FARM CREDIT

FRAUD PROTECTION AWARENESS SERIES

Fraud Tip #9 – Cyber Security

With e-commerce and online banking continuing to outpace in-person transactions, fraudsters are flooding the Internet. It's more important than ever for businesses and consumers to ensure their security when conducting transactions online.

This quarter, we discuss Internet security and the technological elements – such as firewalls, anti-virus software and passwords – which all Internet users should employ to protect themselves from hackers, viruses and other malicious software. We urge you to adopt these best practices to protect your corporate computer network, as well as your home system and mobile devices.

Phishing and the Internet Security Mindset

For all of its utility, the Internet provides a cloak of anonymity upon which fraudsters rely. Authentic-looking emails and websites can be fake. Personal information can be stolen and used to make illegitimate requests like *"Please change my bank account number in your system..."* or *"I need you to send $25,000 immediately to..."* seem legitimate. Seemingly innocent file attachments, often with a note like, *"I thought you might like this..."* can carry malicious software that will open a computer network to criminals.

It is critically important to be mindful of every request, offer or statement you receive electronically. Be especially suspicious of emails like these:

- Emails that claim to be from a financial institution, a government agency or other entity, that request account information or verification of account or login credentials such as usernames, passwords, personal identification number (PINs), etc. These *phishing* attacks often use official logos and mimic other website graphics to make them appear genuine.

- Emails with links or attachments requiring you to change or verify your account information. Such links or attachments often contain malicious code that could expose your company's login and account credentials to fraudsters.

- Unusual or oddly worded emails from friends and acquaintances. Such emails are an indication that the person's account may have been compromised and is being used in a fraud scheme.

- Any bank-related email that comes from an email domain that may be used by the general public, such as *@gmail.com, @yahoo.com, @outlook.com* and others. Any bank-related email or request coming from a domain normally used for personal email rather than the bank's own domain, such as *@cobank.com, @wellsfargo.com* and *@chase.com* is probably fake. Even email that appears to come from the bank should be checked carefully for misspellings or additional characters that make the company name vary slightly from the real domain name. For example, *@cobank.com* is legitimate, but *@co-bank.com* or *@cobonk.com* are not.

When conducting business on the Internet, be vigilant! Trust your instincts. If a request seems odd, it probably is. Pause and take the time to verify through another person or channel that the request is legitimate, such as by making a phone call to a number you recognize – not the one provided in the email.

Online Banking Technical Security

Your company should conduct its online banking only through a dedicated computer that is not used for accessing email or other non-banking websites. The computer – as all company and personal computers – should be running firewall and antivirus software that is updated and checked for security patches regularly. Updates should be run at least weekly, using the software's automatic update feature takes care of this important task. (Fact: According to Equifax CEO Richard Smith's testimony before the House Energy and Commerce Committee, the 2017 Equifax data breach was caused by the company's failure to install certain software security patches.)

Additionally:

- Run anti-virus software in active or real-time scanning mode. This allows the software to actively scan all incoming messages, files or websites being accessed, and to identify and prevent malicious content from running on your computer.

- Conduct comprehensive system scans routinely – at least weekly – to detect viruses or malware that may have been missed by real-time scanning.

- Use web content filters to prevent browsers from accessing known malicious websites.

- Use multifactor authentication to confirm your identity by presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only you know), possession (something only you have) and biometrics (something only you are). One common multifactor authentication method is to have a one-time password sent to your phone when you log in.

Never use public computers or public Wi-Fi hotspots to access your bank account online.

- **A note about Mac OS:** a common misconception is that Apple products running Mac OS are less susceptible to malicious code and viruses. *Not true!* Fraudsters and hackers target Mac OS just as much as Windows and Linux. Firewall and antivirus software should be installed, updated and used routinely on all computers running Mac OS.

User IDs, Passwords and Challenge Questions

Limit account access and online banking activity to the fewest number of people possible – only to those who require account access as part of their documented job duties. Protect user IDs, passwords and responses to challenge questions. Never write them down and never share them among users.

More best practices:

- Do not store login credentials for banking websites in your web browser's password store, and disable any feature that automatically enters your password for you. Malicious software can easily obtain passwords stored in the browser.

- Use long, complex passwords consisting of upper- and lower-case letters, numbers and special characters. Do not use names or special dates that may be known or guessed by others. Length is a greater measure of password strength than complexity, so consider using a longer password for banking websites.

- Use a unique password for each application or website you access to help mitigate the potential for all of the systems you use from becoming compromised if the password for one site or application is stolen.

- Select challenge questions and provide answers that are easy for you to remember, but hard for others to guess. Avoid choosing questions with answers that may be found on social networking sites, such as, "What is your pet's name?"

- Whenever possible, avoid selecting the same challenge questions for online banking that you have used on other sites.

Please note: *A bank will never ask you to provide answers to your security challenge questions via email, phone or text message.*

Securing Mobile Devices

Because they are so portable, mobile phones, tablets, e-readers, etc., can easily be compromised if they're not properly protected either with a passcode, fingerprint or face scan. Avoid using simple passcodes like 1111 or 1234 as well as passcodes based on your birth date, address or telephone number. Install security apps on all mobile devices, and scan for viruses regularly.

Routine System Access Review

To address employee turnover, which may happen at unplanned or inopportune times, the recommendation is to implement a process to immediately remove access to sensitive and password-protected areas and information, especially online banking, when an employee leaves the organization. A full audit of employee online and sensitive system access should be conducted at least twice per year.

As you consider the fraud awareness information provided above, please also bear in mind your important role in the fraud detection and reporting process. Your vigilance in reviewing your accounts and transactions is vital to fraud prevention and detection. Fraud schemes – as well as loss recovery efforts and outcomes – can be complicated. Early detection and prompt reporting of a fraud incident is critical because the passage of time might adversely affect the potential recovery of a fraud loss or the outcome of a customer claim. Your attentiveness often is the first line of defense for fraud, and, if a fraud incident does occur, your diligence might aid in a potential loss recovery.