Cybersecurity Best Practices

MOBILE DEVICES, WORKSTATIONS, EMAIL, & SOCIAL NETWORKS

FBICYBER

As the cyber threat landscape constantly evolves, our nation's critical infrastructure and our internet-connected devices continue to face new cyber threats that can jeopardize the confidentiality, integrity, or availability of our information and cause lasting harm. The following security practices can help you better protect yourself from cyber threats.

Mobile Devices

Mobile devices allow us to access virtually every aspect of our lives from anywhere in the world. Because of this functionality, they are an ideal surface for exploitation. When using mobile devices, take the following precautions:

- **Do** enable a passcode or biometric lock.
- **Do** periodically review your applications and network sharing settings and reset them regularly to maximize security and privacy. Limit access to any stored personal data (e.g., your address book, photos, and financial information).
- **Do** update software in a timely manner and enable automatic updates, when available, and restart your device regularly.
- **Do** disable Bluetooth, Wi-Fi, near-field communication, and personal hotspots when not in use.
- **Do** enable remote wipe capability in the event a device is lost or stolen.
- **Don't** use public/unsecure Wi-Fi. If you must use unsecure Wi-Fi, use a virtual private network (VPN) service that starts upon initial connection.
- **Don't** use publicly available charging ports or stations to charge your mobile device. Only use your own wall chargers and USB cords. Electrical wall outlets should be the primary power source used in these environments.
- **Don't** download applications that are not cleared by the organization for enterprise devices.
- **Don't** "root" or "jailbreak" devices as this compromises the security architecture of the device.

Laptops and Computers

Laptop computers enable employees to access company systems and files when away from the office. When using laptops and computers, take the following precautions:

- **Do** adjust your browser and app data sharing settings to maximize your privacy and security. Periodically review the settings as they can revert to default after updates.
- **Do** keep your devices patched, ideally with automatic software updates. At a minimum, check and run anti-virus software weekly.
- **Do** change your router's default password and choose your network name carefully when setting up your home Wi-Fi. Use the strongest encryption protocol available.
- **Do** check device access for your router and disable unknown or old devices. Enable guest Wi-Fi and have guests or untrusted devices use that network segmented from your personal Wi-Fi.
- **Do** use a reputable cloud service that provides the appropriate balance of privacy, security, and cost for your needs.
- **Do** use a VPN to keep your communications and internet activity more private, especially when using public Wi-Fi.
- **Do** regularly back up and encrypt data.

Social Media

Threat actors will often scour all available information sources on a target for clues about the target's personal information, habits, and motivations. Social media is a great source for this information due to the nature of users' interaction with these platforms. Threat actors can use the personal data gathered from social media to put together possible account passwords, craft highly enticing phishing emails geared specifically to the target, or even create a detailed profile of the user's activities and movements where they might be vulnerable. Below are some tips to prevent social media profiles from revealing excessive information:

- **Do** ensure your profile is private and cannot be accessed by strangers with whom you do not have a connection.
- **Do** refrain from discussing information about the responsibilities and technologies that pertain to your role or any information that confirms your affiliation if your current position in your career requires you to handle sensitive information.
- **Don't** accept friend requests from individuals you don't know or haven't spoken with in a long time before verifying that the profile belongs to the actual person being represented. A quick phone call can allow you to validate that you are not accepting a request from a threat actor posing as a trusted friend.
- **Don't** post pictures with location information of a place you frequent at a consistent interval.
- **Don't** add hometown, birthday, or family names to social media profiles. This information is often used as part of security questions to verify your identity during unknown login attempts.
- **Don't** comment on pictures or posts that asks for security question relevant information (e.g., favorite superhero, first car make and model, middle/maiden name) as part of a social media "trend" should be ignored. These can be malicious social engineering attempts.

Email Precautions

- **Do** mark incoming emails from external companies. Only open emails that are trusted or plaintext only. Embedded HTML emails can redirect you to malicious websites.
- **Do** ensure that the information or content you share originates from a legitimate source.
- **Don't** open attachments or click on email links from senders you don't recognize. If the email came from a trusted source, verify you should have received the document or link before opening it.
- **Don't** provide your login credentials, financial data, or personal information in response to an email request. If the request appears to have come from a legitimate source, ignore the email link and navigate to the website directly through a browser.

General Security Guideline Quick Tips

- **Do** keep systems patched by installing software updates when they are available. Routinely restart your devices and turn them off when not in use. Restarting devices helps enable auto-updated patches.
- **Do** limit privileged user accounts. Use Admin accounts only when necessary.
- **Do** use network monitoring tools and regularly review feedback. Have an external/third-party security partner review and validate it, as well.
- **Do** develop, practice, and exercise system recovery plans. Have a near-, short-, and long-term recovery strategy.