Tips to Safeguard Your Online Privacy and Cybersecurity

Community Protection Division Boulder County District Attorney's Office



Safeguard your personal identifying information (PII)



- PII is essentially any information that could be used to identify you.
- PII includes your name, address, date of birth, social security number, financial account number, and email address.
- PII could also include more indirect. information, like your location or product preferences.
- Cybercriminals, as well as many businesses, value your PII like money, and therefore, so should you.

Update the privacy and security settings for your online accounts and devices



For direct links to instructions, visit the National Cyber Security Alliance's Stay Safe Online site: https://staysafeonline.org/stay-safeonline/managing-yourprivacy/manage-privacy-settings/



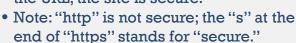
Use complex, unique passwords for all accounts, plus 2-factor authentication (2FA)



- A complex password is hard to guess: at least 12 characters, not a common dictionary word, includes uppercase and lowercase letters, numbers, and special characters.
- A unique password is one that is not used for multiple accounts (for example, for both your email and your online banking accounts).
 - This helps prevent the breach of one account leading to breaches of others.
- For extra protection, enable 2FA. After you enter your password, a one-time passcode is sent to your phone and you cannot access the account until you enter the passcode as well.
 - With 2FA, even if someone has your password, they can't access your account unless they also have your cell phone.
 - For instructions for enabling 2FA, visit the Stop Think Connect site: https://stopthinkconnect.org/campaign s/lock-down-your-login

Only use websites secured by encryption

 Check your web browser's address bar-- if you see a closed padlock symbol or "https" at the beginning of the URL, the site is secure.



Michael Dougherty, District Attorney BOULDER OFFICE: JUSTICE CENTER · 1777 6TH STREET · BOULDER, COLORADO 80302 · 303.441.3700

LONGMONT OFFICE: 1035 KIMBARK · LONGMONT, COLORADO 80501 · 303.441.3700 WWW.BOULDERCOUNTYDA.ORG · EMAIL: BOULDER.DA@BOULDERCOUNTY.ORG · TDD/V: 303.441.4774

Tips to Safeguard Your Online Privacy and Cybersecurity

Community Protection Division Boulder County District Attorney's Office



Keep software updated



- Most software (such as for your operating system, web browsers, apps, and cybersecurity) can be configured to update automatically.
 - Install these updates as soon as possible to minimize the time cybercriminals have to exploit the software's weakness.

Secure your home Wi-Fi network

Your home's Wi-Fi router is the primary way cybercriminals may try to access the data that flows through your home's computer and other internet-connected devices.

- Change your router's default administrative password (which is different than the Wi-Fi network password), since the default passwords are often the same across brands and are easily obtainable.
 - Change the Wi-Fi network's default name (also called a SSID), since the default name could indicate which router you have.
 - Do not choose a network name that indicates your name, address, or other indication of where the network is based.
 - Turn on your router's encryption. When setting it up, choose WPA3 if available, otherwise choose WPA2-
 - Turn off any "remote management" features.
 - Disable any quest networks that don't have a password.

Avoid public Wi-Fi networks





Google Android hotspot

instructions: https://support.google.com/android/ans wer/9059108?hl=en

Protect your video conferences

As use of video conferencing apps has surged, so have instances of uninvited cybercriminals joining in to steal information, send malicious links/files, or harass invited participants.

 Create and use a unique meeting ID number for each meeting (don't use one that the app assigned to you).



- Do not share the meeting ID number or password publicly (for example, on social media). Instead, provide them privately via email.
- Configure the settings so that nobody can join until after the host.
- Enable the "waiting room" feature--it allows the host to see who is attempting to join and decide whether to let them in.
- Once the invited participants have joined, lock the meeting to keep others out.
- Restrict file sharing so that any unwanted quests cannot send or receive files via the chat feature. Instead, send files to the group by email.