converts information with mathematical algorithms, and relies on public and private keys, but there are differences:

- The purpose of encryption is confidentiality—concealing the content of the message by translating it into a code. The purpose of digital signatures is integrity and authenticity—verifying the sender of a message and indicating that the content has not been changed. Although encryption and digital signatures can be used independently, you can also sign an encrypted message.
- When you sign a message, you use your private key, and anybody who has your public key can verify that the signature is valid (see Understanding Digital Signatures for more information). When you encrypt a message, you use the public key for the person you're sending it to, and his or her private key is used to decrypt the message. Because people should keep their private keys confidential and should protect them with passwords, the intended recipient should be the only one who is able to view the information.

How does encryption work?

- Obtain the public key for the person you want to be able to read the information. If you get the key from a public key ring, contact the person directly to confirm that the series of letters and numbers associated with the key is the correct fingerprint.

- Encrypt the email message using their public key. Most email clients have a feature to easily perform this task.
- When the person receives the message, he or she will be able to decrypt it.

Protecting Your Privacy

Before submitting your email address or other personal information online, you need to be sure that the privacy of that information will be protected. To protect your identity and prevent an attacker from easily accessing additional information about you, be cautious about providing your birth date, Social Security number, or other personal information online.

How do you know if your privacy is being protected?

- **Privacy policy** – Before submitting your name, email address, or other personal information on a website, look for the site's privacy policy. This policy should state how the information will be used and whether or not the information will be distributed to other organizations. Companies sometimes share information with partner vendors who offer related products or may offer options to subscribe to particular mailing lists. Look for indications that you are being added to mailing lists by default—failing to deselect those options may lead to unwanted spam. If you cannot find a privacy policy on a website, consider contacting the company to inquire about the policy before you submit personal information, or find an alternate site. Privacy policies sometimes change, so you may want to review them periodically.
- **Evidence that your information is being encrypted** – To prevent attackers from stealing your personal information, online submissions should be encrypted so that it can only be read by the appropriate recipient. Many sites use Secure Sockets Layer (SSL) or Hypertext Transport Protocol Secure (https). A lock icon in the bottom right corner of the window indicates that your information will be encrypted. (See Understanding Web Site Certificates for more information.) Some sites also indicate whether the data is encrypted when it is stored. If data is encrypted in transit but stored insecurely, an attacker who is able to break into the vendor's system could access your personal information.

What additional steps can you take to protect your privacy?

- **Do business with credible companies** – Before supplying any information online, consider the answers to the following questions: Do you trust the business? Is it an established organization with a credible reputation? Does the information on the site suggest that there is a concern for the privacy of user information? Is legitimate contact information provided? If you answered “No” to any of these questions, avoid doing business online with these companies.

- **Do not use your primary email address in online submissions** – Submitting your email address could result in spam. If you do not want your primary email account flooded with unwanted messages, consider opening an additional email account for use online. (See Reducing Spam for more information.) Make sure to log in to the account on a regular basis in case the vendor sends information about changes to policies.
- **Avoid submitting credit card information online** – Some companies offer a phone number you can use to provide your credit card information. Although this does not guarantee that the information will not be compromised, it eliminates the possibility that attackers will be able to hijack it during the submission process.
- **Devote one credit card to online purchases** – To minimize the potential damage of an attacker gaining access to your credit card information, consider opening a credit card account for use only online. Keep a minimum credit line on the account to limit the amount of charges an attacker can accumulate.
- **Avoid using debit cards for online purchases** – Credit cards usually offer some protection against identity theft and may limit the monetary amount you will be responsible for paying. Debit cards, however, do not offer that protection. Because the charges are immediately deducted from your account, an attacker who obtains your account information may empty your bank account before you even realize it.

Take advantage of options to limit exposure of private information – Default options on certain websites may be chosen for convenience, not for security. For example, avoid allowing a website to remember your password. If your password is stored, your profile and any account information you have provided on that site is readily available if an attacker gains access to your computer. Also, evaluate your settings on websites used for social networking. The nature of those sites is to share information, but you can restrict access to limit who can see what. (See Staying Safe on Social Network Sites for more information.)

Choosing and Protecting Passwords

Passwords are a common form of authentication and are often the only barrier between you and your personal information. There are several programs attackers can use to help guess or "crack" passwords. But if you choose good passwords and keep them confidential, you can make it more difficult for an unauthorized person to access your information.

Why you need strong passwords

Think about the number of personal identification numbers (PINs), passwords, or passphrases you use every day: getting money from the ATM or using your debit card in a store, logging on to your computer or email, or signing in to an online bank account. The list of things that you can do online gets longer every day. Keeping track of all of the number, letter, and word combinations may be frustrating at times, and maybe you've wondered if all of the fuss is worth it. After all, what attacker cares about your personal email account, right? Or why would someone bother with your bank account when there are others with much more money? Often, an attack is not specifically about your account but about using the access to your information to launch a larger attack. And while having someone gain access to your personal email might not seem like more than an inconvenience or embarrassment, think of the implications of an attacker gaining access to your Social Security number or your medical records.

One of the best ways to protect information or physical property is to ensure that only authorized people have access to it. Verifying that those requesting access are the people they claim to be is the next step. This authentication process is more important and more difficult in the cyber world. Passwords are the most common means of authentication, but if you don't choose good passwords and keep them confidential, they're almost as ineffective as not having any passwords at all. Many systems and services have been successfully breached because of insecure and inadequate passwords, and some viruses and worms have exploited systems when attackers were able to guess weak passwords.

How to choose good passwords

Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to crack them. Consider a four-digit PIN. Is yours a combination of the month, day, or year of your birthday? Or your address or phone number? Think about how easy it is to find someone's birthday or similar information. What about your email password—is it a word that can be found in the dictionary? If so, it may be susceptible to dictionary attacks, which attempt to guess passwords based on common words or phrases.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it. For example, instead of the password "hoops," use "IITpbb" for "[I] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Your best defense, though, is to use a combination of numbers, special characters, and both lowercase and capital letters. Changing the same example used above to "II!2pBb." creates a password very different from any dictionary word.

Longer passwords are more secure than shorter ones because there are more characters to guess, so consider using passphrases when you can. For example, "Passwd 4 miemale!" would be a strong password because it has many characters and includes lowercase and capital letters, numbers, and special characters. You may need to try different variations of a passphrase—some applications limit the length of passwords, and some do not accept spaces. Avoid common phrases, famous quotations, and song lyrics.

Don't assume that once you've developed a strong password you should use it for every system or program. If attackers do guess it, they would have access to all of your accounts. You should use these techniques to develop unique passwords for each of your accounts:

- Use different passwords on different systems and accounts.
- Don't use passwords that are based on personal information that can be easily accessed or guessed.
- Use a combination of capital and lowercase letters, numbers, and special characters.
- Don't use words that can be found in any dictionary of any language.
- Develop mnemonics such as passphrases for remembering complex passwords.
- Consider using a password manager program to keep track of your passwords. (See more information below.)

How to protect your passwords

Now that you've chosen a password that's difficult to guess, you have to make sure not to leave it someplace for people to find. Writing it down and leaving it in your desk, next to your computer, or, worse, taped to your computer, is just making it easy for someone who has physical access to your office. Don't tell anyone your passwords, and watch for attackers trying to trick you through phone calls or email messages requesting that you reveal your passwords. (See Avoiding Social Engineering and Phishing Attacks for more information.)

Programs called password managers offer the option to create randomly generated passwords for all of your accounts. You then access those strong passwords with a master password. If you use a password manager, remember to use a strong master password.

Other password problems stem from web browsers' ability to save your online sessions in memory. Depending on your web browsers' settings, anyone with access to your computer may be able to discover all of your passwords and gain access to your information. So, always remember to log out when you are using a public computer (at the library, an Internet cafe, or even a shared computer at your office). Avoid using public computers and public Wi-Fi to access sensitive accounts such as banking and email.

For more information on this multi-factor authentication and related password topics, see Supplementing Passwords.

Don’t forget security basics

- Keep your operating system, browser, and other software up to date.
- Use and maintain anti-virus software and a firewall. (See Understanding Anti-Virus Software and Understanding Firewalls.)
- Regularly scan your computer for spyware. (Some anti-virus programs incorporate spyware detection.)
- Use caution with email attachments and untrusted links.
- Watch for suspicious activity on your accounts.

There's no guarantee that these techniques will prevent an attacker from learning your password, but they will make it more difficult.

cyber@cansure.com

www.cansure.com

canSURE