CYBERSECURITY AWARENESS MONTH

10 Ways to Protect Yourself

1

Use strong and unique passwords

and use a password manager (such as 1Password or Bitwarden, though not official recommendations). They'll notify you if one of your passwords was exposed in a data breach and needs to be changed.

2

Enable Multi-Factor Authentication (MFA)

wherever possible (especially on your bank, healthcare and social media accounts). Passkeys or phishing-resistant types are the best, but any type of MFA is better than none!

3

Set all social media accounts to private

and be careful about what you post.

4

Ignore unknown calls and texts.

If it's someone you know—verify that is really your trusted contact. If you're not expecting a call or text do not respond—hang up and call the institution directly.

5

Be aware of refund scams.

If someone "accidentally" sends you money via a payment app, open a case with customer support—do not refund the money yourself.

6

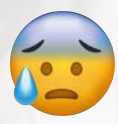
Freeze your credit (USA only)

with each of the three main bureaus so no one can open accounts in your name without confirming with you on the phone.

7

If someone is trying to entice you, scare you,

or pressure you, it is a red flag. If something seems too good to be true, it probably is!



8

Be careful using public WiFi.

It is easy for a bad actor to set up a similarly-named network and monitor all your web traffic.

9

Back up any data you would be upset to lose

in at least two locations. Use a cloud backup service as well as an external hard drive stored in a secure location.

10

Keep your apps and devices up to date!

Download updates as soon as they're issued.

paloalto® NETWORKS