[View as Webpage]

October is National Cyber Security Month

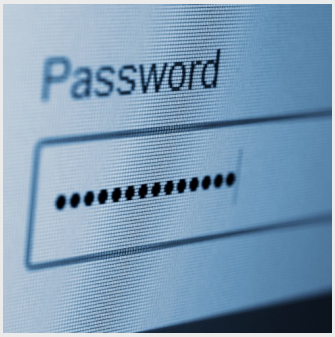
2023 marks the 20th anniversary of National Cybersecurity Month! In this digital age, knowledge of important cybersecurity tips are crucial to protecting your personal information on your devices. **The National Institute of Standards and Technology** (NIST) has selected four general themes for this year's Cybersecurity Month that will help keep your data safe from malicious intent. Continue reading below to learn more!

Enabling Multi-Factor Authentication

The use of multi-factor authentication (MFA) provides an extra layer of security. Even if hackers know your password, MFA requires them to take an extra step to gain access to your account. Some examples of MFAs include:

- Answering a security question.
- Receiving a code via text message or email.
- Using facial recognition or fingerprint entry.
- Entering a PIN.

For more information on MFAs, **click here**.



Using Strong Passwords (And a Password Manager!)

The National Cybersecurity Institute **shares three key components** of a good password. They should be long, unique and complex. Passwords should be over 12 characters long and contain special symbols and a combination of upper and lowercase letters. Steer clear of easy-to-identify passwords, such as children's or pet's names. Additionally, you should **never** repeat passwords. Each should be unique from other accounts for the highest level of safety. With so many passwords, how can you keep them organized? Using a password manager will keep them all in one convenient location hidden behind a master password. Learn more about password managers **here**.

Perform Regular Software Updates

Software and app developers are constantly monitoring the latest trends in hackers to keep their programs safe from criminals. You should consistently check for and take

advantage of any new updates to ensure you're getting the most up-to-date protection.

Many programs and apps will have the option to set up automatic updates so they'll be downloaded as they become available. Continue reading **here** for more tips and to browse a list of common software updates.

Spot and Report Phishing Attempts

Learn how to recognize the signs so you don't get hooked in a phishing attempt! Phishing occurs when criminals attempt to steal your information by posing as a legitimate institution. This is usually done through email, text message or social media. Some of the common red flags of phishing attempts are long, complicated email addresses, threatening or urgent language, and poor grammar or misspellings. **Continue reading** for additional signs of phishing, and information on how to block and report phishing attempts.

For additional security information, you can visitOak Bank's Security Information on our website.

Need help with your account?

Email: bank@oak.bank
Call: 608.441.6000

If your Oak Bank Debit/ATM Card has been misplaced, call 800.472.3272.

If you have misplaced your Oak Bank Visa Credit Card, call 800.423.7503.

VISIT OAK BANK ONLINE

608.441.6000
877.625.2265 Toll Free

Lobby
M - F: 8 a.m. - 5 p.m.

Drive-up
M - F: 8 a.m. - 5 p.m.

Member FDIC

Oak Bank NMLS #434669