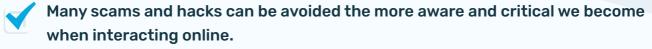


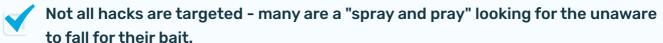




Awareness









Phishing & Ransomware

- Does a message make you feel excited? Nervous? Pressured? STOP! Pause and think before you click a link or download a file.
- To verify you are messaging the right person, give them a quick call.
- Manually type in a domain URL for a trusted website instead of clicking on an email link to avoid phishing links.
- Staying on the lookout for phishing attacks can help prevent ransomware being installed on a device.
- Don't automatically trust messages from co-workers, service providers or even family just because you recognize the sender name.
- Friends and family accounts may be hacked and used to send malicious links or files to their contact list.
- Keep computer and smart devices updated regularly to have the latest security patches!
- Enable two-factor authentication for emails, social media and other apps.
- If two-factor authentication is not turned on and your account gets hacked, the criminal can enable the 2FA making it harder to get the account back.
- Checking for spelling mistakes is not enough to prevent phishing. Call the sender on a trusted number to verify the email came from them.

Password Safety & Multi-Factor Authentication (MFA)



Using the same password for different accounts puts all of them at risk if the password is leaked.

A password alone is not enough to secure your online accounts.

Multi-factor authentication (MFA) can protect your account even if your password has been hacked as criminals do not have the second code generated by your Authenticator app.

MFA is off by default. Turn it on under Settings -> Privacy (or Security)

Authenticator Apps are more secure than text-based (SMS) for 2FA options.

Never share a verification code with anyone.

Policies & Procedures

When verifying sensitive requests don't trust the contact info listed in the email signature.

Always verify a change request through established protocol.

Only use listed contact information for phone and email from your company's vendor management system.

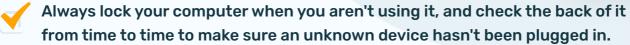
Check with the IT team on the apps / tools you want to use as they may have a more secure alternative.

Don't bypass security for the sake of productivity.











If your device is stolen, immediately change passwords for all your accounts.

Don't leave your computer physically accessible in the hotel room when travelling.

Install apps directly from the company's official site instead of searching through the app store.

Beware of lookalike apps in the App Store - not all are legitimate even if they 'look' official.

Widgets and apps don't need permissions to everything they ask to access.

For public WiFi, ask the business hosting the WiFi for the exact WiFi name.

Avoid sensitive work and personal business such as banking, credit card, or bill paying when using public WiFi.

Data Management

Go above and beyond to verify any request to change bank info and contact details no matter who it comes from or who it is for (vendor, employee, partners, etc)

For sensitive information or data that is regulated, only use approved encrypted messaging tools and processes.





- It's easy to be distracted when working on-the-go via the mobile phone. Wait to deal with highly sensitive data when you're focused and alert on a secure work device.
- Encrypt sensitive data and NEVER keep passwords in a text file or spreadsheet.
- Avoid putting personal data on a portable device such as a USB.
- Sensitive documents should not be left around the office. Instead, make sure to store them in a secure location.
- Retrieve documents with sensitive information immediately and destroy them when no longer needed.
- Don't paste a client's personal information to the body of an email unless it's approved and encrypted.
- Call the recipient before sending the information through a verified number to ensure you have the correct address.
- Keep an offline backup of your data as a last resort.

