ICS2O/3C/4C Case Study C.4 – SIM Swap Fraud Name:

Read the following articles:

· <https://www.digitaltrends.com/mobile/sim-swap-fraud-explained/>

· <https://www.itworldcanada.com/article/warning-protect-your-mobile-phone-numbers-from-being-hijacked/396018>

· <https://www.wired.com/story/sim-swap-attack-defend-phone/>

Questions:

1. What is a SIM card?

A cell phone SIM card stores user data in [GSM](http://gsma.com/) (Global System for Mobile) phones.

2. Why is a SIM card required for your phone to work?

They’re principally used to authenticate cellphone subscriptions — without a SIM card, GSM phones aren’t able to tap into any mobile network.

3. What is “[text-based two-factor authentication](https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication)” ?

The idea of two-factor authentication, he points out, is to test someone's identity based on something they know (like a password) and something they have (like their phone or another device.)

4. How is two-factor authentication related to your phone?

"It’s depending on your mobile phone as a means of authentication [in a way] that can be socially engineered out of your control."

5. How is two-factor authentication related to your SIM card?

Earlier this month, Black Lives Matter activist DeRay McKesson [found that his Twitter account was hacked](https://www.wired.com/2016/06/deray-twitter-hack-2-factor-isnt-enough/) to tweet pro-Donald Trump messages, despite having two-factor authentication in place. The hackers, as he tells it, had called up Verizon, impersonated him, and convinced the company to redirect his text messages to a different SIM card, intercepting his one-time login codes.

6. List some of the services criminals can access if they get control of your SIM card.

a. Banking & Financial

Apple or Google Play Store, Amazon, Netflix

b. Social Media

Facebook, Twitter, Instagram, Snapchat, YouTube

7. Explain how criminals can get control of your SIM card.

a. Collecting Personal Information

Laying the groundwork for a SIM swap scheme involves collecting as much information about the victim as possible. Fraudsters might send phishing mail — messages that impersonate legitimate businesses like credit card companies and health insurers — intended to fool victims into forking over their legal names, dates of birth, addresses, and phone numbers.

b. Create False Identity

They call the victim’s cell phone provider and claim that his or her SIM card has been lost or damaged. Most cell phone service providers won’t acquiesce to those requests unless callers answers security questions, but SIM fraudsters come prepared, using the personal data they’ve collected from across the web to defeat the carrier’s security checks without raising any alarms.

c. Requesting a new SIM card

They ask the customer service representative activate a SIM card or number in their possession.

8. What are some signs of SIM swap fraud?

Most victims discover they’ve been compromised when they try to place a call or text.

9. How can you prevent SIM swap fraud?

a. What are some general methods

b. Who is your Canadian phone company / carrier?

c. What do they offer regarding SIM swap fraud prevention?

1. “There are multiple organizational and technical ways to combat SIM fraud — from introducing user alerting and additional checks for SIM reissuing to sharing knowledge of SIM swap activity between banks and phone companies,” Mohan-Satta said. “Banks can also consider looking for behavioral changes through behavioral analysis technology that can indicate a compromised device. This information may then be used by a bank to avoid sending SMS passwords to compromised devices and as an early way to alert the genuine customer.” Some institutions call customers to determine whether they got a new SIM card or alert them that someone is potentially impersonating them.
2. I do not have a phone, therefore I don’t have a carrier.
3. Again, I don’t own a phone.