NNEDV

Passwords:
Increasing Your Security

While most everyone has heard the basics of password security (use a strong password, don't use the same password on different sites, etc.), many of us may disregard that advice because it seems too complicated, or we just don't have the time. But passwords are an important part of security at work and in our personal lives, and serve as a first line of defense to protect our sensitive data and information. The vast majority of hacking incidents and data breaches are due to weak or stolen passwords. Below we've listed some key tips to increasing your password security.

Before We Start: Prioritize Safety

It is important to acknowledge that for many survivors, using strong passwords isn't enough, and updating passwords can even be dangerous. If an abusive person regularly monitors devices and accounts, they may know that a password has been changed, and may be able to change the password themselves. In addition, abusive people can coerce or force survivors to share their passwords.

There isn't one "right" way to respond to an incident, only ways that do or don't fit your situation. What works for someone else may not work or be safe for you. Always prioritize safety and trust your instincts. Making changes will often alert the other person. They might force you to unlock your phone or share your passwords. They might become more abusive. In some situations, making changes could also erase evidence. You may find these safety steps useful:

- Use a safer device. If you think that someone is monitoring your phone or accounts, use a different device (such as a library computer or a friend's phone) and account that the person cannot access (and that they have not had access to in the past).

- Get more information. Navigating violence, abuse, and stalking can be difficult and dangerous. Advocates can help you figure out options and local resources and help you create a plan for your safety. You can contact a national helpline to be connected with local resources.

What Makes a Strong Password?

Focus on length. The best passwords are at *least* 12 – 15 characters long, and can contain letters, numbers and symbols. This can sound like a lot, but remember – the important part is length! Lowercase letters on their own are just as fine as mixing it up with numbers and symbols, *as long as the password is long enough*. You can keep it simple by creating a short sentence that's easy for you to remember, like summerismyfavoriteseason. Be sure not to use any sentences that others are likely to guess or predict. For added strength, or if a website requires it, you can add numbers and symbols to the mix: Summeri$myfav0riteseason.

Change it up. Use different passwords for accounts that contain sensitive or personally identifying information. The importance of this tip can't be emphasized enough. If you use the same password across these accounts, once it's been cracked for one account, 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

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 primary password. The primary 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, there are a few factors to consider when choosing a Password Manager option. Two important initial things to find out are:

- 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.

Here are some other factors to consider:

Keys vs. Passwords

Instead of, or in addition to, a primary password, some password managers – and some websites – provide the option to use a passwordless authentication key, often called (depending on the company) a Passkey or Secret Key. A key is a piece of information stored *in the device itself* that tells a website or app that this device is allowed to access protected information. It is not uploaded to the Internet, so if the password manager company's data is stolen, or someone obtains your password by some other means, the thief still won't be able to read your information. This can make a passwordless key a useful option for people who control their own devices. Passkeys, which are a specific type of passwordless key that meets certain standards, are discussed more in the Multi-Factor Authentication section of this resource.

Other-Use-Account Password Managers

Some browsers (such as Firefox) and accounts that are used for other purposes (such as Google) have an option to use built-in password managers. While these can be convenient, they also carry the risk that someone who is able to get in to your account will be able to steal your passwords, because the security of the passwords is only as good as the security of your Google account, Microsoft account, Firefox account, or whatever other built-in option you use. For this reason, it is usually more secure to use a separate password manager that is only a password manager, such as 1Password or LastPass.

Multi-Factor Authentication

Use two-factor or multi-factor authentication. All this 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 for multi-factor/two-factor authentication, 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, cell phone, etc. that you previously connected to that account.

As with so many issues in digital privacy and cybersecurity, there is no single "best" answer; it depends on the types of risks you're most concerned about!

Hardware Authentication

For people who are concerned about their devices being monitored or compromised, and as a result are unsure whether entering "something I have" on their devices would be giving the information away to an abusive person, one interesting option is a hardware authenticator, such as a YubiKey – a small object that you can connect to a device as proof that you are who you claim to be. You can take a quiz to determine which type would work best for you.

This can be an excellent method of securing your accounts and devices that doesn't require using information already on your devices. However, if you are concerned that you would not be able to keep an abusive person from discovering the hardware authenticator and taking it from you, this may not be the right option for you.

Biometric Authentication

More and more platforms have an option to use the "something I am" form of authentication – a fingerprint, or your face, for example. Traditionally, these methods of authentication have been considered "more secure" than "something I have" methods. However, law enforcement are currently not restricted from forcing access from you through biometrics to the same degree that they are from forcing access through passwords. And unlike with a password, if your "something I am" data is compromised, you can't readily change it.

Passkeys

A passkey is a type of passwordless authentication key, which we briefly discussed in the password managers section. Passkeys are a joint project of Google, Apple, and Microsoft, to reduce the need for passwords, and they meet certain design standards. Passkeys are stored on your devices – you never have to remember them yourself and website or app operators never see them – and you use them in combination with your device's security method (e.g. biometrics like FaceID or TouchID, a password, a PIN) to log onto apps, websites, and other services that support them.

Passkeys can be a great option to increase privacy and security for many people, including many survivors. However, *if* an abusive person has physical access to one of your devices *and* has the ability to log on to that device – for instance, because they know your laptop login password or might coerce or force you to open the device with your thumbprint or face – this may not be the right option for you, as it could lead to the abusive person accessing not only that device but other devices you own from the same company (e.g. other Apple devices).

Single Sign-On

Many websites offer you the ability to use your social media or email account credentials to sign into their website or create an account (such as using your Facebook or Google account to create an account on or log into LinkedIn, TikTok, a shopping site, etc). This is called single sign-on, and you should be wary of it.

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.

A final risk to consider is that if your social media or email account gets compromised, whether by a hacker or an abusive person, it means the other accounts you've used those login credentials for are also compromised.

How Someone Might Know Your Passwords and When to Change Them

There are a few different ways that someone might know your passwords:

- They might appear in *data breaches*, where someone copies or steals information, such as a website's database of usernames and passwords. You can check what breaches a given email address or phone number has appeared in at HaveIBeenPwned, which can help you figure out which passwords need to be changed.
- A family member or current or former romantic/sexual partner might know them, either through consensual sharing, nonconsensual monitoring, or guessing (if an easy password). The Clinic to End Tech Abuse at Cornell has a helpful guide to "disconnecting" from an ex-partner (or family member) that discusses passwords among many other topics.
- Someone may have tricked you into giving them one or more of your passwords. Many hackers use strategies to trick people into giving passwords up (*social engineering*). 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 (*phishing*). 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.

If you think someone knows your password, changing it from a device that isn't being monitored by that person (such as a library computer) 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. If an abusive person tries to coerce you into sharing your passwords, or threatens you, you can reach out to get help and support from a person you trust and or an advocate.

Other Tips for Password Security

- Be strategic with your secret questions and answers. 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.
- Create a separate email account to use for logging into online accounts or making purchases, and use guest checkout when it's an option. Creating an alternative email account that you can use for online accounts and purchases can help protect your privacy, and make it more difficult for an abuser/stalker/harasser to discover or compromise your accounts. It can also help you reduce spam in your actual email inbox.
- Remember to log off. Unless you actively log out of an account or device, it may remain open indefinitely, allowing others easy access. While it's 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. Getting into the habit of logging out on our own devices also 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.

Supported by US DOJ-OVW Grant #15JOVW-21-GK-02216-MUMU. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of the U.S. Department of Justice.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.