Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-041124-PSA
April 11, 2024

Cyber Criminals Target Victims Using Social Engineering Techniques

The Federal Bureau of Investigation (FBI) is issuing this announcement to inform individuals and businesses about social engineering techniques used by cybercriminals to gain access to financial, corporate, and network accounts. As described in detail below, recently observed social engineering techniques used by cybercriminals to target victims include:

1. impersonating employees,
2. subscriber identity module (SIM) swap attacks,
3. call forwarding and simultaneous ring; and,
4. phishing.

Obtaining personal information through these techniques gives cybercriminals the ability to invade a victim's network, steal victim data, and extort victims by threatening to release private data.

SOCIAL ENGINEERING TECHNIQUES

Impersonating Employees
Impersonating employees is a technique in which cybercriminals 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 cybercriminals will contact a victim's mobile carrier and convince the mobile carrier to transfer the victim's mobile phone number to the cybercriminal's SIM card. In other words, the victim's mobile phone number is transferred by the mobile carrier to a physical device in the cybercriminal's control. This transfer request may be done 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 cybercriminal 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 cybercriminal can potentially bypass multi-factor authentication that is set up to protect a victim's online financial and other network accounts. That means the cybercriminal 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 US Public.

Call Forwarding and Simultaneous Ring
Call Forwarding is a technique in which cybercriminals will contact a victim's mobile carrier to forward the victim's mobile phone number to the cybercriminal's phone number. Cybercriminals may also set up via the mobile carrier the Simultaneous Ring function to enable multiple phones 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 from the handset of a phone that begins with an asterisk (*). These features may allow cybercriminals to bypass multi-factor authentication, similar to the SIM Swapping scheme described above.

Phishing Campaigns
Phishing is a type of social engineering in which cybercriminals 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, please initiate a new call to that company by dialing the verified customer service line of the company.
- Ensure that you have set a unique password for your voicemail on your mobile phone.
- Reach out to your mobile carrier to disable or block SIM card changes, Call Forwarding, and Simultaneous Ring.
- 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 number, address, or other personal identifying information.
- Use "strong" passwords that are unique and random, that 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[1], 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.[2]
- Prevent employees from logging in using anonymous virtual private network (VPN) services.[3]
- Educate help desk and customer support staff about social engineering and phishing schemes used by cybercriminals. Education should include but not be limited to:
    - Regular training using real phishing examples from current high profile threat groups, such as Scattered Spider.[4]
    - Immediate reporting protocols of suspicious messages and interactions to abuse teams.[5]
- Authenticate calls from third party authorized retailers requesting customer information.

VICTIM REPORTING AND ADDITIONAL INFORMATION

If you suspect that you are a victim of social engineering, and your personal information has been compromised:

- Contact your account providers immediately to regain control of your accounts, change passwords, and place alerts on your accounts for suspicious login attempts and/or transactions.
- Report the activity in as much detail as possible to the FBI's Internet Crime Complaint Center at www.ic3.gov

---

[1] (U) FS-ISAC | (U) "Scattered Spider & BlackCat Ransomware: Mitigation Guidance" | November 2023 | https://www.fsisac.com/knowledge ↩

[2] (U) FS-ISAC | (U) "Scattered Spider & BlackCat Ransomware: Mitigation Guidance" | November 2023 | https://www.fsisac.com/knowledge ↩

[3] (U) FS-ISAC | (U) "Scattered Spider & BlackCat Ransomware: Mitigation Guidance" | November 2023 | https://www.fsisac.com/knowledge ↩

[4] For additional information regarding Scattered Spider tools, techniques, and procedures (TTPs), see the FBI and CISA's Joint Cybersecurity Advisory on Scattered Spider. ↩

[5] (U) FS-ISAC | (U) "Scattered Spider & BlackCat Ransomware: Mitigation Guidance" | November 2023 | https://www.fsisac.com/knowledge ↩