United States Secret Service Cybercrime Investigations

Cyber Security Basics
How to Protect Yourself

The U.S. Secret Service recommends following these protective measures when using devices connected to the internet.

Account Passwords

- ✓ Change passwords regularly, and use different passwords for each system and account.
- ✓ Utilize multi-factor authentication for an added layer of login security, when available.
- ✓ Immediately change factory preset passwords on devices, to include Wi-Fi routers and smart devices.
- ✓ Use a secure password management app.
- ✓ For security questions use answers only you know.

Software and Apps

- ✓ Install operating system updates as soon as they are available for all devices.
- ✓ Install antivirus software and update antivirus definitions as soon as they are available.
- ✓ Install only trusted apps and update them regularly.
- ✓ Utilize enhanced social media privacy settings.

Online Activity and Transactions

- ✓ Update browsers as soon as they are available on all devices.
- ✓ Use reputable and legitimate websites.
- ✓ Be mindful of posting personal information on social media.
- ✓ Ensure websites are encrypted, look for *https* and the 🔒 icon on the address line.
- ✓ Do not ignore certificate error notifications.
- ✓ Always verify website addresses by manually typing them, or access websites from internet searches.
- ✓ Use WPA2 or WPA3 security for wireless networks.
- ✓ Do not broadcast your wireless name - Service Set Identifier (SSID).

Social Engineering: Phishing and Smishing

- ✓ Never respond to an email or text message from an unknown source.
- ✓ Never click on a link or open an attachment from an unknown source.
- ✓ Never respond “Stop” or “No” to prevent future text messages, delete the text instead.
- ✓ Never share your financial or personally identifiable information (PII).
- ✓ Always read the entire email and look out for suspicious indicators, such as poor grammar or email addresses disguised to appear legitimate.
- ✓ Always independently verify where a request for sensitive information originates.
- ✓ Always independently type a website address instead of clicking on a link.
- ✓ Always delete a text message from an unknown source.
- ✓ Always mark an email from unknown source as spam.

Mobile and Smart Devices

- ✓ Enable screen lock and device encryption.
- ✓ Use biometric authentication.
- ✓ Turn off geolocation features.
- ✓ Disable Wi-Fi and Bluetooth.
- ✓ Disable AirDrop on Apple devices.
- ✓ Configure devices to automatically update or update them as soon as available.
- ✓ Enable the find my device feature.
- ✓ Consider whether constant internet connectivity is necessary for smart devices.

Connectivity While Traveling

- ✓ Avoid connecting to public Wi-Fi, but if using public Wi-Fi do not transmit any sensitive information or PII.
- ✓ Avoid public charging stations when possible.
- ✓ Use a commercially available Virtual Private Network (VPN) for your devices.
- ✓ Do not connect (Bluetooth, Wi-Fi) or plug phones (USB) into rental vehicles.
- ✓ Use datablocker plugs to charge your devices when necessary.

Contact your service providers for assistance.

Contact your local law enforcement agency if you suspect criminal activity.

www.secretservice.gov/investigation