FRESNO MADERA
FARM CREDIT
AGRICULTURE IS OUR ONLY BUSINESS

# Fraud Protection Awareness Series

## Fraud Tip #5 – Email Account Breach

This article covers Email Account Breaches, which are one of the most common ways for fraudsters to launch impersonation scams, obtain confidential information or insert harmful software onto a victim's computer that will serve as the basis for many other types of fraud scams.

### Email Account Breach

- An Email Account Breach is a fraudster's practice of hacking, or taking over, an individual's email account for the purpose of committing fraud aimed at the victim's business associates, family members, friends and acquaintances.

- Playing off of the relationships between the individual and those people listed in their email account's address book, a fraudster will use the hacked email account to socially engineer the victim's contacts or to send messages with a link that, if clicked, will install malicious software (malware) on the recipient's computer.

- Email takeovers such as this, more commonly occur on public email domains (Gmail, Yahoo Mail, Outlook and others) when the owner's user name and password have been stolen.

- Breached email accounts are often used by fraudsters to steal confidential information included in the email box, such as account numbers or passwords, or by utilizing the breached account to request information from third parties. Since the email is originating from the known valid email account, it may be trusted as proof of the requestor's identity, when in reality, the fraudster is sending the email.

- Another way fraudsters use email to commit fraud is by using a spoofed email address, which looks very similar to a legitimate email address. Spoofed email addresses are commonly used to mimic private domain addresses. For example, a legitimate email address john.doe@COBANK.com could be spoofed as john.doe@C0BANK.com, where the numeral zero - "0" - has been substituted for the letter "O" in COBANK. When words are in all CAPS, the difference is very hard to distinguish.

- More and more frequently, breached or spoofed email accounts are used in impersonation scams to trick company employees to initiate wires and ACH payments to third parties.

## Why Email Account Breaches Are So Effective

- Email Account Breaches succeed largely on the basis of trust and credibility. While not all of a person's email recipients are family members, friends or trusted acquaintances, many will be. Fraudsters succeed by taking advantage of the trust and credibility established between two people and by giving the email recipient a sense of confidence that the message is real - "If this is coming from Jim, it has to be OK."

- Once fraudsters have access to a victim's email account, they will review previous email conversations with selected individuals and tailor email correspondence referencing previous conversations in order to make the email sound more legitimate. After referring to a previous conversation, the fraudster will request a payment be initiated to a third party.

- Trust plays a similar role in spoofed email account requests. A company's employees are simply fulfilling what appears to be an authentic request from a trusted business partner or even the head of their own organization. CEOs are impersonated by fraudsters in order to create the illusion that the payment request should not be questioned because it is coming from the CEO.

## How to Identify Potentially Breached Emails

- Closely examine the email address from which you received a message with an embedded hyperlink
  - Does it seem authentic?
  - Does it match the name and/or entity at the bottom of the email body?
  - An established and recognized company will never send an email using a public domain, e.g. homedepot@gmail.com or fedexcustomerservice@yahoo.com. Do not respond to such emails and do not click on embedded links in these emails.

- Avoid clicking on links where the email or web address is masked - such as "Click here" (in colored and underlined text) instead of the actual address.

- Trust your intuition- ask yourself these questions about an email link or request for information you receive that seems odd or unusual to you:
  - Does this look like emails I have received from this person/company in the past?
  - The entity requesting this information should already have it on file - why do they need to ask me for it?
  - Should this entity really have access to my login name and password, Social Security Number, or the other sensitive information that they're asking for?

- If you are suspicious of an email request, call the company using a publicly available phone number - not one provided in the email - to verify the request. If you use the contact information provided in the email, the fraudster might reply that the message is safe.

- When checking personal email from a company computer, avoid clicking on any embedded links whatsoever. Take the same precautions listed here in clicking on embedded email links from your personal computer or smart phone

- Be extremely cautious when clicking on embedded links - even from family members and close friends - that provide a hyperlink and nothing else, or a very short message and a link, such as “Thought you might like this.”

- Although fraudsters have become more sophisticated in crafting and delivering messages, be extremely wary of emails purporting to be from established businesses that have spelling or grammatical errors, or the look of the message seems “off”, awkward or unrealistic.

- Install and maintain antivirus and firewall software on all computers and mobile devices. 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 to identify and prevent malicious content from running on your computer. Run a comprehensive antivirus scan on a regular basis. Full or comprehensive scans may detect viruses or other malware missed by real-time scanning. Remember that no anti-virus software is perfect so use caution regardless of the ant-virus software being used on your systems.

- Keep your computers up to date with the latest software patches.

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 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 to a fraud, and if a fraud occurs, your diligence might aid in a potential loss recovery.