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 cellphone SIM card stores user data in GSM (Global System for Mobile) phones. They’re used to authenticate cellphone subscriptions — without a SIM card, GSM phones aren’t able to tap into any mobile network.

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

~SIM cards are required for your phone to work because the card stores user data, and they’re used to authenticate your cellphone subscription. If you don’t have a SIM card, your phone can’t connect to a mobile network.

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

~Text-based two-factor authentication is when a site or media sends the user’s phone a verification code to get them into their account.

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

Two-factor authentication is related to your phone because the service or media sends your phone a verification code to verify your identity and let you in. However, it’s very easy to SIM card swap and forge someone’s identity without even needing their physical phone.

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

Two-factor authentication is related to your SIM card because although getting a two-factor SMS message is better than nothing, it won’t help if you get hit with a SIM swap. The authentication is supposed to help protect your SIM card (and, by extent, your identity) but in reality, it doesn’t help much.

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

If criminals gain access to your SIM card, they can make transactions without you knowing and drain money from your account. They can gain access to your private, sensitive bank information and leave you broke.

* 1. Social Media

If a criminal gains access to your SIM card, they can hack into and steal your social media account. From there, they can steal information from your account and post things without your permission. Some hackers deliberately post inappropriate or sensitive things to get the victim suspended or banned from that social media site.

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

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

They call the victim’s cellphone provider and claim that their 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

Most cellphone 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. They say that their old card had been damaged and, if they answer all of the security questions correctly, they get a new SIM card.

1. What are some signs of SIM swap fraud?

Most victims discover they’ve just had SIM swap fraud when they try to send a call or text; messages or calls won’t go through. Banks can also consider looking for behavioral changes through behavioral analysis technology that can indicate a compromised device. Additionally, some institutions call customers to determine whether they got a new SIM card or alert them that someone is potentially impersonating them.

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

Users should probably avoid sharing personal info online. Try using encrypted apps that aren’t as prone to snooping as SMS Messages are. You could also consider activating two-factor authentication or use authenticator apps like Google Authenticator. Users should switch to messaging apps or services like iMessage, WhatsApp, Signal, etc. for any messages you wish to be private.

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

Fido.

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

I don’t believe that they offer anything in regards to SIM swap fraud prevention; however, you can call in and ask about your SIM card if you suspect that you’re a victim of SIM swap fraud.