BC Society of Transition Houses

Passwords: Ways to Increase Your Security

While most everyone has at some point heard the basics of password security (use a strong password, don't use the same password on different sites, etc.), many of us still brush off that advice because it seems too complicated, or it feels like we just don't have the time. We use the same password across different sites; we use passwords that are easy for others to figure out – and just hope for the best. But passwords are just as important as other tools we use to verify our identity – like driver's licenses, social security cards, and passports – and they are just as important to keep secure. Below we've listed some key tips to simplifying your password security – and to understanding why it's so important.

FOCUS ON LENGTH.

The best passwords are at least 12 – 15 characters long and contain letters, numbers and symbols – which sounds like a lot. But remember – the important part is length! You can keep it simple by creating a short sentence that's easy for you to remember, like summerismyfavoriteseason. For added strength, or if a website requires it, you can add numbers and symbols to the mix: Summeri$myfav0riteseason.

Bonus tip: Do NOT use common phrases from pop culture and don't bunch up the numbers or symbols at the beginning or end of the password – spread them throughout, as demonstrated above.

USE DIFFERENT PASSWORDS FOR ACCOUNTS THAT CONTAIN SENSITIVE OR PERSONALLY IDENTIFYING INFORMATION.

The importance this tip can't be emphasized enough. If you use the same password across these accounts, once it's been cracked, ALL of your accounts become vulnerable. Just as you use different keys to protect different places, use different passwords to protect important accounts.

PASSWORD MANAGERS SECURELY REMEMBER YOUR PASSWORDS SO YOU DON'T HAVE TO!

Most of us avoid using different passwords for different accounts because it's just too hard to remember them all, and we know writing them down isn't safe. Luckily, password managers - tools that store and protect passwords like banks store and protect money – can help! These tools can also create passwords that are incredibly hard to crack. All of your passwords (whether you created them yourself or the password manager did it for you) are kept within an encrypted vault, which can only be opened with a master password. The master password should be the longest, most unique password you've ever created, and it should not be stored by the password manager. If you're considering this option, here are two important things to find out:

- Does the company have the ability to see your stored passwords?
- Does the company see or store your master password?

The most secure options will be those that answer **no** to both of these questions.

USE TWO-FACTOR OR MULTI-FACTOR AUTHENTICATION.

It sounds pretty fancy, but all it really means is instead of just entering a password to log in to your account, you will also need to enter a second piece of information. You can usually find this option in the account settings or security settings of the online service. There are a variety of options out there, and they fall within two distinct categories: "something I have" or "something I am". Currently most services use the "something I have" kind. Here's how it works: after entering your password, the company will immediately send a short code to something you have: an email account, a text message or voice call to your phone, or an app you have installed on your device. You then enter that code on the website and, voila! - you are able to access your account. It confirms you are who you say you are, because you verified you have the email account, smartphone, etc. that you previously connected to that account. Some emerging technologies are beginning to use the "something I am" authentication –a retina scan, a thumbprint scan, a facial recognition scan, etc.

BE WARY OF SINGLE SIGN-ON.

Many websites offer you the ability to use your social media or email account credentials to sign into their website, without having to create a new account. While this can be helpful because it means one less account you have to remember a username and password for, there are a number of possible risks involved with using it. When you choose to do this, you are also likely giving Facebook, Google, etc. access to more information about you than they already have, and sharing information from your social media account with the new site or service. (Remember the saying: "If the service is free, your personal information is often the price.") A final risk to consider is that if your social media or email account gets compromised, it means the other accounts you've used those login credentials for are also compromised.

SHARE YOUR PASSWORD WITH…. NO ONE!

Sometimes – especially in new relationships – we want to share everything with our partner, and have them share everything with us. But just as you wouldn't give them your identity documents to carry around in their wallet, it's important to keep your passwords private, and to respect the privacy of their passwords.

DON'T LET BROWSERS REMEMBER YOUR PASSWORDS.

While this feature in many browsers may make it super easy to get in to your accounts, it also makes it easy for someone who's using the same computer or device to access those accounts (and all of your personal information) without needing to know your password. If you need help remembering your passwords (and who doesn't these days?) consider using a password manager.

BE STRATEGIC WITH YOUR SECRET QUESTIONS AND ANSWERS.

Those secret questions aren't really secret. Someone who knows you (or someone who can Google) will be able to guess where you went to high school or your favorite color. There's no rule that you have to be honest when answering those secret questions, so make things up that you'll remember but someone else can't guess.

DON'T TAKE THE BAIT.

Unfortunately, most malicious hackers don't have to work very hard to get access to passwords. They use strategies to trick people into giving them up. One common way they do this is by calling and pretending to be a representative from somewhere you are a customer at and convincing you to give them private information. Another way is by sending an email pretending to be from a website, service, friend, or colleague, and giving you a website link to follow. When you click on that link you're either directed to a fake website that asks for your private information, or the link launches malware onto your computer.

CHANGE YOUR PASSWORD (ONLY WHEN YOU NEED TO).

If you think someone knows your password, changing it from a device that isn't being monitored can keep them from gaining further access to your account. But if your account hasn't been compromised and you have created a strong password using the guidelines above, it's not necessary to change your password often.

REMEMBER TO LOG OFF.

Computers and devices are smart - sometimes too smart – and unless you actively log out, your account may remain open indefinitely, allowing others easy access. While it's certainly convenient to not have to log in every time on our own devices, it's important to weigh that convenience with the risk of what might happen if our device gets in the wrong hands. Also – getting into the habit of logging out on our own devices makes it less likely we'll accidentally stay logged in to our accounts on computers and devices that aren't ours. If you're concerned you may have stayed logged in to an account by mistake, some online services like Facebook and Gmail allow you to go in and see the places where you're currently logged in and give you the option of logging out of them remotely. If you're using an app on a smart device that doesn't allow you to log off, you might want to consider deleting the app or account. This is an additional hassle - but weigh the sensitivity of the information in that account and the risk of someone else accessing that information.

CREATE A SEPARATE EMAIL ACCOUNT TO USE FOR LOGGING IN TO ONLINE ACCOUNTS OR MAKING PURCHASES.

Creating an alternative email account that you can use for online accounts and purchases can help protect your privacy, and also help you avoid all of that spam in your actual email inbox.

Bonus tip: Many companies these days want you to create a new account, even for one time interactions. Online shopping companies often encourage you to do this, even though it's not a necessary part of doing business with them. Before you do, look to see if they have a guest checkout option. If it's not a company you'll be doing business with regularly, consider skipping the account creation process.

Special thanks to Steven Jenkins of EmpowerDB for providing content expertise on this handout.

Adapted from and in cooperation with the Safety Net Technology Project at the National Network to End Domestic Violence, United States