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, GSM phones aren’t able to tap into any mobile network.

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

As stated above, most implementations of this type of authentication generate a string of random numbers that you have to enter after logging into an online account. Currently, this code can be received three different ways, one of them being text.

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

When having to recover your information the first verification will be security questions but there will be a second step so that anybody can’t just do some research

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

Bank accounts, trust fund

* 1. Social Media

Instagram,snapchat, facebook

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

Collect Personal Information

Create a False Identity

Request a new SIM card

1. What are some signs of SIM swap fraud?

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

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

banks and carriers have instituted protections that prevent SIM swap fraud before it happens

,user alerting and additional checks for SIM reissuing to sharing knowledge of SIM swap activity between banks and phone companies

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

rogers

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

**How Can I Protect Myself from Identity Theft?**

* Shred documents that contain your personal information.
* Keep identity documents in a secure place and carry only what you need with you.
* Keep your computing devices updated with online security such as firewalls and virus protection.
* When shopping or banking online, keep an eye out to ensure that the website’s URL contains “https” as this indicates it’s secure.
* Ensure to periodically verify your credit report, bank and credit card statements and promptly report any discrepancies.
* Ensure that your mobile device is password-protected.
* Secure your credit card and bank accounts with challenging passwords that cannot be easily guessed.
* Beware of email fraud and phishing scams.

**Signs That You May be a Victim of Identity Theft.**

* Receiving statements for credit cards or other credit-lending services that you did not authorize or activate.
* Receiving collection notices or calls for debts that you did not incur.
* Unknown or unrecognized credit inquiries or accounts open on your credit report.

**Steps You Can Take if You’re a Victim of Identity Theft.**

* Report the incident to your local police and note the report number as it may be required by the service providers where the fraud occurred.
* Report the incident to local police and the Canadian Anti-Fraud Centre (**1 888 495-8501**) [**http://www.antifraudcentre-centreantifraude.ca/index-eng.htm**](http://www.antifraudcentre-centreantifraude.ca/index-eng.htm)
* Contact the fraud departments at these credit bureaus: