TREMONT FIRST NATIONAL BANK
TREMONT • HOPEDALE • NEW HOLLAND

You have to experience it!

Cybersecurity Tip of the Week- 4/09/2020

FBI Warns of Increase in COVID-19 Related Cybersecurity Attacks

The Federal Bureau of Investigation (FBI) issued an alert this week regarding Business Email Compromise (BEC) attacks. Opportunistic cyber attackers are using the disruption surrounding COVID-19 to perform these and other types of attacks.

Business Email Compromise

BEC is a scam that targets individuals and businesses sending wire transfers, checks, and automated clearing house (ACH) transfers. In a typical BEC scheme, the attacker sends an email that is designed to appear as if it came from someone the victim normally conducts business with; however, the email requests money be sent to an account the attacker controls. The emails can be made to appear as if they originate from someone inside the company, such as a boss requesting an assistant to initiate a wire transfer with the company's bank. Or the emails may be designed to appear as if they come from outside the company, such as from a trusted vendor. The FBI advises to be on the lookout for the following regarding BEC scams:

- *The use of urgency and last-minute changes in wire instructions or recipient acct. information*
- *Last-minute changes in established communication platforms or email account addresses*
- *Communications only in email and refusal to communicate via telephone*
- *Requests for advanced payment of services when not previously required*
- *Requests from employees to change direct deposit information*

Remain alert and follow established procedures for funds transfer requests, whether Working From Home (WFH) or from the office. For more information, see the FBI release here.

Web and Teleconference Risks

Web conferencing and teleconference applications provide another vector for malicious cyber attackers to propagate attacks. Whether in the office or WFH, create non-public, private conferences that require username and password credentials. Do not publicly post meeting access links and credentials, and at the end of the conference session close the application and browser windows used to access the application.

Additional Resources:

The FBI has created a publicly available section on its website that warns of various COVID-19 related scams and provides tips and resources to help protect against COVID-19 related scams:

https://www.fbi.gov/coronavirus

Always check with your financial institution or law enforcement if you think a call or letter might be fraudulent!