Digital Health Checkup

It's likely that at this very moment, some entity somewhere is collecting and storing your personal information. Even though data collectors are subject to multiple laws that are designed to protect your privacy, you can still take matters into your own hands. Here's a quick questionnaire to help you maintain your digital well-being.

Have you reviewed privacy settings for social media accounts?

Social media platforms have a long history of questionable data-collection practices. You can control certain aspects of your privacy by taking the following actions:

- □ Disable location tracking services
- □ Remove permissions from all apps, games, websites, and business pages
- □ Don't allow the platform to connect to other apps or services
- □ Set your profile to private and only friend people you know and trust

Do you know how to spot common online scams?

Train yourself to identify when you're being targeted by staying alert, thinking before you click, and treating all requests for information or money with skepticism. Here are a few common online scams to watch out for:

- □ The one where a pop up claims your computer has been infected
- □ The one where you're offered a large sum of money for an upfront payment
- □ The one where a service or entity asks for payment via gift cards
- □ The one where an email claims an account has been disabled due to fraudulent activity

Did you allow mobile applications to have extended permissions?

Not only do scammers create malicious applications and upload them to popular app stores, many legitimate applications tend to collect excessive amounts of personal data. Always question why an app needs:

- □ Access to your camera or microphone
- □ Access to your contacts
- □ Access to your location
- □ Access to your text messages

Generally speaking, if the permissions granted to the app are not necessary for functionality (especially if it's a function you don't intend to use), block them.

SAC the security awareness™ COMPANY