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.

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

Without a sim card, nothing is stored on a sim card of an iPhone - iPhones cannot store data on a sim card - everything is stored on the phone itself, with syncing via iTunes. You can take the sim card out and nothing will happen to your data - it is all stored on the phone.

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

Two-factor authentication 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: such as something they know, something they have, or something they are.

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

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?
2. List some of the services criminals can access if they get control of your SIM card.
   1. Banking & Financial

If you have any banking information on your phone like your card number or bank card password they can steal money and send money to their own account. Also, if they have any apps with your bank card or account linked they can buy items with your money for themselves.

* 1. Social Media

In social media people can use your identity for illegal crimes and actions and frame you for them. Also, they can catfish people and use pictures of yourself and pretend to be you or they will get private information and sell it.

1. Explain how criminals can get control of your SIM card.
   1. Collecting Personal Information

If your SIM card was stolen, this means the person who took it has potentially gained access to all your contacts (people you know) and any personal or confidential information on your phone, which may include banking PIN CODES, bank account numbers, c/card numbers, shopping accounts online, and potentially your parents' and family info too. This information can be sold abroad to spammers, hackers and anyone who wishes to clone identities, use them to steal money from their accounts, buy things using their details and so build up massive debts for them, and so on. This includes your own details. You can now become the victim of fraud. You need to let your parents, your bank and the local police know immediately.

* 1. Create False Identity

People may open new credit card accounts in your name. They may change the billing address on your credit card so you no longer receive the bills as they continue running up charges on the account. Also, they might commit phone or utilities fraud, opening up new accounts in your name. People may open a bank account in your name and write bad checks. They may clone your ATM or debit cards and make electronic withdrawals in your name. People can take out major loans in your name and not pay off the debt. Lastly, Wanted criminals can begin an entire new life, getting a driver's license or official I.D. using your name and their picture

* 1. Requesting a new SIM card

Criminals 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. 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. 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.

1. How can you prevent SIM swap fraud?
   1. What are some general methods

Major carriers in the U.S. offer security that can help protect against SIM card swapping. The easiest way to prevent SIM card fraud is by exercising a few common-sense rules Users should avoid revealing too much personal data online, and check on what alerts can be set up with their bank or phone company to identify any attempts to access their account.

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

There are many phone companies and carriers such as AT&T, Sprint, T-Mobile, Verizon, Bell, Rogers and many more.

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

-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.