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/>
* <https://krebsonsecurity.com/2015/11/talktalk-script-kids-the-quest-for-og/>

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.

1. 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.

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

Two-factor authentication (also known as 2FA) is a type, or subset, of multi-factor authentication. It is a method of confirming users' claimed identities by using a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are.

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

Set up two-factor authentication for your Apple ID. Two-factor authentication is available to iCloud and iTunes users with at least one device that's using the latestiOS or macOS. You can follow these steps on your iPhone, iPad, or iPod touch to turn on two-factor authentication.

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

When you activate two-factor authentication for a website or a service, you generally provide your mobile phone number. (You can also use an app, but the phone is the most common method of using two-factor authentication.) Most forms of two-factor authentication ask you to sign in with your user name and password, and then enter a code that is sent to you via SMS. This method not only proves that you know something (the user name and password), but also that you have something (the mobile phone), which you have “registered” as a device to receive these codes.

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

* 1. Banking & Financial

Once they’ve gained unfettered access to a victim’s phone number, criminals target bank accounts.“The attacker can read your SMS messages and see who you’re chatting with and what about,” Blaich said. “Many banks will send you a code to log into an account or reset a password to a mobile phone via SMS, which means an attacker committing SIM fraud can request and receive the code and access your bank.”Next, SIM fraudsters mask money withdrawals using a parallel system. They create a second bank account under the victim’s name (banks where the victim is already a customer have fewer security checks). When the criminals execute a transfer between the two accounts, it appears to the bank’s computer system as though the victim is transferring funds between two parallel accounts.

* 1. Social Media

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](https://www.wired.com/2016/06/hey-stop-using-texts-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.

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

* 1. 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.

* 1. Create False Identity

Once SIM criminals have gathered enough information on a target, they create a false identity. First, they call the victim’s cellphone provider and claim that his or her SIM card has been lost or damaged. Then, they ask the customer service representative activate a SIM card or number in their possession.

* 1. Requesting a new SIM card

Hackers request a new sim card with a fake identity to lock you out of the system.

Some institutions call customers to determine whether they got a new SIM card or alert them that someone is potentially impersonating them.

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.

9.How can you prevent SIM swap fraud?

* 1. What are some general methods

Look out for phishing scams on emails or websites. SIM card scammers will try and get your username and password first so this is your first line of defense. Also Have security and anti-virus software installed on your machine. This will alert you if known malicious software is trying to infect your machine. It's also vital to keep your software and system up-to-date.

* 1. Who is your Canadian phone company / carrier?

My phone carrier is Telus.

* 1. What do they offer regarding SIM swap fraud prevention?

They use a two-step process to see if you are that person for example they would said a code to your phone and you would tell that code back and they have a security question.