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 small sized card/chip that stays inside a mobile phone when inserted, carrying an id number unique to the owner, storing personal data, and preventing operation if removed from a locked device.

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

A cell phone SIM card stores user data in GSM (Global System for Mobile) to phones. More specifically, a SIM card is required because it allows you to make or receive calls and text messages.

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

This is when the application that you have visited prompts you to send a message through text, email or even by calling your phone containing a short code that you must provide on the appin order to gain access and continue. This is used for security purposes in account protection like for example, a service like Paypal would use it when an account is logged in at the same time on two different computer systems.

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

A lot of two-factor authentication information is sent through text and call. This helps prevent your phone or any other device’s password and other account info from becoming stolen.

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

Criminals can use that personal data stored on the stolen phone’s SIM Card to bypass two-factor authentication prompts found in applications. This will allow for them to have access to all your created accounts and their functionalities.

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

Online banking services such as Tangerine.

Quick Pay systems such as Google Pay, Apple Pay or even Paypal.

b. Social Media

Facebook, Instagram, Twitter and even Snapchat.

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

Once they have the victim's phone they can obtain some personal information from unsecure apps settings such as from password savers and quick account login processes through saved accounts. Overall, they can see through your personal contacts and messages with deeper detail being found in the phones settings.

b. Create False Identity

People can’t easily identify who these victimisers are as that is the loophole within the user interactions of the internet and web in comparison to actually reality.

c. Requesting a new SIM card

Once they obtain the victim's personal information they can obtain full access to data in the SIM card by falsely tricking your phone’s carrier/provider and get access to more account information

1. What are some signs of SIM swap fraud?

The stolen phone’s previous number will stop working because the original SIM card could have possibly been deactivated. You can get emails saying that your password has been changed and even from some applications such as Paypal who have a security message system in which notifies you that your accounts being logged into on other unknown devices.

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

Overall, try not to give away or reveal too much information about you online.

If you fall victim to your phone becoming stolen, call your provider/carrier ASAP to do some deactivation and reconfiguration that way the criminals don’t call your carrier first and fraudulently trick them using the personal info found on your phone to get full access to your SIM card. In the end, the stolen phone becomes useless for fraud.

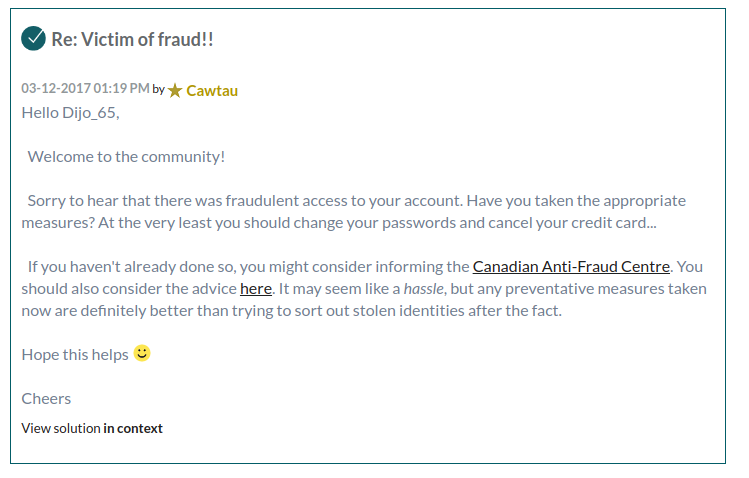
Additionally, major carriers in the U.S. are helping to protect against SIM card swap fraud like AT&T has extra security which requires you to provide a passcode for any online or phone interactions with their customer representative. Sprint asks customers to set a PIN and security questions when they sign up for the service. T-Mobile lets customers create a care password, which is required when they contact customer service by phone.

Who is your Canadian phone company / carrier?

Fido

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

They will tell you to file a claim with the Canadian Anti-Fraud Centre. As answered by customer support in this Fido Forum.



<https://forums.fido.ca/t5/forums/forumtopicpage/board-id/NonTechnical/thread-id/26551>

They provide a guide (forum) on their website on Sim Card Problems

<https://forums.fido.ca/t5/forums/forumtopicpage/board-id/archives/thread-id/25095>

A forum with Online support to change your SIM card.

<https://forums.fido.ca/t5/forums/forumtopicpage/board-id/Smartphones/thread-id/36763>