Security Tips

NEWSLETTER

ETS

MCC **EDUCATIONAL TECHNOLOGY SERVICES**

Communications and
Network Services

Cyber Security and You – Top Ten Tips

This month's theme is "Cyber Security is our Shared Responsibility" and that message has never been more appropriate. While there are many steps that people can take to be safe online, the following is a list of ten things you can do to secure your information.

1) **Passwords:** *Use strong passwords to secure your information. Passwords should have at least eight characters and include uppercase and lowercase letters, numerals and special characters. It is important to keep different passwords for different accounts. This will reduce the chances that if one password fails your other accounts will be vulnerable as well. Do not use the same passwords for accessing work systems on any other accounts.*

2) **Use of External Devices**: *Many organizations have policies that limit the use of external devices (computers or devices such as thumb drives, smartphones and mobile devices that are not the property of the organization). These policies are intended to protect the overall system, and we urge you to follow your organization's policies. As a home user it is important to be cautious about devices that don't belong to you that you let connect to your equipment, as you cannot be sure that they are properly protected.*

3) **Phishing and Social Engineering:** *Phishing is a tactic to obtain your personal data, such as credit card numbers, passwords, account data, or other information. The scam typically attempts to entice email recipients into clicking on a link or opening an attachment that results in malware being downloaded onto your computer. While it may be difficult to spot some phishing attempts it's important to be cautious about all communications you receive, including those purported to be from "trusted entities" and be careful when clicking on links or attachments contained within those messages. Additionally, do **not** respond to any unsolicited emails and do not open attachments contained in those messages.*

4) **Online transactions**: *Only shop at sites for companies you are familiar with and trust. When shopping online, look for the lock symbol or https in the website url to indicate the transactions are secure. Be wary of potential scams—if it sounds too good to be true, it probably is. Do not use a public computer or public wireless. Additionally you should make payments by using a credit card rather than a debit card, as credit cards are protected by the **Fair Credit Billing Act** and may reduce your liability if your information was used improperly.*

5) **Admin vs. Non-Admin accounts:** *Administrator or "Admin" accounts have more control over programs and settings for your computer. Hackers can potentially take control of your computer by accessing these accounts. Non-Administrator accounts, or guest accounts can still use programs, but limit the ability to make changes that hackers need to harm your computer. It is important to change the default password on your Admin accounts and to always run your computer as a non-administrator or non-admin unless otherwise needed.*

6) **Updating your systems and software:** It is important to keep your systems and software up-to-date. System and software vendors often find vulnerabilities that they fix in the latest update. If your computer is not updated, then you are leaving it open to attack via these vulnerabilities. Set programs and systems to auto-update to avoid missing a critical update. This includes your operating system, office suite, Adobe, media players, browsers, and other programs that can access the Internet.

7) **Protecting and securing mobile devices:** It is important to make sure you secure your portable devices to protect both the device and the information contained on the device. Establish a password and enable screen lock or auto lock on all devices. If your device has Bluetooth functionality and it's not used, check to be sure this setting is disabled. Some devices have Bluetooth-enabled by default. If the Bluetooth functionality is used, be sure to change the default password for connecting to a Bluetooth enabled device. Encrypt data and data transmissions whenever possible.

8) **Enable your firewall:** A firewall is a software program or hardware device that filters the inbound and outbound traffic between your network or computer and the Internet. A firewall is a very valuable tool to protect your data and your computers. Firewalls can block intruders and unwanted traffic from getting into your computer. Make sure your firewall is enabled.

9) **Using anti-virus and anti-spyware programs:** Anti-virus programs can stop viruses, worms, and other malware. Anti-spyware programs can stop malware that perform certain behaviors such as pop-up advertising, collecting personal information, or changing the configuration of your computer. It is important to keep these up-to-date by keeping the license active and the program set to auto-update.

10) **Securing wireless networks:** Wireless networks are not as secure as the traditional "wired" networks, but you can minimize the risk on your wireless network by enabling encryption, changing the default password, changing the Service Set Identifier (SSID) name (which is the name of your network) as well as turning off SSID broadcasting and using the MAC filtering feature, which allows you to designate and restrict which computers can connect to your wireless network.

As cyber security is our shared responsibility it is important that everyone keeps informed of the latest threats, and the best ways to stay safe online.

Resources for more information:

DHS Cyber Security
dhs.gov/files/cybersecurity.shtm

Multi-State Information Sharing and Analysis Center
www.msisac.org

National Cyber Security Alliance
Staysafeonline.org

 For more monthly cyber security newsletter tips, visit:
www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within

their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer.

Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by: