0

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 stores user data in GSM (Global System for Mobiles) phones. They are used to authenticate cellphone subscriptions.

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

Without a SIM card, GSM phones are not 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)” ?

Text-based two-factor authentication is when someone sets up their two-factor authentication as a text message that they would receive on their phone.

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

Two-factor authentication is related to your phone because you can set up two-factor authentication using your phone number or your fingerprint. When you use your number, you will get a text message from the website to verify if the user is you. If you use your fingerprint, you just have to verify using your fingerprint.

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

Two-factor authentication is related to your SIM card because you may give your number for two-factor authentication which would require you to have your SIM card in order to receive any messages from the website.

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

* Bank account information
* Can transfer money from your account.
  1. Social Media
* Twitter
* LinkedIn
* Instagram

1. Explain how criminals can get control of your SIM card.
   1. Collecting Personal Information
   2. Create False Identity
   3. Requesting a new SIM card

Firstly, they collect data from social media accounts, websites, bank accounts. From this they manage to get date of birth, legal names, addresses, and phone numbers. Secondly, once they have gathered the required personal data they make a fake/false identity. Thirdly, they call the victim’s service provider and claim that their SIM has been lost or damaged. Lastly, they ask the customer service representative to activate another SIM card in their possession.

1. What are some signs of SIM swap fraud?

* When you can’t place a call or send a text.
* Banks look for behavioural activity that may prove that there is a compromised device.
* Some institutions call customers to check is they have bought a new SIM card recently.

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

* Do not offer too much personal information online.
* Users should check what alerts you may receive if there is an attempts of logging into your account.
* You can use encrypted messaging apps.
  1. Who is your Canadian phone company / carrier?

At&t.

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

It requires a passcode for any online or phone interactions with AT&T customer representative.