

COMPUTER TIPS

Take Control of Your Email

Avoid opening unexpected email attachments no matter who appears to have sent it. Attackers spoof a sender's name to fool people into opening attachments that collect their personal information and forward it to the attacker. If someone asks you for money, double check with the sender and do not send credit card information over the email.

Use Strong Passwords / Hide Them Well

Use a variety of letters, numbers, and special characters — the longer and more complicated the better. Use different passwords for each account. If an account supports it, use two-factor authentication.

Most people know others do not remember their passwords and will therefore put the information on a slip of paper by the computer. Don't do this – hide your passwords somewhere that can and is usually locked.

Keep Abreast of Internet Scams/ Don't Fall Victim to Virus Hoaxes

Don't open or click on links in emails that tell sad stories, make unsolicited job offers, or promise lotto winnings. Also, beware of emails that masquerade as security concerns from your bank or another eCommerce site. These emails may contain links to malicious content.

If you're not sure if an email from your bank or credit card company is legitimate, contact them directly. (Do not use the information from the email to contact them, look it up independently.)

Watch for Shoulder Surfing

This is the method employed by passersby watching what you are doing while using a computer -- like typing in usernames and passwords. Always take a second to glance around briefly before typing in any personal information.

Using Public Computers

Sometimes you will need to access private information (bank accounts, etc) on a public computer. When you do so, make sure to a) disable, reject or delete cookies/history; b) never save your password or click "remember me"; c) use browser privacy mode and always close the browser when finished; d) use only sites with "https" and have the lock logo in the url; and e) remember to pick up any prints you made.

***If you think your password has been compromised, change it.
If you think your personal information has been compromised, report it.***