Team number: T67

Team members: Kaiwen Chen (kach8084@colorado.edu), Qiuyang Fu (qifu3807@colorado.edu)

While writing your project you should also think about and carefully use terms like "vulnerability, threat, asset, risk, attack, etc."

1. **(5 points) In 2-3 sentences, explain what your event was about at a conceptual level. In this, explain how it relates to cybersecurity.**

Answer: The event demonstrates how hackers are able to hijack phone lines and bypass two-factor-authentication (2FA) and eventually take over the accounts easily by breaching weak security methods. It relates to cybersecurity since criminals take advantage of the weak protections and crack online banking or high-value accounts.

2. **(5 points) In 2-3 sentences, explain some of the technical details of your event.**

Answer: The type of attack in the simply starts with phishing personal information often via SMS phishing, once the information is confirmed, fraudsters call the victim's mobile carriers and ask the customer service to port the lines to different SIM devices. The vulnerability of the two-factor-authentication process is that the verification processes are way too weak, and more importantly, many carriers don't ask in-depth security questions. It leads to a problem which the fraudsters can just simply tell the company that they forgot the information and request to reset those data, and finally the access to the accounts is gained.

3. **(5 points) What is the most interesting thing you took away from reading about your article?**

Answer: It's interesting that I never expected mobile carriers are so careless in the verification process, and its strength is as vulnerable as a piece of paper. I can relate this to my personal experience: a few days ago I lost my AT&T SIM card so I went to the local store to get a new one, the staff didn't even ask me for my ID they just simply asked my phone number and I got my card within 50 seconds as I walked into the store. People nowadays don't realize that the significance of cybersecurity plays an important role in modern society, a certain degree of defense can make a huge difference; they might save millions of dollars if they protect them well enough.

4. **(5 points) Analyze some impacts from your event on each of the CIA triad in 1-2 sentences each.**

a. Confidentiality: In the process of transferring the SIM card, the customer service representative might leak the user's account information before verifying the identity, causing the caller (or possibly an attacker) to pass the identity verification easily.

b. Integrity: When fraudsters use their device to control the line, they can use the 2FA text code they intercepted to manipulate the account without the victim's knowledge.

c. Availability: Because it is difficult for the mobile carrier to verify the true identity of the caller, fraudsters can easily transfer the victim's line and intercept their 2FA text code.

5. **(5 points) Pick 3 common design principles and explain the impact on your event in 1-2 sentences each.**

    1. **Fail-safe defaults:** The caller can complete the authentication successfully by answering one question, although other security questions cannot be answered correctly. The mobile carrier should terminate the transaction if the caller cannot answer the security question or can only answer one when performing caller authentication
    2. **Defense in depth:** Most mobile carriers do not have in-depth and challenging security questions for callers so that fraudsters easily control the lines of real users.
    3. **Least Privilege:** If the caller says that he has forgotten the information, the carrier will also give prompts to help the caller (attacker) find the correct information. Customer service representatives are not supposed to provide clues and leak account information.

Sources cited:

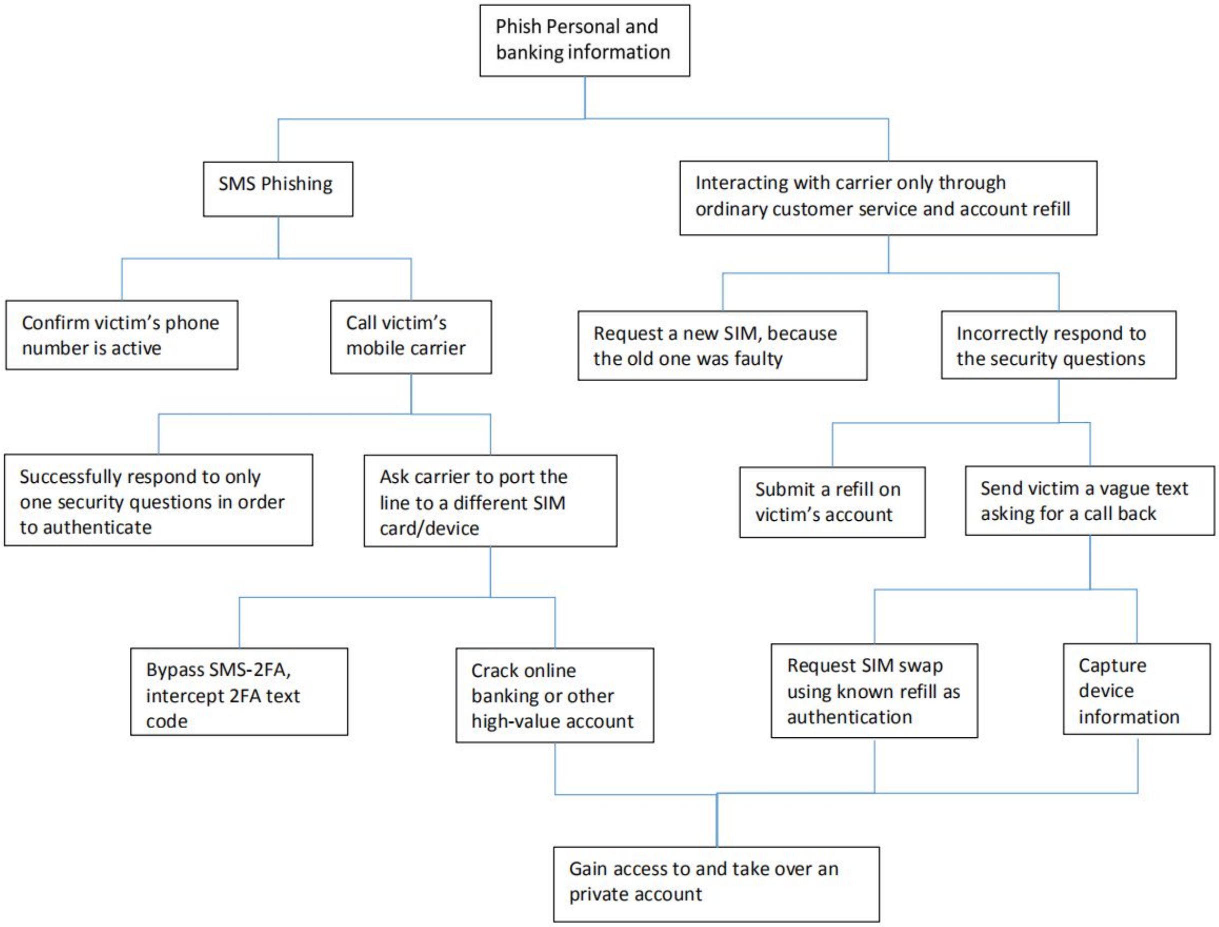
https://threatpost.com/mobile-customer-service-sim-swap-fraud/151993/

https://www.cnbc.com/2019/01/04/how-secure-is-your-account-two-factor-authentication-may-be-hackable.html

https://www.idtheftcenter.org/fbi-warns-of-hackers-bypassing-some-types-of-two-factor-authentication/

Contribution: Qiuyang completed the first half part of the questions, and Kaiwen completed the final half. We did the research together and came up with the topic that we are both interested in. As for the Attack Tree, Qiuyang designed the graph, Kaiwen helped double-check the work and hence significantly improved the quality.

Attack Tree:


Phish Personal and banking information
SMS Phishing
Interacting with carrier only through ordinary customer service and account refill
Confirm victim's phone number is active
Call victim's mobile carrier
Request a new SIM, because the old one was faulty
Incorrectly respond to the security questions
Successfully respond to only one security questions in order to authenticate
Ask carrier to port the line to a different SIM card/device
Submit a refill on victim's account
Send victim a vague text asking for a call back
Bypass SMS-2FA, intercept 2FA text code
Crack online banking or other high-value account
Request SIM swap using known refill as authentication
Capture device information
Gain access to and take over an private account