# October is National Cybersecurity Awareness Month
Let's take steps to *secure our world*.

Cybersecurity Awareness Month is an international initiative that educates everyone about online safety. It seeks to empower individuals and businesses to protect their data from cybercrime. Please read the messages below and learn simple and effective ways to keep yourself safe online, protect your personal data, and ultimately **secure our world**.
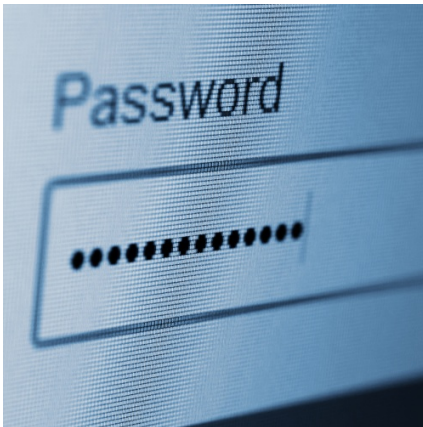
Using Strong Passwords (And a Password Manager!)

The National Cybersecurity Alliance outlines **three key components** of a good password. Passwords should be over 12 characters long and contain a combination of special symbols, numbers, uppercase letters 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**.

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**.

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 visit the **National Cybersecurity Alliance "Online Safety Basics"** and visit **Oak 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 877.755.2957

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.

Oak Bank | 5951 McKee Road | Fitchburg, WI 53719 US