TruStage™

Social engineering fraud

Employee's guide

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

Four primary ways in which social engineering fraud occurs

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 in 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.

Keep in mind…intimidation tactics and urgent requests are common.

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.

Vishing is essentially phishing over the phone. An attacker will call someone, such as the 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.

SMiShing, like phishing, sends fraudulent messages via text messaging 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 you into calling a phone number or clicking on a link to install malware or a virus on your phone.

Impersonation fraud, also known as business email compromise or fraudulent instruction, is accomplished by either phishing an executive and gaining access to that individual's inbox or emailing employees from a look-alike domain name. The spoofed email request is usually looking for you to initiate a wire transfer or send employee personnel information.

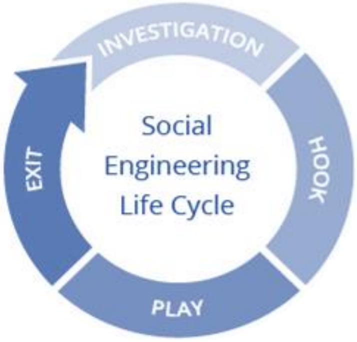
If you receive an attempt at social engineering fraud or a phishing email, you should delete it or use your organization's phishing or credit union's established fraud reporting system immediately.

Notify your IT department, but do not open, respond, or provide information!

Social engineering life cycle

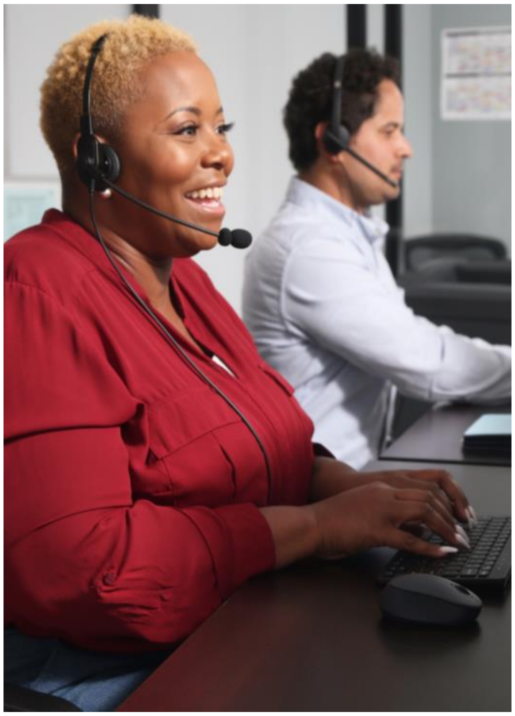
The success of social engineering techniques depends on attackers' ability to manipulate victims into performing certain actions or providing confidential information. The typical social engineering life cycle follows these simple steps:

- **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.

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.



The call center is often a first stop for fraudsters

Fraudsters gravitate to the phone channel because the primary line of defense — call center representatives asking challenge questions — is highly vulnerable to social engineering. It is easier for fraudsters to find answers to challenge questions and then social engineer a rep into granting access to a member account than it is to hack IT infrastructure backed by a dedicated security team.

Call centers are also unique because of the human element involved — call center reps are expected to deliver a consistently positive member experience and simultaneously perform first-line fraud defense. That is a difficult balance in today's customer-centric environment.

Fraudsters will often start in the call center, and then move on to digital channels. Once a fraudster takes over a victim's account via the phone channel, the fraudster may change an online banking password and phone number associated with that account. This sets the stage for fraudsters to steal funds from the accounts.

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.

Reducing social engineering fraud

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.

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.

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.

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.

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.

Many organizations implement the use of a phish alert button where users can report suspicious emails with just one click. This provides a safe way to forward email threats to the security team for analysis.

Conduct penetration & 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.

Create an always alert culture by educating employees & 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 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 links or attachments in such emails; delete or quarantine them.

Train employees to recognize psychological methods that social engineering fraudsters use:

- power
- authority
- enticement
- speed
- pressure

> In social engineering fraud, criminals look for opportunities that can be exploited with minimal effort, offer a low risk of being discovered, and look to exploit the human inclination to trust.

Common red flags of phishing emails

Phishing emails are hard to detect at a quick glance; however, looking for common red flags can help.

Email sender

Identify

- □ I'm not familiar with the sender. Do not trust the display name.
- □ The sender's email address is not someone I usually communicate with.
- □ I have not previously communicated with the email address.
- □ The email address contains a suspicious domain, replaces letters with numerals (e.g., 1rustage.com), or doesn't match between the header and body.

Email heading/subject line

Review

- □ I was cc'd on the email with a group of individuals I don't recognize.
- □ The recipient group seems random or unusual (e.g., all last names begin with the same letter).
- □ The email appears to be a reply to a message that I didn't send.
- □ The subject line seems odd and/or doesn't match the email content.
- □ The subject line contains typos and/or spelling errors.
- □ The date and/or time the email was sent seems out of the ordinary.

Trending!
More phishing email subjects appear to come from HR/IT/Managers. These attacks are often effective because they could potentially affect daily work and cause an employee to react before thinking logically about the legitimacy of the email.

Links & attachments

Confirm

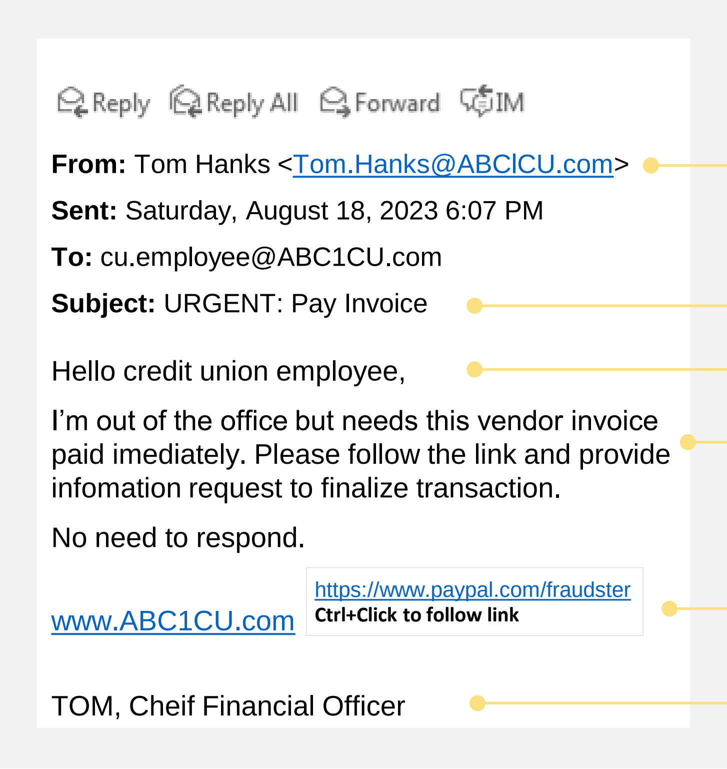
- □ I wasn't expecting an attachment or link.
- □ The message encourages me to click on a link or open an attachment.
- □ The message encourages me to click on a link or open an attachment to avoid a negative consequence or gain something of value.
- □ The attachment file type seems suspicious.
- □ When I hover over the link it appears that it is a different URL destination to which I will be redirected.
- □ The URL contains a suspicious domain or a misspelling of a known website.

Email content

Evaluate

- □ The message contains bad grammar or spelling errors.
- □ The request seems odd or out of character for the person sending it.
- □ The message seems threatening, illogical or makes me uncomfortable.
- □ The message only contains a link or an attachment.
- □ Check the salutation. Many legit businesses personalize.
- □ Be suspicious of urgent or immediate response needed and unauthorized login attempt messages.

Sample phishing email



From: Tom Hanks <Tom.Hanks@ABCICU.com>

Sent: Saturday, August 18, 2023 6:07 PM

To: cu.employee@ABC1CU.com

Subject: URGENT: Pay Invoice

Hello credit union employee,

I'm out of the office but needs this vendor invoice paid imediately. Please follow the link and provide infomation request to finalize transaction.

No need to respond.

www.ABC1CU.com

https://www.paypal.com/fraudster
Ctrl+Click to follow link

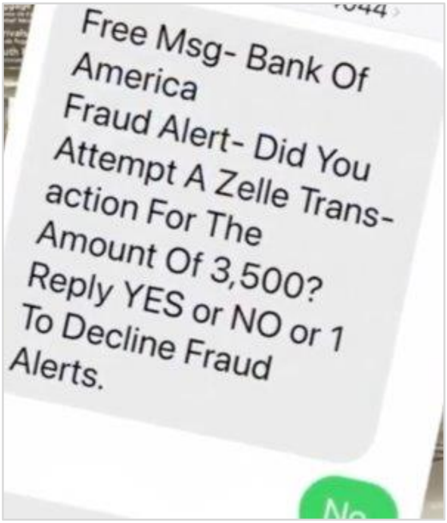
TOM, Cheif Financial Officer

Key red flags to look for:

- Email address includes changed characters
- Creating sense of urgency
- Non-personalized content
- Multiple typos & grammatical errors
- Encourages clicking on a link with a masked URL
- Request from a high-level authority

Sample SMiSHing text

- Fraudsters send a text alert to members – appearing to come from the financial institution – asking the members if they attempted a transaction
- Spoofing the financial institution's phone number, fraudsters call members who respond 'NO' and claim to be from the fraud department
- Fraudster tells member the transaction went through – however, the stolen funds can be recovered
- Fraudster explains to recover the stolen funds, the member must use P2P to transfer the money to himself/herself using the member's mobile number
- The Zelle transfer is actually sent to the fraudster



Free Msg- Bank Of America Fraud Alert- Did You Attempt A Zelle Transaction For The Amount Of 3,500? Reply YES or NO or 1 To Decline Fraud Alerts.

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

This resource is for informational purposes only. It does not constitute legal advice. Please consult your legal advisors regarding this or any other legal issues relating to your credit union. TruStageTM is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy. Please read the actual policy for specific coverage, terms, conditions, and exclusions.

TruStage™