ALLIANCE OF SCHOOLS FOR COOPERATIVE INSURANCE PROGRAMS

ASCIP

Guidelines & BEST PRACTICES

Cyber Attacks & Bank Fraud: Partners in Crime

CONTENTS

Introduction

Cyber attacks and fraudulent bank activity continues to increase, costing entities hundreds of thousands to even millions, of dollars. Many of these occur in the area of Electronic Funds Transfers (EFT) through something known as Social Engineering.

These attacks often start with a phishing email to someone in the target entity, or a perpetrator may intercept an email conversation and then inject themselves into it, taking over the conversation with the intended target while excluding others. A number of cases have started with an actual phone call (faxes, letters and texts are also common) from a third party impersonating a known vendor's executive or a government official.

Sample Incident…*Acme Construction is a known vendor performing numerous modernization and construction projects for your District. Your District makes regular large wire transfer payments to ACME for their work in progress. The ACME Construction CFO, John Brown, calls your District's accounting office and says his bank account has been compromised and is, therefore, opening a new account and requests future payments be sent to it. The accountant tells Mr. Brown he must complete an EFT form from their website. Mr. Brown completes the form and submits it to the accountant during the call. Mr. Brown even cc's the District's CBO in the email. The accountant shortly thereafter receives an email from the CBO approving the change. The accountant makes the change in the system. The next month, Mr. Brown calls the District and states he never received last month's payment. Upon investigation, it is discovered that the real John Brown never called the District. That was a fraudulent caller who provided a fraudulent routing and account number using a similar, but false, email address. The email from the CBO was also from a false email address.*

Since most bank frauds start or involve some sort of cyber-related attack, it's more important than ever that your Finance and IT professionals work together to defend against them. In the above incident, the fraudster may have been monitoring email traffic for months in order to discover key individuals and their processes.

This document is primarily focused on what your finance staff and those who work with them, including their IT colleagues, need to know to protect your entity's assets.

Let's Start by Defining Some Terms

Social Engineering: This is the act of using a phishing email or phone call to get you to actually send a perpetrator money. They will pretend to be someone else and convince you to change the EFT banking information so you send the perpetrator the money instead of your intended recipient.

Note*…Social Engineering scams are not typically covered by standard cyber or crime insurance policies. Special social engineering coverage is required to cover these types of losses.*

EFT: This refers to the electronic transfer of money from one financial institution to another, including banks, your county treasury, and/or the State of California. Electronic Fund Transfers (EFTs) include Automated Clearing House (ACH) transactions, wire transfers, electronic checks, credit/debit card payments, payroll direct deposits, and mobile apps such as Venmo or Apple Pay. All methods are fast and generally safe to use in sending and receiving funds. Recently though, EFTs are becoming a leading way for savvy perpetrators to take advantage of the unsuspecting.

Common EFT Methods

Wire Transfer: This is the method of electronically transferring funds directly from one financial institution to another. The sender usually pays a fee for this type of transfer, which is executed by a bank employee. Funds are transferred immediately, which is desirable to the recipient, and are nonreversible.

ACH Transfer: This is similar to a wire, except this method processes transfers in a batch by the sender. The information is sent to the Automated Clearing House (ACH), which clears the payments and pulls the cash from the sender's bank, then sends it to the various recipient banks involved. ACH transfers are usually free and considered just as safe as a wire

transfer. ACH transfers can take 1-3 days to clear, which allows the sender some time to catch an error.

ACH transfers can be reversed under certain circumstances, provided the funds are still available. This is how payroll direct deposits and transfers made through apps like Venmo and Apple Pay are processed. An electronic check is essentially the same as an ACH transfer.

Inter-Business Unit Transfers via County Office of Education: This transfer option is available to school districts, via a journal voucher. They are relatively safe to process since these entities operate within a closed system which simply tracks individual shares of the larger County Treasury Pool. Potential fraud occurs when you try to transfer funds to an outside entity by way of a wire or ACH transfer.

Paper Checks: Though not an EFT method, let's discuss these too, since physical checks have just as much fraud potential as EFTs. It is generally easier to understand the physical journey of checks from sender to recipient, when compared to what seems like a "black hole" that EFTs journey through.

Checks are ideal for paying small or occasional expenses. On the downside, they can get lost in the mail, "washed" (the ink removed and replaced with different information), copied and more. By the time a check is deposited into the recipient's bank account, it may have passed through many more hands and eyes, exposing sensitive data to a greater number of people and fraudulent opportunities.

Common Email Dangers

Since EFT fraud usually starts with an email communication, let's cover the various forms of email dangers one may face. With a good spam/malware application in place, most people don't realize how many dangerous emails are actually being sent to them. It is estimated that 80% of all email is spam related. Many are simply marketing emails to get you to click on an ad to buy something, but some can contain malware that can take over your entire network with one simple click.

SPAM: This is the general term for unsolicited junk email send out in bulk.

DID YOU KNOW…*The term spam (with lower-case letters) is thought to have become popular following a 1970 Monty Python sketch spoofing the well-known food. Gamers started picking up on the catchy song from this skit and started "spamming" each other with the words SPAM, SPAM, SPAM… (spelled with all caps). The name came from a contraction of the words 'spiced ham' and eventually developed into an acronym for **S**pecial **P**rocessed **A**merican **M**eat.*

Phishing: This is an email or phone call (**vishing**) or text message (**mishing**) that randomly asks you to change your email password or payment information. This is more directed than bulk spam email. **Spear-phishing** is the practice that targets a specific individual in an organization. Another variation, called **whaling**, specifically targets executives.

Business Email Compromise: Similar to phishing, these email scams involve sending a fake email message to a specific employee by a cybercriminal posing as a senior executive, requesting the employee to send a wire or ACH payment to an account controlled by the criminal, which is quickly transferred out, often overseas, making it very difficult to trace. These are very targeted attacks that involve research and advance planning. It is often easy to obtain the names and emails of company executives and key finance staff from an entity's website. Executives should exercise caution when sharing their travel plans on social media, as they could be being tracked by sophisticated predators.

Malware: Short for 'malicious software', this is a virus loaded into an email which asks the recipient to click on a link or open an attachment. By doing so, a malware virus (other terms include **rootkit** or **adware)** is released which is preprogrammed to copy itself and spread instantly from device to device, including printers, tablets, and network servers, eventually reaching the other computers connected with those servers, allowing the perpetrator to take control of all these devices. They may control settings, copy your data, monitor your activities and target you for other manipulative actions. These can remain undetected in the background monitoring your activity for months of even years.

Ransomware: This is a form of malware that can encrypt your files, computer and entire network, completely locking you out of your entire system so that neither you nor others can gain access without paying a ransom of some sort.

Audit your system to confirm it is adequately and reliably backed up in the cloud and completely inaccessible from your network.

This is referred to as Air Gapping and is your best means to recover against a ransomware attack without paying a ransom.

Best Practices to Avoid a Cyber Attack

Remember, scammers may have been monitoring email communications for months. They may copy and use commonly used language, company logos, similar email addresses, sender names and signatures to conceal their illegitimacy. However, there are measures staff can take to avoid these attacks.

- Beware of changes in vendor practices, such as if a vendor suddenly asks to only be contacted via email or provides you with an obvious nonbusiness email address.

- Unless you are expecting an attachment or link from someone, always reach out to them via a phone call to confirm they sent it to you.

- Always call using your known phone number, not the number in the email. Fraudsters are now utilizing **deepfake** technology to replicate an individual's voice and video image to trick you into believing they are the person they are impersonating. A return voicemail is not verification – have a direct conversation.

- Always look for suspicious characteristics in any unsolicited email.

  ✓ Is the sender's email and domain correct? If an email looks suspicious, hover your curser over the sender's email. This can sometimes reveal the sender's true email address.

  ✓ Check the email extension. Does it match the type of entity you are supposedly receiving the email from?

  .com (usually commercial businesses)
  .edu (usually colleges)
  .org (usually non-profits and schools)
  .k12.ca.us (many California schools)
  .ca.us (California public entities)
  .net & **.us** (just a few of the universal domains available)

  ✓ Perpetrators often add an inconspicuous letter, dash, or reorganize a few letters in the email address, or change the extension from ".edu" or ".org" to ".com". Look for misspellings, punctuations or odd formatting.

  EXAMPLE:
  Correct: *anderson@ascip.org*
  Fraudulent: *andreson@acsip.com*

  ✓ Is this email content consistent with the sender's character and writing style?

  ✓ Don't trust an unsolicited email just because you see familiar people cc'd.

- When responding to anyone involving financial discussions, rather than using the "Reply" or "Reply All" feature, use the "Forward" option to reply, then retype in their email. Do not rely on the auto-complete feature, as it may pick up the fraudulent email addresses. Add fresh cc's (carbon copies) to your message. Perpetrators will often add their own fictitious email addresses as cc'd individuals so that you don't add them yourself.

- Consider having the IT department add a cautionary banner to all external-originating email, such as: *ALERT: External message. Exercise caution when opening attachments or clicking links from unknown senders.* This will serve as a constant reminder to staff regarding the dangers they face daily.

- Implement multi-factor authentication for all system logins by staff. This is similar to what bank do now, requiring a verification code be

sent to your mobile phone or other pre-authorized device, to be used to confirm your identity.

- While changing passwords is not popular with staff, a strong password policy is essential.

> *"Don't depend on the enemy not coming; Depend rather on being ready for him."*
> **Sun-Tzu, The Art of War**

- Add end-point protection to all mobile devices, including laptops, tablets and mobile phones. If a device is lost or stolen, this process will lock and encrypt the device to prevent it from being used to access the network by a predator.

- Consider performing simulated phishing attacks with employees so they can get a feel for what to look for. There are many services available to assist with this.

- Provide staff with a go-to resource they can forward suspicious emails to for validation.

Training and raising staff awareness is the key to protecting your system and assets.

Best Practices to Avoid EFT Fraud

EFTs, if properly managed, are an effective and safe method of transferring funds, but extreme care must be exercised in establishing both the initial setup of, and changes to, the recipient's bank information. While today's online environment allows for more efficient movement of money, it also presents many risks for both IT and finance staff to guard against. Consider implementing the following precautions:

- Limit the number of people who are allowed to share financial and banking information in your organization.

- Never send any confidential information via email without encrypting it.

- Never transmit or even discuss confidential information while using a public WI-FI network. Always connect through your company's VPN (Virtual Private Network) or SDP (Software Defined Perimeter).

- Never initiate banking changes or process payments based solely on an unsolicited email, phone call, letter, fax or text message.

- Beware if someone says they need to change the way they receive payments due to an unusual event, such as a pandemic. Everyone has adapted to this situation and should have no problem issuing and receiving checks.

- Occasionally remind your customers and staff that your finance and HR departments will never ask for any financial or personal information via an email.

- If you don't utilized EFTs, consider adding a statement to the email signature of finance staff who handle invoicing, receivables and payables, such as the following: *ALERT: No one from our organization will ever contact you to request or change bank or EFT information.*

- **Remember:** No government entity or financial institution will initiate contact with you to request private or banking information via email.

- Implement a **two-factor authentication** process to approve any financial transaction change. This would include having a second staff person call back the client/vendor to verify a change involving sensitive items such as bank account numbers. Use previously known telephone numbers or look them up online. This includes verifying a change of mailing address to avoid mailing a check to the wrong location.

- Implement **dual-control** when processing any EFT transaction by requiring that at least two individuals are involved in its execution. For example, Employee A creates the ACH batch, but Employee B will have to approve and send the batch. Regarding a wire transaction, Employee A will initiate a wire transfer, but Employee B should review the wire transfer and receive the call-back from the bank to approve the transaction. Many banks utilize tokens to provide a unique transaction verification code, which provides an additional level of protection.

- Always perform a **pre-notification transaction** (or test deposit) with a blind confirmation. Once the ACH vendor is set up, a test payment is issued to ensure the vendor's bank account is the correct account, in the amount of a few pennies, such as $0.04. Then contact the vendor and ask what amount was deposited to their account. If the amount they confirm matches, then issue the first payment.

"Victory awaits him who has everything in order – luck we call it. Defeat is definitely due for him who has neglected to take the necessary precautions - bad luck we call it."
Roald Amundsen, South Pole Explorer

- Always request a signed Form W-9, Request for Taxpayer Identification Number and Certification, from every payee in advance of making any payment or changing their mailing address. Then, double check the address and Employer Identification Number (EIN) or Social Security Number provided. The IRS has a website for this purpose. Also, call the organization to confirm the change. Keep in mind that a W-9 does not prove an entity is not trying to defraud you, as it is very easy to obtain an EIN, but it is another safeguard.

- Consider setting a limit on the dollar value of allowed EFTs or add an additional level of approval for any individual transfer in excess of a certain dollar amount.

- Implement **Positive Pay** for both checks and ACH transactions, as well as placing an **ACH Debit Block** on your accounts, which declines all attempted ACH transactions from outside organizations.

- Consider using a Universal Payment Identification Code (UPIC). Many banks offer this. It is a unique account identifier that looks and acts just like a real account number for ACH payment transactions.

- If you utilize purchase orders, verify they are in place and vendor information is accurate for every transaction which requires one.

- Consider transaction monitoring services or implement your own analysis and reconciliation tools that might flag items, such as vendor payment variances >25% above normal, transactions over a certain dollar amount, first time vendor transactions, larger dollar transactions than usual, and of course, all international EFT transactions.

- Warn staff to be cautious of any emails or phone calls that try to persuade someone via intimidation, a sense of urgency, secrecy, or leveraging authority.

A word about fax machines and internet faxing:

Old fashion fax machines do not use the internet, making them inherently safer to send information. They are also more difficult, but not impossible, to hack. Documents received are safe from having attachment viruses included, but they do have vulnerabilities similar to regular mail. They do result in many more hands and eyes seeing what is sent. If you use an internet fax service, be sure it uses SSL encryption and has a secure web connection.

Guardians of "Your" Galaxy

Diligence, training, and staff awareness of the cyber dangers existing all around us are essential to defending against these types of fraud.

If your Finance and IT staff seem a bit skeptical at times, there is good reason for this. They are the guardians of your entity's financial resources. They take seriously the Russian proverb quoted often by President Ronald Reagan regarding a certain nuclear arms treaty…***"Trust, but verify."***

Additional resources can be found at ascip.org or by contacting your ASCIP Risk Services Consultant.

If you suspect your system has been hacked or breached notify your IT department immediately.

Then call ASCIP's **Cyber Hotline: (909) 477-0474**. We will walk you through the reporting and recovery process.