Oak Bank

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

SECURITY UPDATE - OCTOBER 2020

October is Cyber Security Awareness Month

Oak Bank takes cyber security seriously. We want to help you limit your risk and protect yourself, your family, your company and your money. Cyber criminals try to access your money, computers and identity using e-mail, ATM/gas pump skimmers, dumpster diving, telephone impersonation, physical impersonation, corporate security breaches, web browsing and social media. These tactics are tricky to identify and can lead to unwanted time spent trying to retrieve funds while keeping your personal information safe..

So, how do you protect yourself?

ANTIVIRUS

You should have antivirus software on your computer. Along with installing the software on your computers and devices, you need to make sure you are updating the virus definition files. Ideally you should set a full system scan to run automatically on a regular basis.

BACKUPS

Many things can compromise your data on your computer. Hackers, viruses, malware, hard drive failure, natural disasters, and even something as simple as accidentally deleting a file, could have an impact on your business and your money. If you don't backup your data, it could be lost. Make sure your data is properly backed up and then test it to make sure you can get your files back.

PASSWORDS

Passwords are your first line of defense. The longer and more complex, the better. Remember NOT to use dictionary words, kid's names, pet names, team names, etc. In a recent hacker demo, passwords like Summer2017, Augu$t2017, 04Packers and variations of the company name are the first ones hackers try. Don't use the same password on all of your accounts. Hackers know if they can break into your social media account, you probably use that same password for some other critical accounts.

PHISHING EMAILS

A good rule of thumb when you are questioning an email is "When in doubt, throw it out." According to dictionary.com, phishing is defined as "trying to obtain financial or other confidential information from internet users, typically by sending an email that looks as if it is from a legitimate organization, but contains a link to a fake website that replicates the real one." If you are in doubt, pick up the phone and call the company directly. Don't click on any links in the email or open any attachments.

UPDATES & PATCHES

Keep your work computer, home computer, laptops, tablets, smart phones 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 or online unless you can verify who they are, or if it's from a reputable website.
- Be careful of what you post on social media and public forums. Share with care. 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 use when using public or free Wi-Fi. You should not transmit any personal, confidential or sensitive data while accessing a public connection.
- Check your credit report annually for free. Everyone should watch their accounts. Identity thieves will start with small amounts and build up to larger transactions. If your credit card information is stolen, place a fraud alert on all three reporting agencies to help protect yourself from a damaged credit score.
- Shred all confidential documents.
- Be cautious whenever and wherever you are online. Remember to think before you click.

GOOD BROWSING HABITS

It might be only October, but many stores and online vendors 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.
- Don't click on online advertisements.
- Type the store's URL into the web browser yourself instead of using a link from an email.
- Use HTTPS: - Look for the "S" or a padlock on the address bar when entering your personal or sensitive information.
- Don't save website passwords.
- Turn on your browser's pop-up blocker.

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