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?

Basically a sim card is a card that goes in to your phone and keeps all your memories from that phone you have 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**. ... **Phones** are tracked by their ESN (electronic serial number) so they do not **require SIM cards**. 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)” ?

The most recognized type of one-**factor authentication** method is the password. Two-**factor authentication** – in addition to the first **factor**, the second **factor** is “something a user has.” ... Examples of **a third factor** are all biometric such as the user's voice, hand configuration, a fingerprint, a retina scan or similar.

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

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 latest**iOS** or macOS. ... You can follow these steps on your **iPhone**, iPad, or iPod touch to turn on **two**-**factor authentication.**

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

**Any criminal** act committed using **a SIM card** registered in **your name**, **will make you** legally accountable for the **criminal** act (ex. scams); Losing ... mobile **service** provider and request for all the numbers associated with **your** Personal ... Take **control**: **If you** identify an unknown SIM number under **your name**, report **it .**

* 1. Social Media Some **SIM cards can be hacked** 'in about two minutes' with **a** pair **of** text messages. ... Evidently not, as Karsten Nohl **of** Security Research Labs -- who found **a** hole in GSM call encryption several years ago -- has uncovered **a** flaw that allows some **SIM cards** to **be hacked** with only **a** couple **of** text messages including media.

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

**SIM hijacking** is a little-known but growing threat. To learn how to keep hackers from stealing your phone number, read our guide on how to protect yourself from these attacks. It seemed like any other warm September night in the suburbs of Salt Lake City

* 1. Create False Identity

Knowing a SIM card fraud’s basics can help you protect you against enough information on a target then they create a false identity

* 1. Requesting a new SIM card

1. What are some signs of SIM swap fraud?
2. How can you prevent SIM swap fraud?
   1. What are some general methods
   2. Who is your Canadian phone company / carrier?
   3. What do they offer regarding SIM swap fraud prevention?