Tips for Securing Your System

- Update Your Software
- Beware of Spyware and Adware
- Use Up-to-Date Antivirus Protection
- Use Strong Passwords
- Beware of Email Attachments
- Protect Against Social Engineering
- Avoid Peer-to-Peer Programs
- Establish a Firewall
    - Hardware Firewall
    - Software Firewall

Related articles:

Page:Tips for Creating a Secure Password

Page:Anti-Virus Software

Page:Information about What a Virus Is

Page:Securing your Flash Drive

Page:Tips for Securing Your System

Update Your Software

Many software manufacturers create and release updates that fix known security flaws. Most operating systems, including Windows 7, 8.1, and 10, are set by default to let users know when important updates become available for installation. As a computer owner, it is very important to install new updates as soon as possible in order to minimize the threat to the system.

Security and critical updates can also be installed on Windows automatically by turning automatic updates on. This functionality is included in the Windows Security Center, which is located in the Control Panel. You should never turn these off, as doing so will make your computer vulnerable.

Computer operating systems are not the only software that need updating. Web browsers such as Google Chrome and other applications such as iTunes and Adobe products need updating regularly as well. These applications will typically notify users when updates are available. Updates can also be found by accessing these manufacturers' web sites or by accessing the help menu in these programs.

Beware of Spyware and Adware

Spyware and Adware typically are programs that appear to be one thing, such as a weather watcher or screen saver, but are actually running background processes that track and report your Internet usage, create pop-ups and advertisements, and leave back doors for the spyware author to upload more software.

To keep your computer free of viruses and spyware, be sure to install an antivirus software. Like its name suggests, spyware can collect private information from your PC without your consent. Although not always as malicious as viruses, spyware can also redirect your browser activity and launch advertisements. To keep your computer running smoothly, and sensitive information such as credit card numbers safe, be sure to install and update your antivirus software. Keeping that software updated is one of the ways you can keep your PC immunized.

Exposure to spyware can be limited by following a few steps. First, don't install software if you do not trust the source. Second, always keep antivirus programs installed and up-to-date as some programs will catch spyware on installation. The final step in preventing unwanted spyware is to install, update, and run one or more antispyware programs such as: Spybot Search & Destroy, Lavasoft's Ad-Aware, and Windows Defender.

When dealing with attachments, keep these three points in mind to help keep your system secure:

- Never open unexpected attachments from a sender you don't know or trust.
- If an attachment from a trusted source is suspected as being malware, verify with the sender that the attachment is legitimate.
- Attachments that have an "executable" file extension, such as .exe, .java, and .vbs, should always be suspected as they pose a greater security risk. In fact, these types of files are blocked by default in the Missouri State email system; any attached file with one of these extensions will automatically be stripped from the email before delivery to help ensure campus security.

Use Up-to-Date Antivirus Protection

Main Article: Antivirus Software

Having a strong, up-to-date antivirus solution is arguably the most important thing that one can do to secure a computer. Antivirus (AV) protection is imperative to prevent attackers from uploading and running viruses, spyware, and other malware onto your computer.

Most AV programs are set by default to retrieve and install updates automatically. This is critical in maintaining a virus-free system, as new updates are created when new types of malware are found, and only up-to-date systems are capable of detecting new types of threats.

Microsoft Defender and Microsoft Security Essentials are two robust programs for Windows. Mac information will be forthcoming. In addition to this, AV programs such as Norton and McAfee can be purchased at the local technology store, or free AV programs such as Free AVG and Avast! Antivirus can be downloaded from their respective web sites.

Use Strong Passwords

Passwords are one of the primary security measures preventing hackers from accessing your account. Missouri State University enforces the use of strong passwords to help prevent others from breaking into your account. A strong password, as Missouri State defines it, is at least eight characters containing a combination of three of the following four rules: upper case letters, lower case letters, numbers and symbols. Campus passwords should never be shared with anyone else for any reason!

At any point, students, faculty, and staff can change their Active Directory passwords by navigating to https://cams.missouristate.edu . Missouri State University requires that domain passwords be changed every four months or the account will be disabled.

Beware of Email Attachments

One of the most common ways for worms and viruses to spread is through the use of email attachments. These malware programs often force the email program (Microsoft Outlook, Entourage, etc.) to send the malware attachment to everyone listed in that system's address book. This means that if a mail program is corrupted, a virus or worm can send itself to everyone in your address book without you knowing.

Protect Against Social Engineering

Social engineering is regularly employed by hackers in an attempt to gain your logon credentials and other important information through the simple method of asking for it. The use of social engineering methods, such as claiming to be a computer repairman, crafting an email that appears to be from your bank, or claiming that your PayPal account has been flagged and that you need to log in, is often referred to as phishing. To protect yourself from phishing, don't respond to spam email and absolutely never send your personal information in an email, even if you believe that the email you are responding to is legitimate. Banks, online auctions, and other E-Businesses will never ask for your personal information in an email or over the phone, so if you receive an email from eBay that asks for your password, report that email to the business' fraud prevention team.

Be wary against social engineering methods that attackers might use like sending an email requesting your username and password, rifling through the papers on your desk looking for your password on a sticky note, or calling you and claiming they are with Computer Services.

Avoid Peer-to-Peer Programs

Main Article: Peer to Peer File Sharing
Peer to peer file sharing programs, also known as P2P programs, are frequently used to violate copyright laws and may allow your personal information to be leaked through the programs file searching features. While there are many legitimate uses of Peer-to-Peer file-sharing clients, they have all the associated risks of downloading information from any server, along with a few of their own. Furthermore, use of P2P clients on the university network will trigger an excessive traffic violation, causing your network port to be shut down.

Establish a Firewall

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. A firewall protects your computer by regulating the flow of information between computers with different trust levels. Basically, it is used

to keep outside networks from entering your private network. To set up a firewall, you must first decide on what kind of firewall you need. Both Windows and Mac operating systems come pre-installed with software firewalls.

There are two different types of firewalls:

Hardware Firewall

- A firewall may be integrated into the router or DSL/cable modem supplied by your ISP
- A hardware router/firewall can be purchased from companies like LinkSys, Microsoft and D-Link.

Software Firewall

- Protect only one computer at a time.
- Can be customized

For questions or comments, contact the Computer Services Help Desk
HelpDesk@MissouriState.edu
417-836-5891