TIPS TO PROTECT YOURSELF

Think before you click!

Always be suspicious of email, texts and messaging from senders you don't know especially those that include links and attachments.

Complex Password and don't re-use

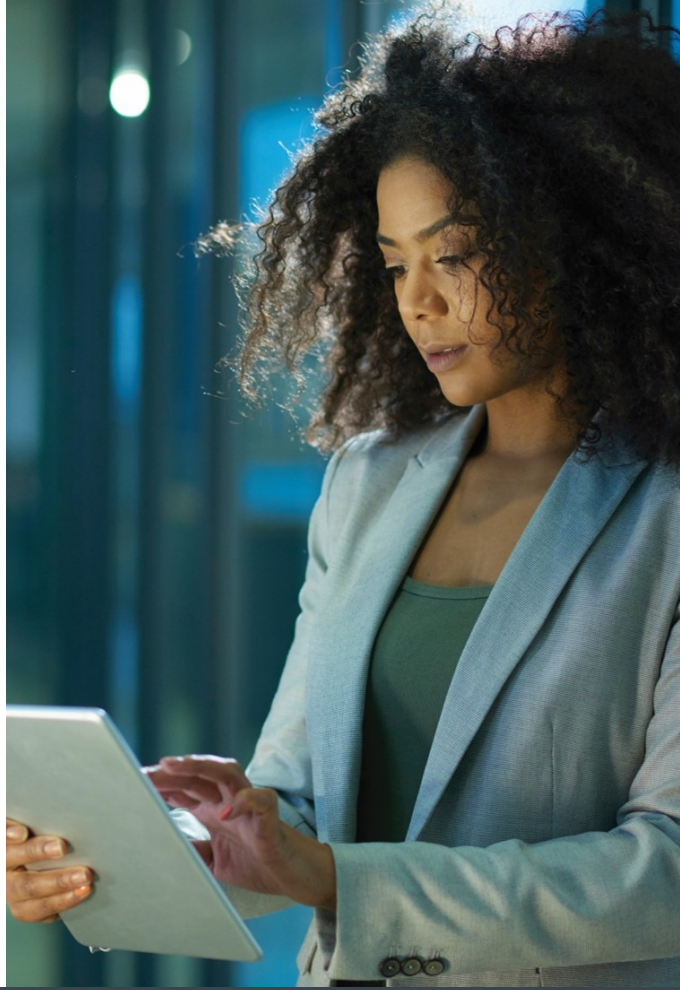
Password123 is NOT OK. Use different passwords for different sites. Use a password manager for safe keeping of passwords

Practice Digital Hygiene

Anti-virus is NOT dead! Auto-update your anti-virus protection and update Windows and Mac as soon as updates are released.

And, of course, use Identity Theft Protection service!

Leverage an identity theft protection service to watch your back 24x7.



WHAT YOU CAN DO

Office Files

Verify that your PII needs to be stored

Ask how your PII is used and stored

Use *Identity Theft Protection Services* and *Bureau Freeze* options

Phone Phishing

Always use the published call-back number for your institution

Never answer log-in questions for inbound callers; *always* call back

Verify any account related issue via email or portal log-in

Public Wifi

Limit what you share

Use personal VPN products

Don't conduct transactions

Online Shopping

Make sure your connection is secure

Make sure you are on a secure website

Don't store info with online sites

Use complex passwords or a password manager

Social

Manage privacy settings

Use complex passwords

Be aware of geo-tagging

Assistant/IoT

Use device security

Enable lost phone functions

Be aware of geo-tagging

Disable wifi and bluetooth when not in use

Mute microphone when not in use

Understand Risk and Security

Trusted resource: https://otalliance.org/