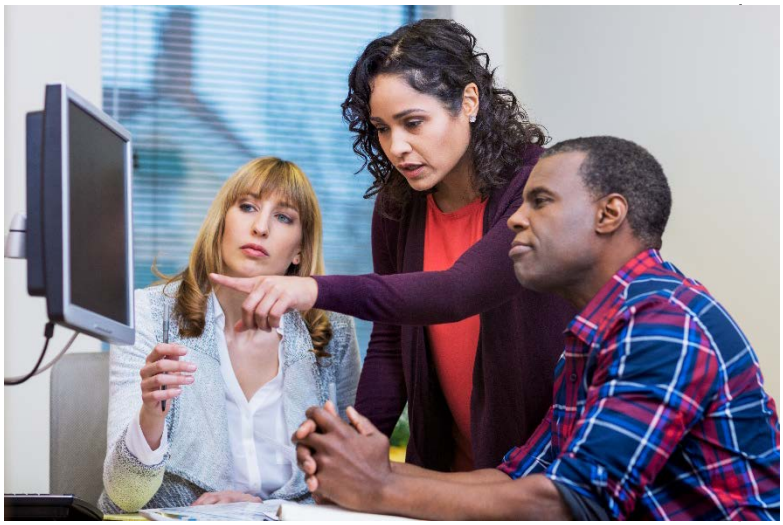
The Rise of Social Engineering Fraud

RISKS AS YOU GROW

Fraudsters use social engineering tactics to succeed by tugging at the basic human instincts to please. These scams look to catch employees off-guard, dupe you to comply with instructions from a malicious actor, and get you to act quickly.



Targeting the Weakest Link: Humans

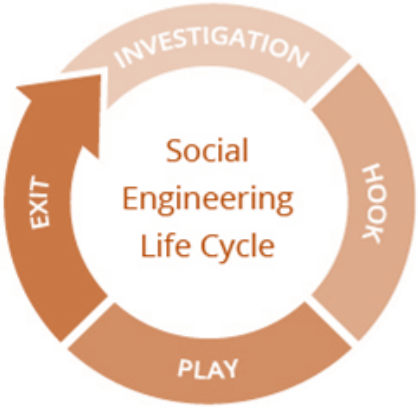
One of the fastest-growing corporate crime threats does not exploit IT or information security weaknesses; instead, fraudsters are targeting the weakest link: humans. Social engineering fraud is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

The four main ways in which social engineering occurs is by **phishing**, in which the hacker uses email to trick someone into giving them access to some kind of account, login, or financial information; **vishing**, which is the same but through voice, such as a phone call; **impersonation**, which is done on-site, through email, or text; and **SMiShing**, which occurs through SMS text message. What makes social engineering fraud especially dangerous is that it relies on mistakes made by legitimate users – like your employees using technology.

Social Engineering Life Cycle

The success of social engineering techniques depends on attackers' ability to manipulate victims into performing certain actions or providing confidential information. The typical social engineering life cycle follows these simple steps:

- **Investigation:** The fraudster prepares the ground for the attack by identifying the victim(s), gathering substantial background information, and selecting the attack method.
- **Hook:** The fraudster looks to engage the targeted victim by spinning a story, developing a relationship, and gaining buy-in. The goal is to take control of the interaction.
- **Play:** The foothold of the fraudster is expanded as more information is obtained over a period of time. The attack is executed by instructing the victim to take certain action or introduces malware which disrupts business and/or siphons additional data.
- **Exit:** With the interaction complete, the fraudster removes all traces of malware to cover the tracks without arousing suspicion.



Source:2018 Imperva

94% surveyed IT and C-suite execs have seen untargeted phishing attacks with malicious links in the past 12 months.

Source: Mimecast, Vanson Bourne; State of Cybersecurity Research Report. 2018.

Key Terminology

- **Social Engineering:** non-technical malicious intrusion that relies on human interaction and often involves tricking people into breaking normal security procedures and divulging confidential information.
- **Data Mining:** the search for and review of public records, social networks, credit reports, and/or mailed account statements for the purpose of committing identity fraud. Fraudsters typically gain access to substantial account holder information including last transactions, family member names, account numbers, Social Security numbers, real estate information and automobile make & model.
- **Malware:** short for malicious software, malware is designed to infiltrate a computer system without the owner's informed consent [Key Loggers, Banking Trojans, Worms and Viruses].
- **Dumpster-diving:** sifting through trash or recycle bins to find items and information that may be useful in identity theft.
- **Insider Job:** employees using their employment, job function, and computer or file access to steal valuable financial and intellectual information.
- **Spoofing:** a person or program that successfully masquerades as another person or program by falsifying data.
- **Web Spoofing:** the act of creating a website with the intention of misleading readers that the website has been created by a different person or organization. Normally, the spoofed website will adopt the design of the target website and sometimes has a similar URL.
- **Waterholing or Watering Hole Attack:** a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit.
- **Phishing:** one of the most popular social engineering attack types. Phishing attempts to acquire sensitive information such as usernames, passwords, and account or credit card details by masquerading as a trusted entity and creating a sense of urgency, curiosity or fear in victims. It then prods recipients into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.
- **Spear Phishing:** a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. A spear phishing message is usually based on job positions, characteristics, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks or months to pull off. They're also much harder to detect and have better success rates if done skillfully.
- **Whale Phishing or Whaling:** a form of spear phishing aimed at the very big fish — CEOs or other high-value targets.
- **SMiShing:** a type of phishing attack where mobile phone users receive text messages containing a website hyperlink, which, if clicked would lead to a malicious URL and/or download malware to the mobile phone.
- **Vishing:** voice phishing is the telephone equivalent of phishing attempting to scam the user into surrendering private information that will be used in identity theft.
- **Synthetic Identity Fraud / Theft:** using a combination of real and fake information to create a new identity for the purpose of opening fraudulent accounts. Fake info such as name and birthdate could be combined with a real Social Security number and fraudster-controlled address.

Interested in learning more about fraud, scams & protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

Fraud On The Rise

Phishing ♦ CEO / Executive Impersonation ♦ Synthetic Identity Theft ♦ Call Center Fraud

Recognizing scams can be difficult, especially after the impact of having personal information exposed following a data breach. But, you can minimize the potential impact by knowing what to look for, taking the right action steps, and remaining vigilant.

Phishing

Phishing is a cyber attack that uses a method of trying to gather personal information using deceptive emails and websites. The goal is to trick the email recipient into believing that the message is something they want or need — a request from the credit union, for instance, or a note from someone within the organization — and to give out personal information, click a link, or download an attachment. Phishing emails often contain attachments or links to malicious or spoofed websites infected with malware.

What distinguishes phishing is the form the message takes: the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business with.

It is one of the oldest types of cyber attacks, dating back to the 1990s; however, criminals continue to find this one of the best forms of stealing personal information or installing malware or viruses on computers. This can happen to your members, as well as employees, and can be devastating to your systems and confidential data.

Like an angler casting a baited hook hoping to lure a bite; the phishing email does the same. In fact, phishing kits – with website resources and mailing lists - are now available on the dark web to assist fraudsters. Even those with minimal tech skills can successfully launch phishing campaigns.

Two Primary Types of Phishing Campaigns

The fraudster typically is looking for the victim(s) to do one of two things:

- Trick the user to **share sensitive information** like a username and password that can be used to breach a system or account; or
- Get the victim to infect their own computer by **downloading malware**, such as an attachment or link to a job seeker's resume sent to HR or a hiring manager can be used to deliver malware.

While there are a number of types of phishing attacks: spear phishing and whale phishing are targeted campaigns that are often used.

Similar to phishing, **SMiShing** uses SMS text messaging to send fraudulent messages in the hopes you will click on a link or text back personal information to be used for identity theft, install malware, and steal funds. Fraudsters can be well disguised into luring the victim into calling a phone number or clicking on a link to install malware or a virus on your phone.

Vishing is essentially phishing over the phone. An attacker will call someone, such as a help desk, and with a little bit of info about a person (e.g. name and date of birth) either get login credentials or more info about the individual, such as a Social Security number.

Interested in learning more about fraud, scams & protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

Managing Against Phishing Risks

Regular education of employees and members is key! One of the best ways to learn to spot phishing emails is to study examples and be aware of warning signs.

Common Warning Signs

- **Be mindful of emails or phone requests** claiming to be from the business or financial institution which was breached.
- **Don't trust the display name** - fraudsters will spoof the name of an email to appear to be legitimate.
- Look but don't click. **Avoid opening attachments and clicking on links** contained in emails received from unfamiliar sources.
- **Avoid clicking on text message links or calling the telephone number** received from unfamiliar sources.
- **Check for bad grammar and misspelled words** in the content and within links.
- **Monitor the sender's email address** for suspicious domains – often using similar letters and numbers (like www.cunamutua1.com).
- **Check the salutation** - many legitimate businesses will use a personal salutation.
- **Do not provide personal information** when asked.
- **Be suspicious** of "urgent" or "immediate" response needed or "unauthorized login attempt" of your account.
- **Don't believe everything you see.** Brand logos, names and addresses may appear legitimate but if it looks suspicious, delete it.
- **Always check the spelling of the URLs** in email links before you click or enter sensitive information.
- **Watch out for URL redirects,** where you're subtly sent to a different website with identical design.
- If you receive an email from a source you know but it seems suspicious, **contact that source with a new email or phone call**, rather than just hitting reply.
- **Always, be wary of tempting offers.**

If an employee has received a phishing email, it should be deleted or submitted through your organization's phishing reporting system immediately. Do not open it.

Instill the "always alert" mentality into your culture by conducting frequent social engineering training for all employees as part of your security awareness training efforts. The goal is to change employee behavior to reinforce good data security practices.

Using a sample case study for discussion is a good way to engage employees. Some credit unions have also shared the best practice of testing employees. For example, credit union IT departments or third-party vendors can send phishing emails to employees to determine who will open the attachment or click on the link. This approach allows your credit union to better assess your employee-related risk and create metrics to demonstrate how well the training program is working.

Remember…cyber thieves continue to target the weakest link at organizations – most often, the employees. Don't just think it is front-line staff though; these criminals often hit the jackpot when the malware compromises credentials of key administrators. This allows them to move about the network and access sensitive data without being noticed.

Defenses Credit Unions Can Take

Defend against malware and spear phishing attacks:

- Deploy a spam / email filter capable of detecting malicious attachments / links to malicious websites;
- Use a web filter capable of detecting malicious websites;
- Maintain an up-to-date antivirus / antimalware solution;
- Update your operating system whenever security patches are available;
- Block access to personal email accounts;
- Monitor all network traffic including inbound, outbound, and internal traffic; and
- Conduct frequent security awareness training, including social engineering, for all employees.

Interested in learning more about fraud, scams & protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

CEO / Executive Impersonation

These fraudulent schemes are increasingly more common, frequently spoofing or imitating a business executive or vendor's email request to initiate a wire transfer or send employee personnel information.

Impersonation fraud, also known as Business or CEO email compromise, is accomplished by either phishing an executive and gaining access to that individual's inbox or emailing employees from a look-alike domain name. These spoofed domains may only be one or two letters off from the true domain name. For example, if the target domain was "ABC1cu.com" the thieves might register "ABClcu.com" (substituting the letter "L" for the numeral 1).

Unlike traditional phishing, the spoofed emails used in CEO / executive impersonation fraud are rarely detected by spam filters because they are targeted to one individual within the credit union organization.

87%

surveyed IT and C-suite execs have seen

email-based impersonation attacks asking to initiate wire transfers.

Source: Mimecast, Vanson Bourne; State of Cybersecurity Research Report. 2018.

In cases where executives or employees have had inboxes compromised, the perpetrators will examine the victim's email correspondence for key terminology like "payment" or "deposit". The perpetrators will then create a request appearing to be from the executive to initiate an urgent payment – typically a wire transfer to pay a vendor, for an investment, or a "confidential matter."

A message may also be sent delegating authority to an attorney or another third party to provide payment or changes to previously established payment instructions. In at least one case, the credit union's email system was compromised which led to a fraudulent email request for a large wire transfer.

Unfortunately, once the money is wired, there is little recourse to recover those funds, particularly as almost all involve overseas accounts.

Synthetic Identity Fraud

Synthetic identity fraud uses a combination of real and fake information to create a new identity for the purpose of opening fraudulent accounts. Fake info such as name and birthdate can be combined with a real Social Security number and fraudster-controlled address. In fact, the scope of the problem is difficult to determine because it can go undetected for years.

When setting up a synthetic identity, fraudsters assemble multiple components:

- Social Security number (SSN)
- Fictitious name
- Fictitious birthdate
- Address controlled by the thief

This provides the fraudster with enough information to set up an account, apply for a credit card or loan, or piggyback on an authorized member's account. The fraudster then has the ability to establish a credit history and good credit score for this fictitious member.

Once high card or loan limits are established, it is time to "bust-out." The identity thief charges cards or lines of credit up to limits, pays northing back, and discards the identity.

Credit unions with nonprofit organizations within their field of membership are especially attractive to fraudsters pursuing synthetic identity fraud. They only have to join the nonprofit organization, or make a small contribution to a charitable organization, to qualify for credit union membership.

SSNs should always be closely guarded – as it doesn't change making it the ultimate prize for an identity thief.

Interested in learning more about fraud, scams & protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

Helping Members Protect Children and Minors

Most minors under the age 18 may not have a credit report available for review. However, children are regular targets of identity theft, and parents should take care to protect their children's financial future.

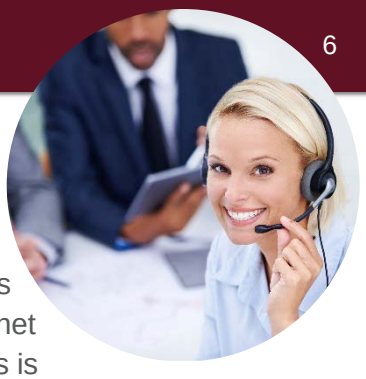
Look For Warning Signs

- Collection notices or calls regarding products or services in your child's name.
- Notice declaring a child owes back income tax, or that his/her identifying information was used on multiple tax returns.
- Marketing offers for pre-approved credit in a child's name could be a sign that an account was opened at a financial institution.
- Be careful about sharing a child's private identifying information especially SSN. If asked to share, ask and understand how it will be used.

Check the Child's Credit

- Contact each of the three nationwide credit reporting bureaus – Equifax, Experian, and TransUnion - and request a credit report in the child's name.

  Consumers are entitled to a free credit report from each of the three major credit bureaus annually. Simply go to www.AnnualCreditReport.com to get started. Items to watch for are "new" or "re-opened" accounts and other suspicious activity.
- If there is a credit report in a child's name, request a fraud alert, and consider placing a credit freeze.
- Contact the local police department or Attorney General's Office to file and report the identity theft and request a copy of any report generated.
- Contact any financial institution and business listed on a child's credit report and explain the account was opened because of theft and request it be closed. Documentation from the credit bureaus and law enforcement may need to be produced.
- Keep a detailed list of any phone calls made and/or documents received as these may need to be produced later.



Call Center Fraud

Call center fraud spiked over 100% in 2016 according to darkreading.com and criminals are using Voice over the Internet Protocol to spoof caller ID; this is making it increasingly more difficult for call center representatives to feel confident they are speaking to the actual member.

As credit unions continue to strive to provide the best customer service; they can also open themselves up to more risk. Speaking to a call center agent provides the criminal an upper hand knowing their job is to provide the best member experience.

One approach fraudsters take is to call and speak to different representatives in hopes to obtain information on your members' accounts piece by piece. In addition, the fraudsters generally will use the call center to change contact information such as a phone number (mobile or home), email address and physical address, or to reset or change a password.

Fraudsters also have been known to request a copy of a canceled check including HELOC checks. With this copy, they are able to create counterfeit checks against the member's account or the HELOC account.

Some red flags to watch for are:

- Member calls several times in a short period of time
- Requests to change information on file such as the address and/or phone number
- Caller redirects conversation when unsure of answers regarding authentication
- Long pauses or incorrect verification answers
- Sets up member accounts for audio response and/or online banking
- Asks how to wire transfer money and/or requests wire transfers to foreign organizations

A strong method of verifying the identity of members who call the credit union is critical. Consider deploying an identification verification solution in the call center that relies on strong out-of-wallet questions.

Interested in learning more about fraud, scams & protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

Tips to Reduce Social Engineering Risks

1 Require Redundancies

Set a policy, establish procedures, and consistently enforce that multiple employees are required to sign-off on transactions such as wire transfers. This dual control can ensure more than one set of eyes are reviewing transactions for suspicious activity – especially for those employees handling funds regularly.

2 Maintain Antivirus / Antimalware Software

Make sure automatic updates are scheduled and engaged. Periodically monitor that updates have been applied and make sure your systems are scanned for possible infections and malware.

3 Use Multifactor Authentication

Require different forms of authentication such as verifying requestors via other means of communication. If a request is made by email, for example, then make a phone call to a previously-established number to verify the transaction.

4 Limit Public Information

Don't make it easy for the scammer. Credit union websites, mobile apps, and social media pages should limit the amount of information available on employees. Be cautious with job duties, descriptions, and out-of-office details connected to employee names.

5 Consider Safeguarding Tools

Integrate safeguards like a centralized email address to forward suspicious messages to IT for investigation; block IP addresses or domains in malicious messages; and, build in official credit union branding to distinguish between authentic and fraudulent emails.

6 Conduct Pen & Social Engineering Tests

Frequent penetration testing exercises and test phishing emails can assist employees in knowing what to look for, in addition to providing you with a measurement of how good staff is at following procedures and scouting out scams, spam, and other shams. Remember to use penetration testing on multiple channels…not just email.

7 Educate Employees (and Members)

As fraudsters get more sophisticated in the ways they exploit technology and humans; it is even more important to know what to look for, to take the right action steps, and remain vigilant. We're all human, after all.

Provide employees, volunteers, and members with proactive tips – like those found in An Employee's Guide to Phishing Emails - to ensure personal and sensitive information is not compromised. Encourage them to be suspicious of unsolicited emails and only open those from trusted sources. Never forward, respond to or access attachments or links in such emails; delete or quarantine them.

Train employees to recognize psychological methods that social engineering fraudsters use: power, authority, enticement, speed and pressure.

Create an always alert culture.

In social engineering fraud, hackers exploit the human inclination to trust.

Interested in learning more about fraud, scams & protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

Conclusion

The area most susceptible to fraud or a successful cybersecurity breach isn't always your credit union's network perimeter or web applications. It could actually be with your people and member services support. The human factor is far easier to compromise than your credit union's technology.

Social engineering criminals look for the opportunities that can be exploited with minimal effort, offer a low risk of being discovered, and have the potential for higher pay-offs.

Make cybersecurity a significant part of your credit union's fabric and culture. Every employee of your credit union should be an active part of your approach to cybersecurity. Set aside time and resources for training. Make it clear that protecting your credit union's data is a collective effort, not just the responsibility of a few employees in IT.

CUNA Mutual Group is dedicated to help you understand these pressing risks and provide you with the most relevant resources you need to build a strong risk management strategy and make confident decisions.

To gain additional insights about cybersecurity vulnerabilities, protections, and access to more resources to help you rise above the risk of social engineering fraud, contact a CUNA Mutual Group Risk Consultant at:

Risk & Compliance Solutions
• 800.637.2676 •
riskconsultant@cunamutual.com

Additional Resources

Additional resources to assist your credit union in managing risks of social engineering fraud can be accessed at:

- Anti-Phishing Working Group
- Fraud.Org
- Internet Crime Complaint Center (IC3)
- Stop. Think. Connect.
- Consumer.gov: Scams & Identity Theft

Report scams to the Federal Trade Commission at 1.877.IDTHEFT

CUNA Mutual Group, cybersecurity insurance carriers, credit union associations and leagues also release free resources on emerging threats – like RISK Alerts, whitepapers, webinars, and risk assessments. These resources provide your credit union with actionable risk management techniques. In fact, you can use these resources as a launching pad for education and your credit union's customized cybersecurity approach.

Access the Protection Resource Center (UserID and Password required) at www.cunamutual.com/prc for exclusive cyber risk and security resources:

- Ransomware Risk Overview
- Member Protection Tips
- Post-Breach Consumer Tips
- An Employee's Guide to Phishing Emails

Beazley Cyber Insurance policyholders can access additional employee tip sheets at beazleybreachsolutions.com.