Serianu Cyber Security Advisory

Social Engineering Attack: Mobile Banking

Serianu SOC Advisory Number:

TA – 2020/006

Date(s) issued:

7th August 2020

OVERVIEW:

Serianu research team has identified an increasing number of social engineering attacks within organisations. According to the research, attacks frequently take place over phone and via phishing emails. Humans who are the weakest link in the information security chain remain susceptible to manipulation by social engineers.

In social engineering attacks, scammers impersonate trusted officials, like customer service, representatives at a bank, into giving up confidential information. Financial institutions in particular, are at a heightened risk of social engineering attacks. Top techniques include phishing to harvest bank account information and voice scams that trick customers into making authorized, yet fraudulent transactions.

This advisory provides an in-depth research on the social engineering attacks, detection strategies, and prevention procedures.

Credential and Personal Information Harvesting

1. **Phishing**

Phishing is the most common form of social engineering attack. Attackers disguise false communications to appear as though they are coming from a legitimate source. Victims may then click a false link and install malware on their device or enter in personal information, such as credit card information that the hackers then steal. Some of the top targets for phishing attacks are popular payment providers and financial institutions.

2. **Vishing**

Vishing, or phone based phishing is a common type of credential or personal information harvesting. The scammer will impersonate as an IT professional, a tech support claiming that something is wrong, or your account has expired. The fraudsters will then ask for information to verify your account and then additional information to be able to fix the situation, whether personal information, credit card information or credentials.

3. **Smishing**

Smishing, or SMS phishing, is an emerging form of social engineering attack that cyber criminals are using to target victims on their smartphones. In smishing, fraudsters use text messaging to trick users into giving out confidential information or to download malware or a virus onto their phone. Fraudsters are also using smishing to bypass two-factor authentication and multi-factor authentication (MFA).

Real Time Social Engineering Scams

1. **Voice Scams**

Fraudsters represent themselves as legitimate representatives of a bank or other organization in order to trick users into making a transaction or money transfer. Social engineers rely on elaborate and very clever scripts to gain people's confidence and trust so they willingly disclose confidential information.

After convincing a victim of the urgent need to move funds, the victim then logs into their account. Under the guidance of the fraudster, the user initiates a transfer, following instructions to enter details like payee, payment amount, and more. Once complete, the victim completes a fully authorized transfer that goes undetected by fraud tools. Once sent to the scammer's account, funds are nearly always irretrievable.

2. **Remote Access Tools (RAT) Attacks**

In this form of social engineering, the scammer will convince the user to install a remote access tool to allow the scammer to take control and act on their behalf. For example, the scammer will pose as an IT or tech support company or as the financial institution, and ask the user to give them control so they can perform operations on their behalf. Once the user is convinced to give control to the scammer, the scammer will quickly take over an online banking session and transfer funds to malicious accounts.

Several instances have occurred wherein people receive phone calls that appear to be from their bank. The caller usually pretends to be a bank representative or someone from the bank's technical team. In most cases, the caller sounds professional and provides a convincing reason for calling the customer. After giving a false sense of security, the caller then tricks the victim into giving away their personal and confidential data such as:

- One-Time-Password (OTP)
- ATM PIN
- Credit or debit card number
- The card's CVV number [Card Verification Value – 3 to 4-digit number printed on the flip side of the card]
- Expiry date
- Secure password
- Mobile Banking login ID and password and other personal information

With all such crucial information at hand, the fraudster can easily carry out illegal financial transactions using the victim's name.

Prevention Measures

1. Never respond to emails, embedded links, calls asking you to update or verify User ID, Password, Debit Card Number or PIN. Inform your bank about such email, SMS or phone call. Immediately change your passwords if you have accidentally revealed your credentials.
2. Do not provide any personal or confidential information on a page which might have come up as a pop-up window.
3. Always remember that information like password, PIN are strictly confidential and are not known even to employees or service personnel of the bank.
4. Never provide your identity proof to anyone without any genuine reason.
5. Never click on any links in any e-mail to access the bank's site.
6. Access your bank website only by typing the URL in address bar of browser.
7. Avoid opening attachment of emails from unknown senders.
8. Avoid accessing Internet banking accounts from cyber cafes or shared PCs.
9. When on your bank website, look for the padlock symbol either in the address bar or the status bar (mostly in the address bar) but not within the web page display area. Verify the security certificate by clicking on the padlock.
10. Keep your system up to date.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organisation or individual that has access to social engineering related attacks to share it with us through our email: info@serianu.com to allow us analyze.