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 SIM card is a small chip put in a cell phone. It stores user information such as phone numbers or personal information like your name, date of birth, etc. Without a SIM card in your phone, you cannot make any phone calls.

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

The purpose of a cell phone is to be able to make phone calls away from a landline. A cellular phones purpose is basically to be a portable phone. To make the phone calls, a cell phone requires a SIM card. The SIM card connects to a network for the phone calls to go through. Without a SIM card in a phone, no calls can be made.

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 security method for accounts like social media. They require the user to verify their accounts using their phone number as a form of extra security. With two factor authentication, whenever the user logs into an account, he/she has to verify over text message that the login was made by them. If it wasn’t, it could mean a hack was made towards your account. 2 factor authentication isn’t the best because if you lose your phone, you have to recover your phone and SIM card and that can be difficult.

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

To verify the login was made by you, a text message is sent to your phone and you have to reply to it using the phone

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

To receive the text message for two factor authentication, you need a phone number that you get from a SIM card. Without a SIM card, two factor authentication can’t be done. If you activate two factor authentication and lose access to you SIM card, you cannot login to any accounts without recovering your SIM card or contacting your provider.

1. **List some of the services criminals can access if they get control of your SIM card.**
   1. **Banking & Financial**
   2. **Social Media**
2. **Explain how criminals can get control of your SIM card.**
   1. **Collecting Personal Information**

If the criminal collects enough information (full name, birth date, etc.), the can contact your provider and request a SIM card. Once they get access to your SIM card, they can access all your contacts and all accounts that were linked with 2 factor authentication.

* 1. **Create False Identity**
  2. **Requesting a new SIM card**

Your SIM card provider will ask the criminal security questions to confirm that the correct person is retrieving the correct SIM card. Once the criminal answers the security questions correctly, they will get the requested SIM card and have access to your contacts and accounts.

1. What are some signs of SIM swap fraud?
2. **How can you prevent SIM swap fraud?**
   1. **What are some general methods**

Contact your provider regularly to make sure your SIM isn’t duplicated or with another person, setup extra security questions with your provider, don’t release too much personal information online.

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

Bell

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

You have to setup a username and password or give your account number so every time you call for anything related to services, they ask you for your username that can be private or your account number that can be up to 12 digits