1. What is a SIM card:
   1. A SIM card is a small chip that is inserted into your phone, it contains your phone number and any relevant information that you chose to store on it like your contacts. Without the SIM card you phone cannot receive data or receive / make calls.
2. Why is a SIM card required for your phone to work?
   1. A SIM card is required because without it you won’t be able to make or receive calls or text messages. It pretty much connects you to the cellular network. That allows you get data from your provider, vise versa.
3. What is “Text-based two-factor authentication”
   1. This is when a website, or service sends a text message to your phone containing a short code that you must provide on the website / service to continue. This could be caused because of a change of your normal login location, or simply because you have it enabled to verify its you each time you log in.
4. How is two-factor authentication related to your phone?
   1. Well since these companies would assume that you would always have your phone on you, or generally in your possession, it would be a good idea to send important login codes to the device itself by text. But once someone swaps the SIM, your sort of screwed until you request it to be cancelled or you take action.
5. How is two-factor authentication related to your SIM card.
   1. Well since your SIM card pretty much connects the associated phone number to the cellular networks, if someone has the SIM card they pretty much have your phone. Since any calls or texts that are sent to that number will be received on the phone with that SIM card with the assigned phone #.
6. List some of the services criminals can access if they get control of your SIM card.
   1. Banking & Financial:
      1. Bank account verification codes
      2. PayPal login
      3. Anything that lets you to log in with your phone to be completely honest.
   2. Social Media:
      1. Twitter
      2. Facebook
      3. Instagram
      4. Google / YouTube
7. Explain how criminals can get control of your SIM card.
   1. Collecting Personal Information:
      1. We live in an age where everything about a person can generally be found quite easily on line, its as simple as googling the person’s full name and see what comes up. If they have a social media account, there’s a good chance they will get quite a lot of information about you, like family, friends, birth, location.
   2. Create False Identity:
      1. Once you gather of the information that you think is required to request a SIM card or even get access to account information you can begin. Companies don’t know how you sound, or what you do during your everyday live. So if you did your research about someone and got the details about their life, you can easily fake being them.
   3. Requesting a new SIM card:
      1. I would hope the process of getting a new SIM card has gotten much more difficult since the rise of all these frauds. But once you create yourself a fake identity of whomever you’re targeted, it’s as simple as making a call and proving all the information you gathered mostly online. Some people could take the extra step and make it sound like they’re having a bad time, maybe fake baby noises in the background to add to the “identity” possibly pursing the operator to send out a new SIM card.
8. What are some signs of SIM swap fraud?
   1. Your current phone will stop working, since the original SIM card would usually be deactivated.
   2. You get emails saying that your password has been changed to accounts with two step verification.
   3. When you try to log into a site and it ask for the two-step verification, no text would be sent to your phone if so, something happened.
9. How can you prevent SIM swap fraud?
   1. What are some general methods?
      1. Do not reveal too much information about you online
      2. Setup private pins that only you know on the carrier website itself.
      3. Do not use text-based two-step verification, use apps like google authenticator, they require you to scan a one-time QR Code, it’s saved on your phone, so the pretty would physically need to have your phone.
   2. Who is your Canadian phone carrier?
      1. Virgin Mobile
   3. What do they offer regarding SIM swap fraud prevention?
      1. They have a pin that is required for specific information changes. That’s the only thing I personally know that they have in place at the moment.