Online Safety

Maxwell Memorial Library's Technology Class
Thursday, January 23, 2020

0. Introduction

Contrary to the Hollywood depiction, most computer hacks don't come about because some super-genius finds a way to crack a database of encrypted passwords. Cracking strong encryption is a very time consuming process, but getting someone to give you their passwords (or something equivalent) is much more doable.

The ransomware attack on OCPL this past summer brought this reality of online security home to Onondaga County. It was, like many other ransomware attacks, accomplished by social engineering: getting someone in the system to "open a door" to someone they mistakenly thought should have an open door.

Today's program will talk about some skills for keeping your online data safe:

- Recognizing phishing,
- Managing secure passwords, and
- Keeping software up-to-date.

1. Phishing

See FTC print out: "How to Recognize and Avoid Phishing Scams" at
https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

2. Passwords

2.1. Basic ideas in safe password management

A good way to think about passwords is to view them as the keys or combinations to the locks on your various online "boxes." In this analogy, some "boxes" are like safes. These are the accounts that you're willing to put some real effort into keeping secure (for example, your financial accounts). You would like these passwords to be unique[1] and effectively uncrackable, and you probably wouldn't walk around daily with these passwords in your wallet. On the other hand, though, just as you want to be able to find your safe deposit key when needed, you don't want to forget them. So you'd like some system that makes it easy for you to remember them and virtually impossible for anyone else to guess them.

Continuing with the analogy, other "boxes" are more like your house or car (for instance, email, social media, and so on): you don't want anyone cracking these accounts any more than you want them cracking your financial accounts, but you might need to have access to these passwords frequently and easily. Just like your car or house keys, then, you'd like to "carry" them with you everywhere.

This is where the analogy starts to break. Because if you carry your passwords in the same way as your car and house keys (as physical items in your bag or pocket), it's not the same as carrying physical keys. It's more like carrying the keys and a key duplicating machine that will make perfect copies. If someone sees your house key, you're still pretty safe from being burglarized; if someone sees your password, they now *have* your password.

So how do you create safe passwords that you can remember without writing them down? We'll talk about methods in a bit, but first consider the properties we want passwords to have:

1. Easy to remember

   Many OCPL patrons use their birthdate or part of their phone number as the PIN for their library cards. This would be a bad choice for any password that needed to be at all secure. However, since there is little incentive for bad actors to crack your library account, these patrons find that the ease of remembering the PIN is more important to them than making sure it stays secret.

   To push a bit on the analogy above, some accounts are like luggage with a cheap luggage lock: sure, a really good password would be the most secure way to go, but is it worth the bother?

2. "Uncrackable"

1 Ideally, you'd like them to be completely unique in that they are strings that aren't already used by anyone for anything. More realistically, you'd like them to be unique at least within the set of all of your own passwords.

I've put scare-quotes around the word *uncrackable* since absolute uncrackability is an impossible requirement. However, the more random a string of characters is, the harder it is to guess, and the longer it will take a computer to crack it.[2]

The word *random* in the previous paragraph is important. If we could actually remember arbitrary strings of characters, the ideal way to come up with passwords would be to roll a 95-sided die (1 face for each character on a standard keyboard) multiple times and use the resulting string. Given reality, though, see item (1) above.

3. Hard to guess

   This is where those security questions like “What was the name of the street you grew up on?” are coming from. Personal details that are not easily accessed, obscure hobbies, and other things about you that are off the beaten path can make good sources for material to use in passwords.

4. Fresh

   None of your accounts should have the same password for long stretches of time. A saying among tech-types is that passwords are like underwear: they shouldn't be shared, and they should be changed regularly.

   In particular, if you have an account with a provider who's system got hacked, change your password with them as soon as you can.

5. Unique

   Ideally, none of your accounts use the same password. There are at least 2 reasons for this ideal:

   a. Most importantly, if someone gets a hold of 1 of your passwords, then only 1 of your accounts is placed at risk.

   b. From the standpoint of public cyberhealth, as it were, the more duplication there is in a site’s encrypted password database, the easier it is to crack if it falls into the wrong hands.

As you can see (and as you have no doubt experienced), these ideals contradict one another. We'll now look at some methods people have come up with in order to craft workable compromises among the ideals.

2.2. Password managers

One way around the problem of generating passwords, remembering them, and keeping them fresh is to use a password manager. A password manager is an application that is effectively like

2 Longer is better and more random is better.

the computerized version of carrying a piece of paper with all your passwords but with more security to it and with more capabilities. Storing all your passwords in plain, unencrypted text on your computer or on a USB stick would be a bad idea since anyone who got a hold of the file would have all your passwords without any further effort. The manager encrypts your data, though, so it is secure.

As an aside (but an important one), I should mention here that if you have your internet browser (for example, Chrome, Edge, or Firefox) remember your passwords, you probably do have your passwords stored on your computer as unencrypted text.[3]

Most password manager apps store your data on their servers, making it available on all your devices. Storing all that personal data does make those servers attractive targets for hackers, however, so you want to be sure that the company making the app is taking security seriously.

Password managers are not just a secure means of storing your passwords and giving you access to them wherever you go. Some apps can also generate near-random strings as passwords, taking care of the problems of coming up with secure passwords. Another feature is alerting you to when a site you have an account with has been hacked so that you can change your password with it quickly. Also, some offer wizards that help you with determining your overall password "health" — which passwords you currently have are weak or are duplicates — so that you can work on strengthening at least the more important ones.

Below are some password managers that get recommended often. Note that you should download any password management software directly from an official site since hackers have been known to distribute rogue versions.[4]

- Dashlane (https://www.dashlane.com/)
- LastPass (https://www.lastpass.com/)

3. Articles and webpages with more information

Bojana Dobran, "9 Strong Password Ideas For Greater Protection," PhoenixNAP (blog), PhoenixNAP Global IT Services, September 29, 2018, https://phoenixnap.com/blog/strong-great-password-ideas

Charlotte Empey, "How to create a strong password," Avast (blog), Avast, August 15, 2018, https://blog.avast.com/strong-password-ideas

3 Firefox's settings can be changed such that the file will be encrypted. That setting reduces the security risk from having Firefox store your passwords, but it doesn't give you the additional features of a password manager.

4 This is particularly true for KeePass since it is open source. While open source software has security advantages over proprietary software in that its code is open to inspection by the community of experts, its free distribution status means that you have to be sure that your source for an open source app is trustworthy.

Hoffman, Chris. How to Create a Strong Password (and Remember It). How-To Geek. May 29, 2015. Updated May 9, 2018. https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

"How Do I Create a Strong and Unique Password?" Webroot: Smarter Cybersecurity. Accessed May 19, 2019. https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password