Oak Bank

You can't be the best,
if you're only the same!

SECURITY UPDATE - OCTOBER 2021

It's Cybersecurity Awareness Month!

Cybercriminals are always finding new ways to steal your personal information – so we take cybersecurity very seriously. This year's Cybersecurity Awareness Month theme is #DoYourPart #BeCyberSmart. Being cyber smart means using these tips to safeguard your data, information and money from being stolen.

So, how do you protect yourself?

ANTI-VIRUS SOFTWARE

Your computer should be protected by anti-virus software. When you install the software on your computers and devices, you should also make sure that the virus definition files are up to date. Ideally, you should set up an automated full system scan to run regularly.

BACKUPS

Data can be compromised in a variety of ways: by hackers, viruses, malware, hard drive failures, natural disasters or simply deleting a file. Backing up your files regularly ensures you can access your important information anywhere, anytime.

MULTI-FACTOR AUTHENTICATION

The use of multi-factor authentication (MFA) provides another layer of security in addition to stronger and longer passwords. Your MFA will make it difficult for hackers to gain access to your accounts because they'll have to pass an extra step of authentication like a verification code sent to your email address. If you use a password manager, it likely has an option to enable multi-factor authentication for your login.

PASSWORDS

The longer and more complex your password the better. Remember NOT to use dictionary words, kids' names, pet names, etc. Don't use the same password across all of your accounts. You can use a secure password manager to store your passwords. Many of these encrypted tools will also let you know if your password has been compromised.

PHISHING EMAILS

Online fraud occurs when someone poses as a legitimate company to obtain sensitive personal data and illegally conducts transactions on your existing accounts. Often known as "phishing" or "spoofing," the most current methods of online fraud are fake emails, websites and pop-up windows, or any combination of these. A good rule of thumb when you are questioning an email is, "When in doubt, throw it out." It is best to pick up the phone and call the company directly and don't click on any links in the email or open any attachments.

UPDATES & PATCHES

Keep your work computer, home computer, laptops, tablets, smartphones and other web-enabled gadgets up to date. Updates and patches fix problems in the software and patch security holes that a hacker could use to gain access to your system or data.

The Equifax breach was due to a critical patch not getting installed. Applying updates and patches as soon as you can after they are released can minimize your risk.

IDENTITY THEFT PROTECTION

Not only are criminals looking for money transfers, they also want your personal information.

There are many safeguards you can utilize to protect yourself from identity theft. Here are just a few of them:

- Don't give anyone your private information over the phone unless you can verify who they are (e.g. call them back on a publicly available line) or online unless it's from a reputable website and you have a secure connection.

- Be careful of what you post on social media and public forums. Don't post TOO much personal information.

- While public Wi-Fi might be free for you, it's also free for criminals to use. Be cautious of what applications you are using when using public or free Wi-Fi. You should not fill out any personal, confidential or sensitive data while accessing a public connection.

- Check your credit report annually and check your bank accounts often. Identity thieves will often start with small amounts and build up to larger transactions. In the event, your credit card information is stolen, place a fraud alert at all three credit bureaus to help protect your credit score.

- Shred all confidential documents before disposing of them.

- Be cautious whenever and wherever you are online. Remember to think before you click.

GOOD BROWSING HABITS

It might only be October, but many people are getting ready for the holiday season.

Before you start shopping, here are a few things to remember:

- Stick to legitimate websites (i.e. only shop online with companies that you know).

- Check the website URL for typos or misspelled words.

- Type the store's URL into your web browser yourself instead of using a link from an email.

- Use HTTPS: - Look for the "S" or a padlock on the address bar before entering your personal or credit card information.

- Don't save website passwords.

- Turn on your browser's pop-up blocker.

*For more information and resources about cybersecurity, click **here**!*

*For additional security information you can visit **Oak Bank's Security Page** on our website.*