Preventing Fraud In Digital Channels

Eltropy White Paper

Credit Unions, Banks and their consumers face a growing volume of fraud attacks each year. According to this FTC report, consumers lost over $5.8 Billion in 2021, up 70% over 2020. While there are many types of frauds Credit Unions and Banks have to deal with, the ones that are within the scope of this white paper include the two most common around Digital Communication::

1) Member Phishing Scams
2) Inbound Contact Center Scams

Member Phishing Scams

Phishing is when attackers send malicious digital communication or make phone calls designed to trick people into falling for a scam. Typically, the intent is to get users to reveal financial information, system credentials, or other sensitive data.

eltropy

Phishing

Encompasses deceitful email, websites, text messages and more, cyber criminals use phishing campaigns to steal confidential personal and organizational information. Often, hackers will hide behind email senders or websites that are familier to the intended victim.

Quid Pro Quo

Quid pro quo social engineering scams hinge on an exchange of a reward or information that convinces a victim to act. A common technique is for a criminal to contact an employee, claiming to be an IT support employee and urging them to confirm login details.

Pretexting

Leverages a false identity to trick the victim into giving up confidential information. A common example is when cyber criminals impersonate a customer service representative for a known company where a user recently made a purchase.

Examples of Common Social Engineering Tactics

Waiter-Holding

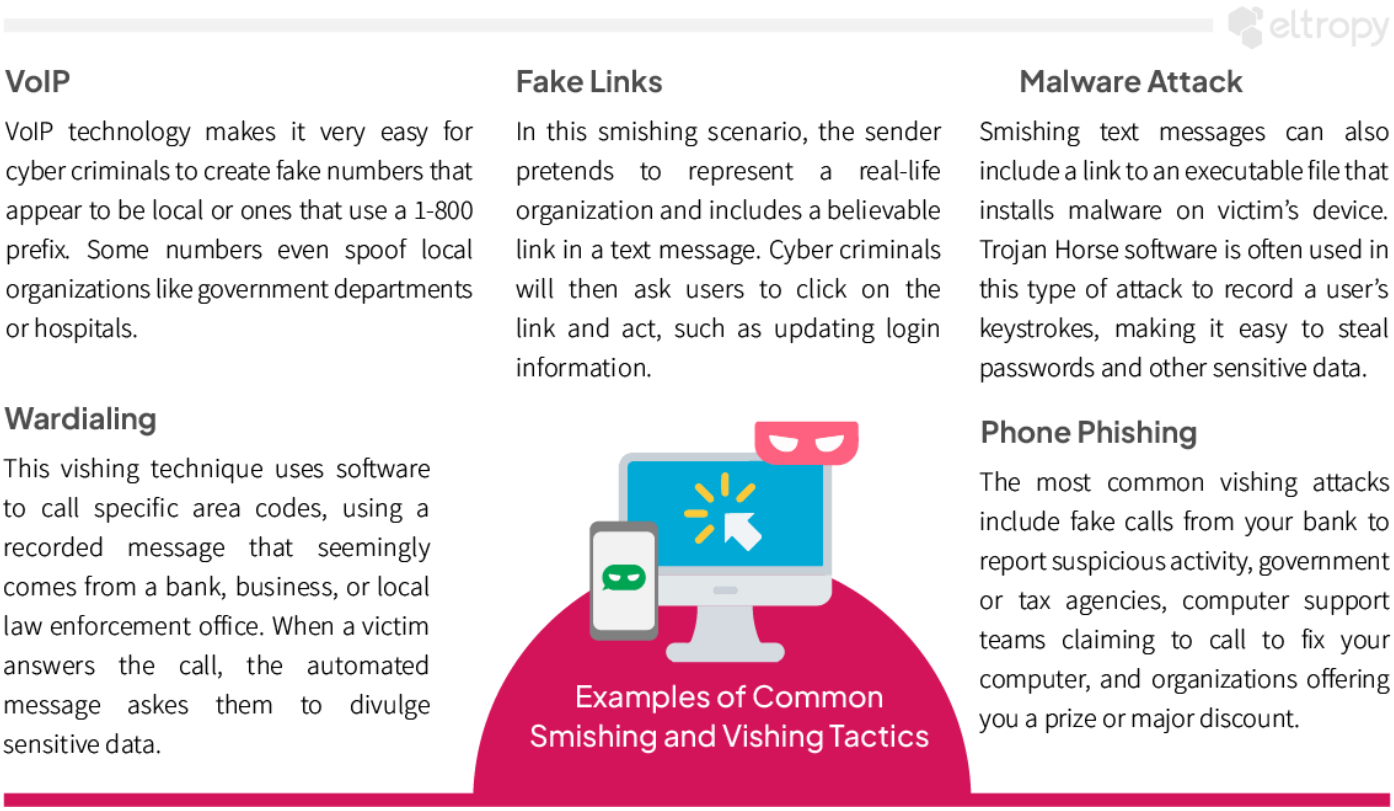
Targets a group of users and websites they normally visit. Security vulnerabilities are exploited to infect those websites with malware, which in turn will affect one or several members of the targeted group.

Baiting

Baiting is both an online and in-person social engineering tactic that relies on the human desire for reward. The attacker will promise the victim something tantalizing, like a prize, in exchange for their immediate action.

Phishing is an example of social engineering: a collection of techniques that scam artists use to manipulate human psychology. Social engineering techniques include forgery, misdirection, and lying—all of which can play a part in phishing attacks. On a basic level, phishing communication uses social engineering to encourage users to act without thinking things through.

While phishing is nothing new-phishing via phone calls is as old as phone-the scale and the effectiveness of phishing via Text channel is on the rise. As more and more financial institutions communicate to their customers via Text, fraudsters have adopted Texting as a channel of their choice for their phishing scams.



Smishing and Vishing are respectively Phishing via SMS and Voice.

See Appendix 1 for examples of phishing scams seen by actual Credit Unions.

To help your members not to fall for phishing scams, you need to proactively provide education and reminders to your customers and put safeguards in place like 2FA, ID Verification, Video Banking, etc (more of this below in the next section) to prevent fraudsters from using your customer

Here are the links to educational content on the website of some of the Credit Unions we have collected for your to review to help you formulate your own educational content.

Please ensure that you ask your members and customers to report the phishing issues here

How Eltropy Can Help?

While Eltropy supports sending SMS from as many numbers as you like, Eltropy suggests and assists our clients to use a limited number of vetted numbers (Short Code, Long Code, 10 DLC) to send Texts to their customers. Consider buying Vanity Short Codes so that they are easy for your members to remember. Using Skill-Based Routing, you can route the incoming replies to outbound Texts to the right teams from the limited numbers you use for outbound Texting.

Also, store marketing and other content in Eltropy or your website when you need to link to the content from your Text message. Never use bit.ly or some other URL Shortener services as they are frequently used by fraudsters.

Once you've standardized on a few numbers you send Text messages from and how you include URLs in Text messages, communicate to your members the numbers you will text from and the domains your URL will come from. Encourage your members to add those numbers to their phone contacts.

You can use Eltropy Texting APIs to send fraud alerts like unusual activity, known phishing attacks, etc, to customers immediately to prevent the scale of the financial damage.

Finally, use Eltropy Text Marketing capabilities to send educational Texts about phishing at least once a month. Create a series of educational Text campaigns and highlight different aspects of fraud prevention in each Text in the series and keep repeating the series. Consumers appreciate the proactive reach out on topics like fraud prevention.

To make sure all your customers are aware of potential scams prevalent in Texting, frequently educate the members about the same via email. See Appendix 2 for examples of emails you can send to your members to help them not fall for Text scams.

Inbound Contact Center Scams

Helping your members not fall for phishing scams can help reduce inbound contact center scams. If a phishing scam is successful, with verified account numbers and some basic information, a fraudster has all they need to execute fraud through the phone channel using convincing scripts involving the current crisis to socially engineer contact center agents and individuals.

Scammers are using new versions of old tactics to leverage times of uncertainty, fear, and heightened emotion to expose individuals and contact centers to an increase in fraud incidents.

Here are four categories of current fraud tactics to be on the lookout for, including examples of the most common "scripts" reported by contact center agents and fraud analysts around the country.

Travel-Related Inconveniences and Emergencies

Many of the most common scripts involve appeals for emergency financial assistance due to travel restrictions and guidelines set forth by the federal and state government. One narrative that we're hearing from a number of agents involves fraudsters claiming to be stuck outside the country. It sounds something like:

I left the country over a month ago and don't even know when I'm going to be allowed to come home. This is an emergency. I need you to wire me money because of the travel restrictions from this pandemic, or make an immediate ACH transfer, now.

There's typically a sense of urgency, as fraudsters are aware of the high call volumes that agents and analysts are currently contending with. Armed with the consumer data they've acquired from a vast increase in phishing scams, fraudsters are primed to scam the contact center and take advantage of agents who are attempting to assist people in genuine need.

Caretaker Fraud

What is an agent supposed to do when a scammer calls in frantically, asserting that a person they're caring for is in dire need of financial assistance to pay for emergency medical bills?

I'm calling on behalf of Mrs. Smith, who's in the hospital right now with complications due to COVID-19. She's isolated from her immediate family, who live out-of-state, and she has asked me to help her get access to the funds she badly needs for bills, rent, and everything else. I'm the only person she has access to and I'm the only one that can help her.

There has been a marked increase in fraudulent activity targeting the elderly. In an attempt to stay on top of important financial and health updates, seniors may inadvertently click on a scammer's link and make their private financial data and login credentials vulnerable, which fraudsters then use to gain access to their banks, insurance companies, mortgage lenders, credit card issuers, and more.

Send Me a New Card / Raise the Spending Limit

The current public health crisis has reverberated throughout financial markets, leading to an unprecedented number of unemployment claims in the past month, opening both individuals and FI's to the associated scams that prey on people's financial panic.

A red flag should go up for any direct requests for a new card or increased spending limit. Fraudsters aren't calling in to set up payment plans or request payment forbearances. Rather, they're attempting to scam the contact center with urgent messages about how the current pandemic has put them in a position where they need access to more of their money, and right now.

I lost my job due to all this craziness. At first, I worked from home but was laid off a month ago and I'm still waiting on the loan assistance and unemployment I filed for. I'm facing eviction, can't afford groceries, and need to feed my kids. I really need you to raise the spending limit on my card.

-or-

I'm quarantined at my parent's house in Michigan and all of my credit cards, not to mention everything else I own, are back at my apartment in New York. I need you to send me a new card. I was also furloughed, so please increase the limit on the card so I can bridge the gap until I receive unemployment.

Financial Surrogate Scams

Finally, fraudsters are targeting some of the largest financial institutions by gathering consumer data with mobile and email scams that claim an individual's account has been compromised. Unwitting people concerned about their financial security click on bad links, providing the sensitive information to fraudsters who turn around and use it to drain their bank accounts and max out their credit cards acting as financial surrogates.

I have legal power of attorney for Mr. Johnson, who is gravely ill and in no position to speak to anyone in person, let alone over the phone. He has medical bills to pay. Please wire money / make a direct ACH deposit into this other account.

Even as most people are rallying together to get through the current challenges facing our world, bad actors are attempting to exploit vulnerabilities and capitalize on the uncertainty of the time. Contact centers should be on alert as fraudsters continue to adapt their tricks and tactics, appeal to emotions, and convey urgency to carry out their scams.

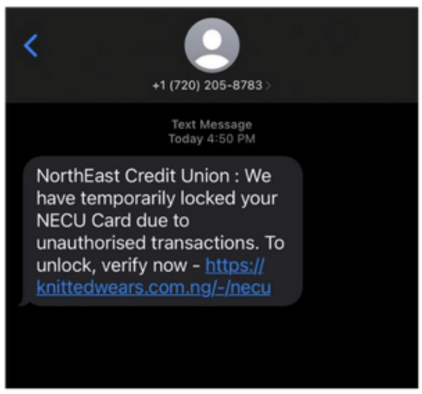
How Eltropy Can Help?

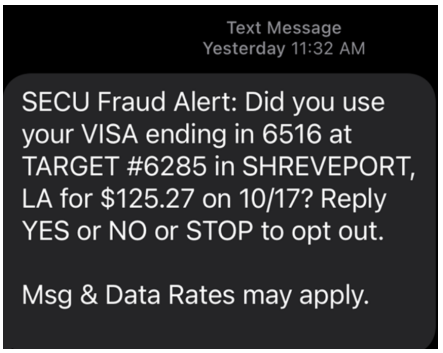
If you are using Eltropy Secure Chat or Texting for inbound communications from your members and customers, leverage 2FA (Two Factor Authentication) built into Eltropy. To verify the customer, send a verification code Text to their verified number in your Core system before providing any services. You can use Eltropy 2FA with direct calls and any number of channels and has been particularly successful in Contact Centers.

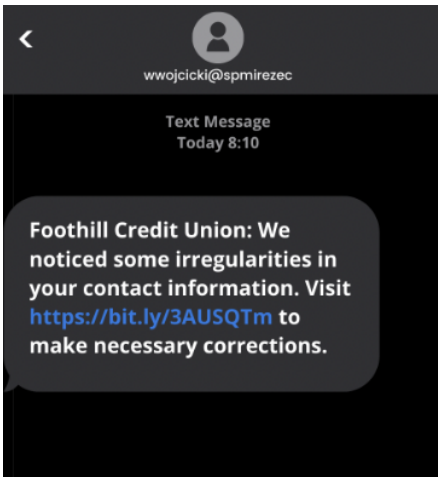
Eltropy also provides Real-Time ID Verification capabilities. Using public and private data sources, with Eltropy Real-Time ID Verification you can do Dynamic KBA and Photo ID verification before providing sensitive services via digital channels like Video, Chat & Text, or phone.

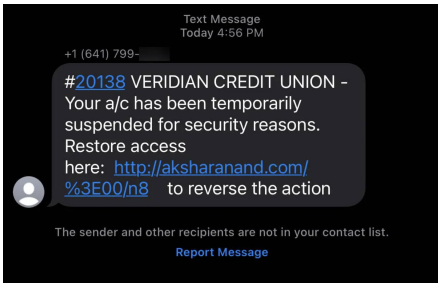
Eltropy Video is another strong fraud deterrent. Some Eltropy customers request remote Wire transfers to be conducted via video where robust KYC can occur. Using Video Banking can help cut down fraud dramatically.

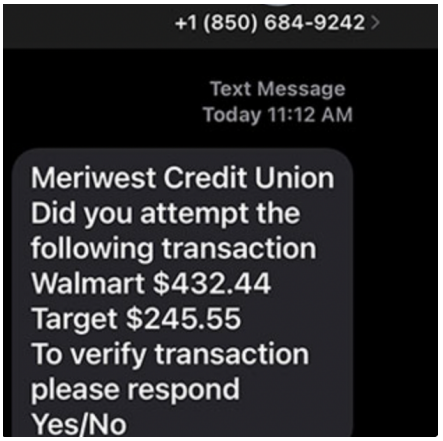
Appendix 1: Example of Phishing Scam











Appendix 2: Example of Education Emails

Sample Email 1: Inform members of new Text Communication Service

Subject: Stay Connected with Our New Text Communication Service

Dear <customer first name>,

We are excited to announce a new way for you to stay connected with your credit union – our text communication service. This service will allow us to quickly and easily send you important account updates, fraud alerts, promotional offers, and more, right to your mobile device.

To ensure you have the best experience possible, we wanted to provide you with some important information before we start texting you:

1. Opting in: If you would like to receive text messages from us, simply reply "YES" to this email or let us know at your next visit. If you change your mind in the future, you can opt-out at any time by replying "STOP" to any text message from us.
2. Fees: There is no charge from us to receive text messages, but your mobile carrier's message and data rates may apply.
3. Protecting Your Information: We take your privacy and security very seriously. Our text communication service will comply with all applicable laws and regulations, including the protection of your personal information.
4. Terms and Conditions: Our text communication service is governed by the terms and conditions of your overall agreement with us. Please let us know if you have any questions or concerns.

We are committed to providing you with the best possible service and look forward to staying connected with you through this new channel. If you have any questions, please do not hesitate to contact us.

Best regards,

[Your Credit Union Name]

Sample Email 2: Educate members of potential fraudulent Texts

Dear <customer first name>,

We are dedicated to protecting your financial information and ensuring your safety while using our text communication service. Unfortunately, fraudsters may try to impersonate financial institutions, including credit unions, and send fraudulent text messages in an attempt to obtain sensitive information or steal money.

To help you identify and protect yourself from fraudulent text messages, we would like to share the following tips with you:

1. Verify the sender: Make sure the text message is from a trusted source by verifying the sender's phone number. Our official phone number is [insert phone number].
2. Don't click on links: Fraudulent text messages may contain links to fake websites. Do not click on any links in a text message unless you are certain they are from a trusted source.
3. Don't respond with personal information: Never respond to a text message requesting personal information, such as your Social Security number, account numbers, passwords, or other sensitive information. We will never ask for this information via text message.
4. Report suspicious activity: If you receive a text message that you suspect is fraudulent, do not respond to it and report it to us immediately.

We hope these tips help you stay safe and secure while using our text communication service. If you have any questions or concerns, please don't hesitate to reach out to us.

Best regards,

[Your Credit Union Name]

Sample Email 3: Educate members about phishing scams

Subject: Protect Yourself from Phishing Scams

Dear <customer first name>,

At [Your Credit Union Name], the security of your personal and financial information is our top priority. Unfortunately, phishing scams are becoming more common and sophisticated, so it's important to be aware of the warning signs and know how to protect yourself.

Phishing is a type of scam where fraudsters send emails or text messages that appear to be from a trusted source, such as a financial institution, in order to trick you into revealing sensitive information or steal money.

Here are some tips to help you identify and avoid phishing scams:

1. Verify the sender: Be wary of emails or text messages that appear to be from a financial institution, government agency, or other trusted source, but have slight variations in the sender's email address or phone number.
2. Don't click on links: Don't click on any links in an email or text message unless you are certain they are from a trusted source.
3. Don't respond with personal information: Never respond to an email or text message that requests personal information, such as your Social Security number, account numbers, passwords, or other sensitive information.
4. Report suspicious activity: If you receive an email or text message that you suspect is a phishing scam, do not respond to it and report it to us immediately.

We are committed to protecting your financial information and keeping you informed about potential threats. If you have any questions or concerns, please don't hesitate to reach out to us.

Best regards,

[Your Credit Union Name]

Sample Email 4: Educate members how to protect themselves from different types of scams

Subject: Protect Yourself from Texting Scams

Dear <customer first name>,

At [Your Credit Union Name], the security of your personal and financial information is our top priority. Unfortunately, texting scams are becoming more common, so it's important to be aware of the different types and know how to protect yourself.

Here are some of the most common texting scams and tips to help you avoid falling victim:

1. Phishing scams: Fraudsters send text messages posing as a trusted source, such as a credit union, to trick you into revealing sensitive information or steal money. To avoid falling for this type of scam, always verify the sender's identity and never respond to a text message that requests personal or financial information.
2. Smishing scams: Similar to phishing scams, smishing scams use text messages to trick you into revealing sensitive information or steal money. To avoid falling for this type of scam, always be cautious of text messages from unknown numbers and never respond to a text message that requests personal or financial information.
3. Premium texting scams: Fraudsters send text messages offering a free service or prize, but then charge a fee for continued use. To avoid falling for this type of scam, never respond to text messages that offer free services or prizes and always read the fine print before agreeing to any charges.
4. Debt collection scams: Fraudsters send text messages posing as debt collectors and demand immediate payment for a supposed debt. To avoid falling for this type of scam, always verify the identity of the sender and never provide personal or financial information over text message.
5. Charity scams: Fraudsters send text messages requesting donations to fake charities. To avoid falling for this type of scam, always verify the identity of the charity before making a donation and never provide personal or financial information over text message.

We hope these tips help you stay safe and secure while using your mobile device. If you have any questions or concerns, please don't hesitate to reach out to us.

Best regards,

[Your Credit Union Name]