Oak Bank

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

SECURITY UPDATE - JULY 2022

Ransomware: Understanding the Ins and Outs.

Did you know that by 2031, ransomware will attack a business, a consumer or an electronic device every two seconds?

Ransomware is a type of malware that locks electronic devices or files on your electronic device until a ransom is paid. Hackers use ransomware to steal organizations' sensitive and important information, like user data. They threaten to release private information unless they are paid a ransom. Cybercriminals prey on human error by using sophisticated social engineering techniques (e.g., phishing) to trick employees and consumers and bypass security defenses.

How does ransomware get on your devices?

When you visit a malicious website or download an attachment from a spammed email, you can download ransomware onto your device. This can happen when you click on a link, especially shortened ones, or an unknown or corrupt QR codes.

When this happens, ransomware can encrypt your electronic device, restricting access to files and spreadsheets. Typically, an image appears on your screen with instructions regarding how to pay the ransom.

As reported by Cybersecurity Ventures, ransomware damage costs in 2015 were $325 million. The amount increased to $20 billion in 2021; by 2031, it's projected to exceed $265 billion.

As ransomware attacks increase, institutions, employees and everyday users need to raise awareness and protect themselves against fraud and phishing.

How to protect yourself and organization from ransomware:

1. Educate yourself and if you own a business, your employees, about safe practices and how to recognize warning signs for different phishing emails.
2. Make sure that you have an anti-malware solution in place on your personal device and, if you own a business, at your company. This software should be updated regularly.
3. Ensure that only authorized users can access sensitive information and that passwords are secure.
4. Back up your data. Once your information has been compromised, cybercriminals may prevent you from accessing it. You should save the data in an alternate location, such as on a hard drive.
5. Contact the FBI if you are attacked.

Maintaining a high level of protection against ransomware is a continuous process. Make sure you are always up to date on risks and prepared for attacks.

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