Top 10 Secure Computing Tips

Tip #1 - You are a target to hackers

Don't ever say, "It won't happen to me." We are all at risk and the stakes are high - both for your personal and financial well-being and for the university's standing and reputation.

- Cybersecurity 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(link is external) 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.

Check out our Phishing Resources section for details about identifying phishing scams and protecting yourself.

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(link is external) 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.

Our Protecting Your Credentials how-to article contains detailed recommendations for keeping your password safe.

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 install (often silently) and compromise your computer.

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

ISO recommends using Click-to-Play(link is external) or NoScript(link is external), browser add-on features that prevent the automatic download of plug-in content (e.g., Java, Flash) and scripts that can harbor malicious code.

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 protected data on a flash drive or external hard drive, make sure their encrypted and locked up as well.
- For desktop computers, lock your screen or shut-down the system when not in use.

Tip #7 - Safeguard Protected Data

Be aware of Protected Data that you come into contact with and its associated restrictions. Review the UCB Data Classification Standard to understand data protection level requirements. In general:

- Keep high-level Protected 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.

Unsure of how to store or handle sensitive data? Email us at security@berkeley.edu(link sends e-mail).

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 (Apple AppStore, Google Play).
- Keep the device's operating system up-to-date.
- 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 (link is external) or the Android Device Manager (link is external) tools to help prevent loss or theft.

Tip #9 - Install antivirus/anti-malware protection

Only install these programs from a known and trusted source. Keep virus definitions, engines and software up-to-date to ensure your programs remains effective.

See our Minimum Security Standards Anti-Malware Software Guidelines for more information

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.

Reference: https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips