Commercial Services Security Newsletter

June 2024 | CSN – Q2 - 2024

Is Your Business Prepared for Social Engineering?

Summary

The Federal Bureau of Investigation (FBI) recently announced that individuals and businesses should be aware of social engineering techniques used by cyber criminals to gain access to financial, corporate, and network accounts. As described below, recently observed social engineering techniques are being used by cyber criminals to target victims. Obtaining personal information through these techniques gives cyber criminals the ability to invade a victim's network, steal a victim's data, and extort victims by threatening to release private data.

Social Engineering Stats:

- Social engineering accounts for 98% of all cyber attacks. (Statista)
- Data breaches initiated through social engineering techniques averaged costs over $4.5 million. (IBM)
- The most common vector in the 2022 report was stolen credentials, but phishing took the lead by a small margin over stolen credentials. (IBM)
- Smishing (SMS Phishing) attacks target 76% of global businesses. (Statista)

Social Engineering Tactics, Techniques, and Procedures

Impersonating Employees

Impersonating employees is a technique in which cyber criminals obtain credentials, pose as company employees, and contact IT and/or helpdesk staff to update employee login information, and gain access to a company's network.

SIM Swapping

SIM swapping is a technique in which cyber criminals contact a victim's mobile carrier and convince the mobile carrier to transfer the victim's mobile phone number to the cyber criminal's SIM card. In other words, the victim's mobile phone number is transferred by the mobile carrier to a physical device in the cyber criminal's control. This transfer request may be made in person at the mobile carrier's retail store or by calling the mobile carrier's customer service line.

To transfer the mobile phone number, the cyber criminal must provide personal identifying information and must answer security questions from the mobile carrier to confirm the account holder's (i.e., the victim's) identity. By gaining access to the victim's phone number, the cyber criminal can potentially bypass multi-factor authentication that is set up to protect a victim's online financial and other network accounts. That means the cyber criminal may be able to access the victim's accounts and then steal funds and/or other personal data from those accounts. For more information on SIM Swapping, please see PSA Alert I-020822-PSA: Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from the US Public.

Call Forwarding and Simultaneous Ring

Call forwarding is a technique in which cyber criminals contact a victim's mobile carrier to forward the victim's mobile phone number to the cyber criminal's phone number. Cyber criminals may also deceive the

mobile carrier to set up the simultaneous ring function to enable the cyber criminal's phone to be reached when a victim's phone number is dialed. Call forwarding and simultaneous ring features may be enabled by contacting the mobile carrier or by dialing a code that begins with an asterisk (*) from the victim's phone. These features may allow cyber criminals to bypass multi-factor authentication, similar to the SIM swapping scheme described above.

Phishing Campaigns

Phishing is a type of social engineering in which cyber criminals pose as a trusted institution (bank, employer, etc.) or as the employer's VPN portal to solicit victim information and login credentials. For example, the criminal may send an email that appears to be from the victim's phone company asking the victim to click a link to update account information or may direct the victim to a new employer portal to access a corporate intranet. After clicking the link, the criminal will collect any personal information entered (i.e., employer credentials, birthday, SSN, account number, password, answers to security questions, etc.). For more information on phishing, please see the Multi-State Information Sharing and Analysis Center (MS-ISAC) publication, Phishing Guidance: Stopping the Attack Cycle at Phase One, and Cybersecurity and Infrastructure Security Agency Publication, Implementing Phishing-Resistant MFA.

Tips On How to Protect Yourself

The FBI recommends individuals take the following precautions:

- Do not reply to calls, emails, or text messages that request personal information, such as your password, PIN, or any one-time password sent to your email or phone. If someone claiming to be a company "representative" contacts you and asks you to provide personal information or to verify your account by providing a code, initiate a new call to that company by dialing the verified customer service line of the company.
- Reach out to your mobile carrier to disable or block SIM card changes, Call Forwarding, and Simultaneous Ring.
- Ensure that you have set a unique password for your voicemail on your mobile phone.
- Regularly review your mobile phone provider's account page to monitor account login history or any changes made.
- Avoid posting personal information online, such as mobile phone numbers, addresses, or other personal identifying information.
- Use "strong" passwords that are unique and random, contain at least sixteen characters, and are no more than 64 characters in length. Avoid reusing passwords and disable password "hints."

The FBI recommends companies take the following precautions:

- Add an email banner to emails received from outside your organization. For example, label emails received from outside of your organization as "EXTERNAL EMAIL."

- Consider disabling or blocking SIM changes and Call Forwarding for employee equipment.
- Monitor accounts for suspicious login attempts or compromised credentials and implement multiple failed login attempt account lockouts.
- Refine multi-factor authentication (MFA):
  - Do not use email-based MFA.
  - Monitor privileged logins for unusual activity.
  - For bring your own device (BYOD) equipment, require MFA enrollment.
- Prevent employees from logging in using anonymous virtual private network (VPN) services.
- Educate help desk and customer support staff about social engineering and phishing schemes used by cyber criminals. Education should include but not be limited to:
  - Regular training using real phishing examples from current high-profile threat groups, such as Scattered Spider.
  - Immediate reporting protocols of suspicious messages and interactions to abuse teams.
  - How to authenticate calls from third-party authorized retailers requesting customer information.

If You Think You've Been Scammed

- Contact [YOUR INSTITUTION NAME HERE] immediately so we can act and provide recommendations
- Report suspicious activity to the Internet Crime Center, www.ic3.com, and/or your local law enforcement agency.

