Ten Tips for Securing Your Data & Technology

Tue, 02/15/2022 - 11:11
|
Tulane IT Staff

View PDF

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 the security and confidentiality of your personal information 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 updated

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 and security software.
- 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

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

- 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.
- If you are suspicious of an email, always check that the sender name matches the sender email. Often times, only the name appears in the “From:” line, but if you click on that name you may see a suspicious email address that indicates it is a phishing email.
- Even if the sender is a known contact, if you are not expecting the email, text message, direct message, or phone call, you should verify the legitimacy of the communication before opening any attachments or clicking any links.

MORE INFO

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 manager can help you 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.

Some additional password-related tips to keep in mind:

- Always use complex passwords. Passphrases can be used to create passwords that are complex, yet easy to memorize (e.g., “Lets go Tulane Green Wave! Class of 2022” = “LgTGW!Co22”.
- Use multi-factor authentication wherever possible.
- Incorporate upper- and lower-case letters, numbers, and special characters.
- Do not include your name, initials, date of birth, or any other personal identifiers.
- Do not share your passwords with others or store your passwords in an unsecure manner (like a sticky note near or on your computer).
- Avoid using the same password for your work/school accounts, and any social media or banking accounts.

For more information, see the Tulane University Password Policy and Guidelines for Passwords for End Users.

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 an email are unexpected or suspicious for any reason, don't click on or open it.
- Don't click on links or attachments from unsolicited emails or texts.
- Be wary of false browser updates, which if clicked, may download malware to your device.

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 or see 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 shutdown 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. 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.
- Only use Tulane sponsored storage systems (such as Box or OneDrive).
- Ensure you have the appropriate settings (i.e., private vs public) applied to applications that maintain personal or Protected Data. Similarly, keep user lists current and remove users/members who no longer require access to certain information.
- Securely remove/delete sensitive data when it is no longer needed.
- Always use encryption when storing or transmitting sensitive data.
- Your Tulane email and calendar may contain protected data. Only delegate your email and calendar to the appropriate parties and check your share settings to ensure they are set to the correct view for each party. Learn more about Outlook's share settings.

Tip #8 - Use portable devices safely

Considering how much we rely on portable devices—such as cell phones, tablets, and laptops—and how susceptible they are to attack, you'll want to make sure you keep them protected and secure:

- Lock your device with a PIN or password—and never leave it unprotected in public. If leaving a mobile device in a vehicle (even if locked), you should store the device where it is not visible from outside the vehicle.
- Only install apps from trusted sources (Apple AppStore, Google Play).
- Limit what you do on public Wi-Fi networks, as such networks are not always secure and can allow hackers easy access to your sensitive information. Where possible, use a mobile hotspot instead.
- Keep the device's operating system, security software, and web browser up-to-date.
- 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.
- Before disposing of portable devices, perform a data reset or “hard reset” to bring the device back to factory settings and securely remove data.

For more information, see the Tulane University Mobile Device Security Policy.

Tip #9 - Install anti-virus/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 remain effective.

Tip #10 - Backup your data

Backup your data regularly. If you are a victim of a security incident that results in the loss of important information, the only guaranteed way to have access to the lost data is via a viable backup. By storing your data on Tulane’s Box and OneDrive, your data will already be backed up for you.