west protect℠

SAFE
Security Awareness For Everyone

Tip Sheet


Your online activity collects a large amount of data about you that you might not realize. Ranging from your interests and purchases, where you go and spend time, to your online behaviors, and is collected by websites, apps, devices, services, and companies all around the globe. Even including information about your physical self, like health data – think about how an app on your phone might count how many steps you take.

**YOU CAN'T ALWAYS CONTROL HOW EACH BIT OF DATA IS COLLECTED, BUT YOU STILL HAVE A RIGHT TO DATA PRIVACY. YOUR DATA IS YOURS, AND YOU CAN HELP MANAGE YOUR DATA WITH THE FOLLOWING REPEATABLE TIPS.**

**DON'T CLICK THAT LINK** - in emails, texts, or documents. Instead, type the URL you want directly into the browser. ***Why?*** Phishing is still the number one favorite method of cyber-attacks.

**USE TWO-FACTOR AUTHENTICATION** for logging into your accounts. ***Why?*** With that second authentication piece in place, you are much less likely to lose personal data due to phishing.

**DELETE YOUR RECORDED CONVERSATIONS** - Regularly delete any recorded conversations used by your "personal assistant." ***Why?*** There have been cases where Alexa revealed personal data to unknown persons without consent.

**KEEP IT CLEAN** - delete old files you don't use/need to make sure you keep data replication to a minimum. ***Why?*** There can never be 100% security, but reducing the places that can be compromised helps lessen your risk.

**TRY TO BE LESS SOCIAL** by minimizing the personal data you enter on social media platforms. ***Why?*** Information like your mother's maiden name or other personal information is sometimes used to recover account logins.

**DON'T SYNC DATA JUST BECAUSE THEY ASK** - disable automatic file and media sharing whenever possible? ***Why?*** Many devices set up cloud syncing when first configuring the device. Think twice and make sure you want to store that data in the cloud.

**KEEP OFF THE BEATEN TRACK** - Disable location tracking on each app. ***Why?*** A recent study of almost 1 million Android phones demonstrated that apps regularly harvested tracking data.

**LET SLEEPING BLUETOOTH LIE** - If you are not using Bluetooth, switch it off. ***Why?*** Bluetooth vulnerabilities can allow data to be siphoned off your device.

**ENCRYPT STORED DATA** - Encrypt any data you store on hard drives and use an email encryption tool if you share personal data. ***Why?*** Encryption is a layer of protection that can prevent lost or stolen data from being exposed.

**PATCH YOUR DEVICES** - Keep your computers and mobile devices patched and up to date. ***Why?*** Software vulnerabilities allow malware to infect your devices, stealing data and login credentials.