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/>
* <https://krebsonsecurity.com/2015/11/talktalk-script-kids-the-quest-for-og/>

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?

A SIM card is necessary for activation because it allows the cellular network to know which phones are using it. Therefore, iPhones (and every other cell phone, too, by the way) need SIM cards to communicate with the cell carrier, which allows them to activate.

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

Multi-factor authentication (MFA) is a method of confirming a user's claimed identity in which a [computer user](https://en.wikipedia.org/wiki/User_(computing)) is granted access only after successfully presenting two or more pieces of evidence (or factors) to an [authentication](https://en.wikipedia.org/wiki/Authentication) mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

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

With two-factor authentication, your account can only be accessed on devices you trust, like your iPhone, iPad, or Mac. When you want to sign in to a new device for the first time, you'll need to provide two pieces of information—your password and the six-digit verification code that's automatically displayed on your trusted devices. By entering the code, you're verifying that you trust the new device. For example, if you have an iPhone and are signing into your account for the first time on a newly purchased Mac, you'll be prompted to enter your password and the verification code that's automatically displayed on your iPhone.

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

SIM hijacking recently emerged as fraudsters’ latest tactic to access your personal accounts. And to be honest, it’s impressive. By tricking mobile service providers into believing he’s actually you, a hacker can transfer your telephone number to his device. Once the switch is made, the hacker gains access to your online accounts and can even receive two-factor authentication codes sent to your phone. Although SIM hijacking takes a devastating toll on users’ privacy and digital security, the mobile industry is still struggling to prevent these kinds of attacks. But here’s what we know for sure: Phone numbers are a deeply flawed method of security.

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

Once they’ve gained unfettered access to a victim’s phone number, criminals target bank accounts.“The attacker can read your SMS messages and see who you’re chatting with and what about,” Blaich said. “Many banks will send you a code to log into an account or reset a password to a mobile phone via SMS, which means an attacker committing SIM fraud can request and receive the code and access your bank.”Next, SIM fraudsters mask money withdrawals using a parallel system. They create a second bank account under the victim’s name (banks where the victim is already a customer have fewer security checks). When the criminals execute a transfer between the two accounts, it appears to the bank’s computer system as though the victim is transferring funds between two parallel accounts.

* 1. Social Media

At its most basic level, a SIM swap is when someone convinces your carrier to switch your phone number over to a SIM card they own. They’re not doing it for prank call cover, or to rack up long-distance charges. By diverting your incoming messages, scammers can easily complete the [text-based two-factor authentication](https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication) checks that protect your most sensitive accounts. Or, if you don’t have two-factor set up in the first place, they can use your phone number to trick services into coughing up your passwords.

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

Laying the groundwork for a SIM swap scheme involves collecting as much information about the victim as possible. Fraudsters might send phishing mail — messages that impersonate legitimate businesses like credit card companies and health insurers — intended to fool victims into forking over their legal names, dates of birth, addresses, and phone numbers.

* 1. Create False Identity

Once SIM criminals have gathered enough information on a target, they create a false identity. First, they call the victim’s cellphone provider and claim that his or her SIM card has been lost or damaged. Then, they ask the customer service representative activate a SIM card or number in their possession.

* 1. Requesting a new SIM card

Hackers request a new sim card with a fake identity to lock you out of the system.

Some institutions call customers to determine whether they got a new SIM card or alert them that someone is potentially impersonating them.

1. What are some signs of SIM swap fraud?

It’s tough to detect SIM card fraud before it 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. But some banks and

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

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

* Use better two factor
* Stick a PIN in it
* If a hacker has a phone number that’s associated with some of your online accounts, they can sometimes circumvent two-factor requirements altogether—which gets back to the problem of using phone numbers as identifiers in the first place. Disentangling yourself from those seven digits is hard to do at scale, but it’s worth at least trying on especially sensitive accounts, or if you might be a high-value target.
  1. Who is your Canadian phone company / carrier?

**Bell**

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

Bell said in a statement that it is “continually updating our security measures to counter threats of cybercrime, including those related to SIM swapping and identity theft schemes. As always, we encourage our customers to remain vigilant about password protecting their devices and to be careful about sharing of personal information.”