FRESNO MADERA FARM CREDIT
AGRICULTURE IS OUR ONLY BUSINESS

Fraud Protection Awareness Series

Fraud Tip #4 – Cyber Account Takeover

One of the common ways that fraudsters commit these scams is through cyber account takeover – the ability to take control of an online account by stealing a user's login credentials or hijacking an online session. Once in control of an account, a fraudster steals funds by initiating outgoing wires or ACH transactions, which can be extremely difficult – if not impossible – to recover if not identified timely.

Cyber Account Takeover

Cyber account takeover occurs in several steps:

- Malware – Cyber account takeovers are routinely initiated through malware, which is transmitted by an email attachment or a hyperlink embedded in an email. All it takes is for the recipient of a fraudster's email to click on a link or open an attachment, and the malware – a malicious software program, also called "spyware," a "worm," a "virus" or a "trojan horse" – is secretly installed on the recipient's computer. Malware programs can record a user's keystrokes in order to capture passwords, redirect a user's internet session to a fake, but real-looking site, or even take control of the user's online banking session.

- One specific type of cyber account takeover is the Man-in-the-Browser (MITB) attack, also called *Man-in-the-Middle (MITM).* Due to the sophistication of this type of malware, traditional anti-malware programs are less effective at detecting it. A fraudster using a MITB can "see" and manipulate the information being displayed or typed into an infected computer's web browser (Internet Explorer, Safari, Firefox, Chrome and others). Since the MITB attack takes place inside the browser itself, security controls, like website encryption, are largely ineffective.

- Once on the user's bank web site – *which can occur at the same time as the user* – a fraudster can initiate wire transfers or ACH transactions in the background without the user's knowledge. The fraudster can even change the images displayed on the user's screen in real time – masking these transactions, and even displaying fake account balances and completed transaction records that exclude fraudulent wires/ACHs.

This sophisticated malware can also be programmed to perform these functions without the fraudster's active participation. The same technology can be used to capture login credentials in order to access the site at another time.

Why Cyber Account Takeover is Effective

- MITB's are used to secretly take over a computer being used by a company's employee to access the company's business bank accounts on the Internet. Highly sophisticated technology makes these attacks – or takeovers – easy to perpetrate and very difficult to identify.

- While they are sophisticated, MITB attacks fundamentally rely on a user to click on a link or open an attachment in order to infect the computer. Malware can originate in legitimate looking business emails, but may also be in emails from a legitimate sender's account that has been compromised. They are also often delivered as personal emails from a user's friend or family member. The message may be as simple as – *"Hi, I thought you might find this interesting!"* followed by either a link masked as a phrase (usually colored and underlined text) or a URL (web site address, also in colored and underlined text).

- An MITB attack's ability to display different images on a user's screen also makes it effective in defeating two-factor authentication, such as requesting to enter a second passcode delivered separately by text message.

How to Prevent Cyber Account Takeovers

- Train all of your employees – not just those with online banking access – to be cautious when clicking on any web links or attachments in company emails. Personal emails sent to an employee's company e-mail address, or emails accessed through a public domain email server (Gmail, YahooMail, Outlook and others) using a company computer also pose potential threats.

- Consult with your end-user services department or IT provider on ways to strengthen your Internet/technology infrastructure to inhibit MITB attacks and other outside threats.

- Be suspicious of unusual behavior on websites, especially if the input of a second set of credentials is requested on a single computer.

- Update your computers with the latest software patches and perform comprehensive anti-virus scans on all computer systems on a frequent basis.

As you consider the fraud awareness information described 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 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 to a fraud, and if a fraud occurs, your diligence might aid in a potential loss recovery.