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**](http://gsma.com/)**(Global System for Mobile) phones**

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)” ?

**The**[**text-based two-factor authentication**](https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication) **is something that protect your most sensitive accounts.**

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

**If you don’t have two-factor** authentication **set up in your phone, they can use your phone number to trick services into giving up your passwords.**

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

**If you don’t have two-factor set up in your phone , they can use your personal information to trick services into giving them your SIM card.**

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

* **TD bank**
* **BMO**
* **CIBC**
  1. Social Media
* **Instagram**
* **Snapchat**
* **FaceBook**

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

**They can go through your social media accounts.**

* 1. Create False Identity

**Once SIM criminals has gathered information on a target, they create a false identity. First, they call the targets cellphone provider and claim that his or her SIM card has been lost or damaged.**

* 1. Requesting a new SIM card

**They can request for a new SIM card, from your phone service provider.**

1. What are some signs of SIM swap fraud?

**One way to find out if you have SIM swap fraud, is when you try to place a call or text.**

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

* [**AT&T**](https://www.digitaltrends.com/mobile/att-unlimited-plus-unlimited-choice/)**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 my AT&T app.**
* [**Sprint**](https://www.digitaltrends.com/mobile/sprint-offers-free-year-of-unlimited-data/)**asks customers to set a PIN and security questions when they establish service.**
* [**T-Mobile**](https://www.digitaltrends.com/mobile/t-mobile-plans-explained-2/)**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**](https://www.digitaltrends.com/mobile/verizon-plans-explained/)**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.**
  1. Who is your Canadian phone company / carrier?

**I do not have a phone, which means I am not connected to a phone company.**

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

**I do not know.**