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 smart card inside a mobile phone, carrying an identification number unique to the owner, storing personal data, and preventing operation if removed.

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

SIM cards are the small cards which contains a chip that must be inserted into GSM phones before they will work. Without a SIM card, a GSM phone won't be able to tap into any mobile network. ... Once activated, a CDMA phone is tied directly to that particular carrier's network.

3. What is “text-based two-factor authentication” ?

Apps like Google Authenticator and Authy give you that extra layer of security like SMS-based two-factor does, but they also tie it to your physical device rather than the number the phone company assigned to you. They show you a six-digit code that updates every 30 seconds or so, and stays in constant sync with whatever service you connect them to.

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

If a hacker has a phone number that’s associated with some of your online accounts, they can sometimes circumvent two-factor requirements altogether—which gets back to the problem of using phone numbers as identifiers in the first place. Disentangling yourself from those seven digits is hard to do at scale, but it’s worth at least trying on especially sensitive accounts, or if you might be a high-value target.

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

At its most basic level, a SIM swap is when someone convinces your carrier to switch your phone number over to a SIM card they own. They’re not doing it for prank call cover, or to rack up long-distance charges. By diverting your incoming messages, scammers can easily complete the text-based two-factor authentication checks that protect your most sensitive accounts. Or, if you don’t have two-factor set up in the first place, they can use your phone number to trick services into coughing up your passwords.

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

a. Banking & Financial

b. Social Media

If you haven’t experienced SIM swap fraud, count yourself lucky. It’s a relatively new, sophisticated form of fraud that allows hackers to gain access to bank accounts, credit card numbers, and other personal data. It’s tough to spot, and even tougher to undo the resulting damage.

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

a. Collecting Personal Information

b. Create False Identity

c. Requesting a new SIM card

1st step: Through social engineering and phishing scams, criminals gather as much information from a potential victim as they can. They browse through social media posts, use search engines or engage victims in online chats in hopes of acquiring details that can be used for security questions (i.e. mother's maiden name, name of first pet, etc.).

Criminals can also use keylogging or spying malware or buy personal information databases from the Dark Web.

2nd step: With the personal information gathered, the fraudster will contact the victim's cellphone carrier and claim that their phone has been lost, damaged or stolen and they need to activate a new phone with a fresh SIM card. If they successfully pass the carrier's identity checks by answering the security questions, the old SIM card is deactivated and the SIM card in the criminal's hands is activated. All of the victim's calls and texts are now received on the criminal's phone.

Once the victim's SIM card is deactivated, their phone, of course, will stop working, usually with a "No Service" warning. This is the first warning flag you'll have to watch out for.

3rd step: The criminals then attempt to claim the victim's online banking account, again using the personal information gathered, but this time, they will also use the victim's phone number for two-factor authentication codes. With this crucial window of opportunity, they start changing profile settings then add and set up withdrawal accounts.

4th step: With these additional accounts set up, the criminals start draining the victim's bank account. The banks will ask for confirmation via two-factor authentications via text messages to your phone number, which unfortunately, is still under the criminal's control. At this point, it's game over.

8. What are some signs of SIM swap fraud?

It’s tough to detect SIM card fraud before it happens. Most victims discover they’ve been compromised when they try to place a call or text. Once the perpetrators deactivate a SIM, messages and calls won’t go through. But some banks and carriers have instituted protections that prevent SIM swap fraud before it happens. “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.”

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?

Major carriers in the U.S. offer security that can help protect against SIM card swapping.

AT&T has “extra security,” a feature that requires you provide a passcode for any online or phone interactions with an AT&T customer representative. You can turn it on by logging into AT&T’s web dashboard or the myAT&T app.

Sprint asks customers to set a PIN and security questions when they establish service.

T-Mobile lets subscribers create a “care password,” which it’ll require when they contact T-Mobile customer service by phone. You can set one up by visiting a T-Mobile store or by calling customer care.

Verizon allows customers to set an account PIN, which they can do by editing their profile in their online account, calling customer service, or visiting a Verizon store.