Top 10 Secure Computing Tips

Tip #1 - You are a target to hackers

We are all at risk and the stakes are high - to your personal and financial well-being.

- Keeping our computing resources secure is everyone's responsibility.
- By following the tips below and remaining vigilant, you are doing your part to protect yourself and others.

Tip #2 - Keep software up to date

Installing software updates for your operating system and programs is critical. Always install the latest security updates for your devices:

- Turn on Automatic Updates for your operating system.
- Use web browsers such as Chrome or Firefox that receive frequent, automatic security updates.
- Make sure to keep browser plug-ins (Flash, Java, etc.) up to date.

Tip #3 - Avoid Phishing scams - beware of suspicious emails and phone calls

Phishing scams are a constant threat - using various social engineering ploys, cyber-criminals will attempt to trick you into divulging personal information such as your login ID and password, banking or credit card information.

- Phishing scams can be carried out by phone, text, or through social networking sites - but most commonly by email.
- Be suspicious of any official-looking email message or phone call that asks for personal or financial information.

Tip #4 - Practice good password management

We all have too many passwords to manage - and it's easy to take short-cuts, like reusing the same password. A password management program can help you to maintain strong unique passwords for all of your accounts. These programs can generate strong passwords for you, enter credentials automatically, and remind you to update your passwords periodically. There are several online password management services that offer free versions.

Here are some general password tips to keep in mind:

- Use long passwords - 20 characters or more is recommended.
- Use a strong mix of characters, and never use the same password for multiple sites.
- Don't share your passwords and don't write them down.
- Update your passwords periodically, at least once every 6 months (90 days is better).
- Enable Multi-Factor Authentication for all accounts possible.
Tip #5 - Be careful what you click

Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically, and often silently, compromise your computer.

If attachments or links in the email are unexpected or suspicious for any reason, don't click on it.

Tip #6 - Never leave devices unattended

The physical security of your devices is just as important as their technical security.

- If you need to leave your laptop, phone, or tablet for any length of time - lock it up so no one else can use it.
- If you keep sensitive information on a flash drive or external hard drive, make sure to keep these locked as well.
- For desktop computers, shut-down the system when not in use - or lock your screen.

Tip #7 - Protect sensitive data

Be aware of sensitive data that you come into contact with, and associated restrictions - review the DOD Data Classification Standards to understand data protection level requirements. In general:

- Keep sensitive data (e.g., SSN's, credit card information, student records, health information, etc.) off of your workstation, laptop, or mobile devices.
- Securely remove sensitive data files from your system when they are no longer needed.
- Always use encryption when storing or transmitting sensitive data.

*If you suspect you have been sent classified material please contact cyber@westpoint.edu

Tip #8 - Use mobile devices safely

Considering how much we rely on our mobile devices, and how susceptible they are to attack, you'll want to make sure you are protected:

- Lock your device with a PIN or password - and never leave it unprotected in public.
- Only install apps from trusted sources.
- Keep your device’s operating system updated.
- Don’t click on links or attachments from unsolicited emails or texts.
- Avoid transmitting or storing personal information on the device.
- Most handheld devices are capable of employing data encryption - consult your device’s documentation for available options.
• Use Apple's Find my iPhone or the Android Device Manager tools to help prevent loss or theft.
• Backup your data.

Tip #9 - Update anti-virus protection

Keep virus definitions, engines and software up to date to ensure your anti-virus program remains effective.

Tip #10 - Back up your data

Back up regularly - if you are a victim of a security incident, the only guaranteed way to repair your computer is to erase and re-install the system. Contact our helpdesk and we can assist you.

https://usmakb.blackbelthelp.com/ or 877-326-8762

Here are some additional tips to help keep you safe and secure online:

Use public wireless hot-spots wisely (connect to a VPN before transmitting any personal data)

Be conscientious of what you plug into your computer (flash drives and even smartphones can contain malware).

Be careful of what you share on social networking sites.

Monitor your accounts for suspicious activity.

Bank or shop online only on trusted devices and networks - and logout of these sites and close the browser when you've completed your transactions.