10 A USER'S GUIDE: WAYS TO PROTECT YOUR PERSONAL DATA

1 Don't click that link!

What to do: Don't click untrusted links in emails. Instead, type the URL you want directly into the browser.

Why: According to Microsoft, phishing is still the number one favorite method of cyber-attacks.

2 Use two-factor authentication

What to do: Use a second factor for logging into accounts.

Why: If you have a robust two or multi-factor in place, you are much less likely to lose personal data due to phishing.

3 Delete recorded conversations

What to do: 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.

4 Keep it clean — delete old files

What to do: Make sure you keep data replication to a minimum. Delete old files you don't use.

Why: There can never be 100% security, but reducing the places that can be compromised helps lessen your risk.

5 Be less social

What to do: Minimize the amount of personal data you have on social media platforms.

Why: Information like your pet's name or mother's maiden name is sometimes used to recover account logins. Don't give hackers an easy way into your online accounts!

6 Don't sync for sync's sake

What to do: Disable automatic file and media sharing whenever possible.

Why: A lot of devices set up cloud syncing when you first configure the device. Check if you really want to store these data in the cloud.

7 Keep off the beaten track

What to do: Disable location tracking on each app.

Why: A recent study of almost 1 million Android phones demonstrated that apps regularly harvested tracking data.

8 Let sleeping Bluetooth lie

What to do: If you are not using Bluetooth, switch it off.

Why: Bluetooth vulnerabilities can allow data to be siphoned off your device.

9 Encrypt stored data

What to do: 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.

10 Patch your devices

What to do: Keep your computers and mobile devices patched and up to date.

Why: Software vulnerabilities allow malware to infect your device, which can steal data and login credentials.