InfoSight Newsletter

November 10th, 2023 | Volume 17 | Issue 43

League InfoSight Highlight:
Internal Spoofing Attacks are on the Rise - Is Your Staff Prepared?

Spoofing is a scam where cybercriminals impersonate a company with a fake email address, display name, text message, or website URL to convince a target that they are a trusted, well-known source from the company. It can be as simple as changing one letter, symbol, or number in a communication that is difficult to spot. The benefit of spoofing for cybercriminals is that the person will likely disclose financial and personal information, download malware, wire funds, and more.

Types of spoofing attacks:

- **Email Spoofing:** This technique is one of the most common types where cybercriminals send an email posing as a trusted source. They usually ask for an urgent request or attempt to lure the target to click a malicious link or attachment.
- **Domain or Website Spoofing:** These attacks aim to lure users into logging into their accounts on fake websites or exposing other personal information about themselves. The cybercriminals can then use the stolen credentials to log into the actual account on the real website.
- **Caller ID Spoofing:** Similar to email spoofing, caller ID alters the phone number to show up as someone familiar to the target they are calling. For example, the fraudster may pose as a customer service representative from the target's bank and attempt to gather personal information like their banking credentials, social security number, etc. in order to gain access to their account.
- **Text Message Spoofing:** This technique targets a person via text message posing as a trusted source like their bank or a friend. They substitute the sender ID with a recognizable source and use the text message as a springboard for data theft, spear phishing, and scams.

The reality is that credit unions are being targeted, as well as employees. Implementing a Proactive Security Awareness Program aims to empower users with skills to identify and report suspicious activity, including emails, texts, or website links. People are the first line of defense for the credit union, and when equipped with cybersecurity awareness, it will only propel their security posture.

The following tips can help identify a spoofed message in the email headers:

- **Identify that the 'From' email address matches the display name.** The from address may look legitimate at first glance, but a closer look in the email headers may reveal that the email address associated with the display name is actually coming from someone else.
- **Make sure the 'Reply-To' header matches the source.** This is typically hidden from the recipient when receiving the message and is often overlooked when responding to the message. If the reply-to address does not match the sender or the site that they claim to be representing, there is a good chance that it is forged.

Question the Content of the Message

Sometimes the best defense against phishing is to trust your instincts. If you receive a message from a supposed known source that appears out of the ordinary, it should raise a red flag. When receiving an unsolicited message, users should always question the content of the message, especially if the message is requesting unusual information or directing the user to click on links or open attachments.

Before responding to any questionable message, perform the following tasks to ensure the message is reliable.

- **Ask yourself:**
  - Was I expecting this message?
  - Does this email make sense?
  - Am I being pushed to act quickly?
- **Examine the email and look for:**
  - Sense of urgency
  - Unsolicited request of personal information
  - Generic greeting/signature
  - Unfamiliar links or attachments
- **Contact the sender of the message through a trusted channel**
  - If the email appears legitimate, but still seems suspicious, it is best to contact the supposed sender through a trusted phone number or open a new outgoing email message using their

real email address found in the address book. Do not reply to the message in question.

It is important to always remain vigilant when receiving mail whether it is from an unknown sender, someone you are close with, and sometimes even when it is someone you are familiar with within your organization. Cyber scammers are always looking for new ways to exploit individuals for their own personal gain.

We are seeing an increase in criminal activity where individuals are targeting credit union employee's email addresses inside and outside of the credit union. Do you have procedures in place if one of your employees receives an email requesting a monetary transaction from management? Now is the perfect time to add Spoofing to your training plan for 2024!

**This article is courtesy of the League of Southeastern Credit Unions & Affiliates*

News and Alerts!

CFPB Proposes New Federal Oversight of Big Tech Companies and Other Providers of Digital Wallets and Payment Apps

The Consumer Financial Protection Bureau (CFPB) is proposing to supervise larger nonbank companies that offer services like digital wallets and payment apps. The rule proposed today would ensure that these nonbank financial companies – specifically those larger companies handling more than 5 million transactions per year – adhere to the same rules as large banks, credit unions, and other financial institutions already supervised by the CFPB.

Read More

CFPB Issues New Report on State Community Reinvestment Laws

The Consumer Financial Protection Bureau (CFPB) published a new analysis on state Community Reinvestment Act laws, highlighting how states ensure financial institutions' lending, services, and investment activities meet the credit needs of their communities.

Read More

NCUA’s Hood Lauds Growth of DEI Summit and Industry Progress

At the National Credit Union Administration’s 2023 Diversity, Equity, and Inclusion Summit, Board Member Rodney E. Hood celebrated the significant evolution of the event and the ongoing commitment of the credit union community to DEI principles.

Read More

The Second/Third issue of the "Consumer Compliance Outlook" from the Federal Reserve System has been released

Consumer Compliance Outlook is a publication from the Federal Reserve system. The most recent issue includes the following articles:

- Top Federal Reserve Compliance Violations in 2022
- Compliance Risk Assessments
- Compliance Spotlight: Supervisory Observations on Representment Fees

Read More

FinCEN Finalizes Rule on Use of FinCEN Identifiers in Beneficial Ownership Information

The Financial Crimes Enforcement Network (FinCEN) is issuing a final rule that specifies the circumstances in which a reporting company may report an entity’s FinCEN identifier in lieu of information about an individual beneficial owner.

A FinCEN identifier is a unique number that FinCEN will issue upon request after receiving required information. Although there is no requirement to obtain a FinCEN identifier, doing so can simplify the reporting process and allows entities or individuals to provide the required identifying information directly to FinCEN.

Read More

Questions, Comments, Concerns? We are here to help! Email us at **info@leagueinfosight.com**