Script for “A Regular Person’s Guide to Cybersecurity”

(Numbering corresponds to the slides)

1. Hi everyone! Thank you for coming! I hope you are excited to learn a little bit about cybersecurity. [INSERT JOKE HERE - perhaps cybersecurity/job security? Banana42?] At this point, technology is so integrated into our daily lives, that it doesn’t make sense to leave cybersecurity to the experts. We can all benefit from being a little more informed about the risks we face, and the things we can do to mitigate them.
2. For those of us who remember the days of [INSERT 90s JOKE HERE], we first started thinking about cybersecurity risk in terms of credit cards. Online shopping quickly multiplied the number of places our credit card number was stored, and many of these companies were not well-equipped to manage the risks to their systems, as it was not their main focus or expertise. Nowadays, it can be overwhelming to even try to list all of the companies that are storing our credit card info, and most of us rely more on the fact that cards can be easily cancelled rather than really trying to protect our credit card numbers online.
3. Beyond credit cards, we now have information at risk online that can cause much more lasting damage. Our email accounts, for instance, can contain a lot of confidential information, and we now access them from multiple accounts on multiple devices. Even mentally cataloging all of these is starting to become a bit of a challenge.
4. If we look for advice, things quickly spiral into a long list of questions. [SHOULD INSERT A FUNNY QUESTION LAST ON THE SLIDE – somethings “asking for a friend”?]
5. The advice we get is often not very helpful. It might be full of jargon we don’t understand, like:
6. Or so inconvenient to follow that even those who should know better don’t do it.
7. A third category of advice is stuff that makes sense *from a very particular perspective.* Like the common advice that writing down complicated passwords on paper in your home is preferable to choosing ones that are easier to remember, because it’s unlikely that a “hacker” will have access to your physical space. This ignores the very persuasive insider threat scenario, where an abusive partner or family member might be using technology to surveil or control you.
8. So we’re not going to go through a list of specific recommendations, because this isn’t a one-size fits all situation. Instead, we’re going to build up a *process* for thinking through cybersecurity threats, so you can generate the kinds of tailored recommendations that would make the most sense for you.
9. We’ll start our exercise with a little bit of cataloging. Get out your workshops, and we’ll spend about 2 minutes here on the first step, which is making a list of the most sensitive devices, accounts, passwords, etc. that you interact with.
10. Now look through your list, and put a \* next to every kind of device/account/etc that you also had when you were 20. See how much your list has grown. [INSERT JOKE HERE? Something about generational disconnect?]
11. Now we’re going to think about how the things on our list might be connected. Sometimes one of them can be used to access another – like a password being used to open a gmail account. Visually we can represent this kind of relationship with an arrow – denoting that control of one thing can be used to get access to another.
12. Sometimes these relationships chain together. For example, it’s common to set a gmail account as the backup for resetting an amazon account password. This means that control of the gmail account can be used to get access to the amazon account, so by looking at this path of arrows, we see that the password that opens our gmail account can effectively be used to get into our amazon account as well.
13. Sometimes these connections between things are 2-to-1 – in the sense that you might have a combination of items that can be used to gain access to another item. For example, if you have your gmail account permanently logged in on your iphone, then an attacker could gain access to your gmail account by having the combination of your physical iphone as well as its passcode.
14. These kind of dependencies between accounts, devices, and passwords are typically created by account settings, password reset mechanisms, … etc.
15. Let’s pause here and take a couple of minutes to list all the kinds of dependencies between your items that you can think of.
16. Ok! So now that we have some understanding of the objects that populate our digital universe and the direct relationships between them, let’s map it out!
17. Take about 5 minutes to draw a map of your most important accounts, devices, passwords, etc. and put arrows to represent the direct dependencies between them.
18. Our map can help us picture how we, as legitimate users, access all of the items in our digital universe. For instance, you might get into your facebook account by using a password, and you might get into your iphone using either a passcode or a fingerprint. You might use the same password for multiple purposes.
19. But this map also gives us a framework for thinking about how we might be exposed to cybersecurity threats. Let’s look at our map from the perspective of an attacker.
20. There is a really unfortunate and rampant misconception that terms like “secure” can be meaningful without a detailed context. A cybersecurity expert will never ask if a system is “secure” or not. This is like asking if a politician is “corrupt” or not. It’s never a binary question: it’s always a question of context and degree. A better question is: will this politician vote for an estate tax cut if they are paid $100,000? Similarly, a better cybersecurity question is something like: “can a stalker get access to my real-time location data with a reasonable amount of effort?” To develop a reasonable sense of what an attacker can do, we have to put ourselves in the shoes of the kind of attack we are worried about. What does the attacker want? What might they have access to? How much effort and money are they willing to spend?
21. To get into the mindset of the kinds of attackers that commonly threaten our personal security in cyberspace, I want to introduce you to 4 typical attacker characters. The first one is a thief. The Thief is looking to steal physical devices, like phones or laptops, and is probably looking to make a quick buck. A thief might be vary street-savvy, and might look out for opportunities to observe passcodes or passwords being entered before swiping a device.
22. Our next attacker character is a con artist. The con artist is also looking to make money, and might try to do so through spamming many accounts, selling identifying info on the black market, using malware to infect and encrypt machines and then demanding a ransom from victims, etc. This kind of attacker probably won’t have physical access to you or your devices, but may obtain information about you that was compromised in prior large data breaches, and may try to send fake emails to get to you click on malicious links to infect your devices. Cybersecurity related fraud is estimated to cost corporations more than $500 million a year. With all of that financial incentive floating around, con artists can be very technologically savvy, and very well-resourced. Most of us ignore this kind of threat because we think we are not “important enough” to fall victim to it. But actually, once a con-artist has crafted a piece of malware and a phishing email, it’s really really easy to send it to a *lot* of people. So it’s not very logical to think we are immune. [Anecdote about gmail account being hacked while teaching crypto in order to send spam emails]
23. Our next attacker character is a stalker or cyberbully. This is somebody who is in your life, who is personally targeting you and wants to control or embarrass you. This person is probably not as sophisticated as the con artist, but they may have some physical access to your devices, and they may be willing to put in a lot of effort to accomplish their goals.
24. Our last attacker is the ultimate insider threat. This is someone who is close to you and who you may or may not realize is a threat. Their goal may be to control you, manipulate you, or steal from you. This person might have very close access to your devices, may even have legitimate accounts on your devices, or share some of your passwords, etc. For passwords they don’t share, they might have many opportunities to observe you entering them.
25. However you imagine the most salient threats to your cybersecurity, just don’t picture the attacker like this:
26. When I imagine an attacker threatening my cybersecurity, I picture a bully. Let’s call her Jamie. Her goal is to get dirt on me that she can use to embarrass me in front of my friends. Who she is hoping to steal because she is a bully. She is an entirely fictional character. And nothing exactly like the girl who bullied me in middle school.
27. I want each of you to take a few minutes to get into the head of a villain in your cybersecurity universe. Develop an attacker character who may threaten you – what do they want? What kind of access do they have? What kind of resources or skills do they have? How much effort are they willing to put in?
28. Now you’re going to go back to your map of important devices, accounts, etc. and come up with a difficulty score for each, for the particular attacker character you developed. Don’t worry about the arrows for now – just score each item from 1 (easy) to 10 (hard), on how difficult it would be for your attacker to get *direct* access to that item. How easy would it be for them to guess that password? Or gain temporary possession of you phone? For my bully Jamie, I imagine it would be very easy for her to see me enter my passcode at some point. We are classmates, after all. And probably not very hard for her to get access to my phone. Like she might ask to borrow it with a good excuse in front of other people so that I’ll look really mean if I say no. But getting into my Facebook account directly would probably be impossible for her. I mean, unless she works for Facebook now. Which I guess she might. Kind of seems like a Jamie thing to do. So take just a couple of minutes and score the items in your map for your attacker.
29. Now we’re going to see what the combination of the scores and the arrows implies about our overall vulnerability to this kind of attack. We’ll take this one step at a time.
30. First, pick a number between 1 and 10 to represent how much effort you imagine your attacker putting in. I’m going to set Jamie at a 2. Don’t get me wrong, she puts a lot of total effort into her mean-girl-ness. But she does spread it out over more than just me. So I think an effort of 2 into me specifically is realistic.
31. Now look through your map and circle all of the items that are scored less than or equal to your attacker’s effort: for me this is my iphone and my passcode. Now let’s follow any arrows and circle any new items that the attacker can get access to. In my case, Jamie’s access to my iphone and my passcode imply that she can get into my iphone contents, and from there she can get to the facebook app, where my account is perpetually logged in. Follow your arrows from any circled items, and keep circling any new acquired targets until you’ve traced through all of the implied consequences of the attack on your universe. In fancy math speak, this is called “breadth first search on a directed hypergraph”. That’s what I’d call it if I were trying to collect a fat consulting fee. But since I’m actually trying to teach you something, I’ll call it “Follow the arrows”!
32. Now let’s look at the things that were compromised. What if we don’t like what we see? Maybe we want to consider changes that could prevent that same attack from compromising some of those things.
33. One thing we can try to do is remove dependencies between things. For example, if you don’t leave your amazon account permanently logged in on your laptop, you can eliminate the arrows that correspond to this in your map.
34. Another thing you can do is to change a single dependency into a more complex one. When you add two-factor authentication to your gmail account, for instance, you make it so that the password alone is no longer enough to access your account. This is what “two-factor” means – it means you set a policy that requires at least two specified things to get access to the account. Typically it’s something like a password and a passcode texted to your phone.
35. Overall, it makes sense to identify your most critical points, and try to minimize any arrows going into them. We want our most critical things to be very difficult for an attacker to get, but they are only as strong as the weakest ways in. So for instance, if you typically use your gmail account as the backup that can be used to reset your access to critical services like online banking, then you really want to make sure it’s hard for an attacker to get into your gmail account. You may want to add two-factor authentication. You may want to make sure you don’t use your gmail password for anything else. And you may want to think carefully before you let a browser store your gmail password, or before you type it into a shared computer.
36. Finally, you might want to think about ways to make the individual difficulty scores higher for a particular kind of attacker. For New Yorkers – don’t keep your smart phone in your back pocket. Seriously. That’s for tourists.
37. So now that we have a framework for expressing and vetting our digital security set-up, let’s see how we can use this generate answers to common questions. We’ll start with: should you use a password manager? This is asking you to compare two possible maps: which one is stronger? Well, it depends on the difficulty scores. The thing about a password manager is – a good one is probably pretty hard to break. It is kind of their whole business model. So that score itself should be pretty high. Whether the net effect is better than what you had before will naturally depend on what you were doing before. If you were reusing the same password everywhere, the password manager is probably a big improvement.
38. Another common question is: is 2-factor authentication worth the inconvenience? That depends on what kinds and strengths of attacks you feel it’s important to defend against. I for instance, worry about a shoulder surfing attack by an evil roommate. Let’s just call her “Pam”. Which is definitely not exactly the name of my least favorite freshman year roommate. I think it’s reasonable to worry that Pam might at some point observe me entering both my iphone passcode and my gmail password, so if I don’t have 2-factor authentication turned on, she’ll get into my gmail account, and reap all the spoils thereof. But if I do have 2-factor authentication turned on, then my password alone is not enough. And I do keep my actual devices out of her evil reach at all times. I mean, she may act all nice and all with other people, but I don’t trust her for a second. Hypothetically.
39. Now you may be naïve and trust your roommates (good for you! What’s it like living in Brooklyn?) , but you might also be worried about a phishing attack that is trying to gain control of your email. In this case, if someone infects your machine and gets your password, they can log into your gmail remotely and wreak havoc if you don’t have two-factor authentication turned on. Again, the financial incentives here make this more likely than you might think.
40. Wrap up and lead into activity: look at your unlocked phone through the eyes of an attacker. Can you figure out where you live? Can you get to embarrassing photos or content? Can you tweet something? Can you read emails? Can you change your email password? Can you spend money? How much? Can you install a key-stroke logger? How quickly can you do these things?