Password Security Tips

Passwords have become a mainstay of 21st Century life, as unfortunate as it is for all of us. They are annoying, unwieldy, not very safe, inconvenient, and did I mention annoying. Unfortunately, they are also absurdly important until there is a safe and convenient way to protect ourselves online that doesn't involve memorizing a password that's 213.71 characters long and contains both uppercase, lowercase letters, as well as a number, symbol, ancient Egyptian hieroglyph, and pi to the 100th point.

That might be a slight exaggeration, but every IT professional knows when the system forces you to change your password, and we find it just as annoying as anyone else. But it is important to know good password procedures and policy; which is why you hear the same points every time there's any sort of computer security notice or issue. It can be difficult to keep passwords straight, especially if you have many different ones for work and personal life, but a password is all that stands between your most private and sensitive information and the rest of the world, so shouldn't you at least treat it with the same respect you treat your house or car keys? If your house locks could be opened by a pen it wouldn't be very useful at all, and a weak password is the cyber equivalent of keying your house using a Bic pen.

However, there are many great tools that are free and powerful for keeping passwords straight and strong.

KeePass is a password database and generator software that is open source and free, so you can use it for your personal and professional life. KeePass requires you to remember exactly one password, your Master Password, and then handles the generation and saving of the rest of your passwords. It is secure and has backup capabilities. For a tutorial on how to set up and use KeePass, you can refer to the following video to install Keepass, set up a database, and start saving your passwords.

https://www.youtube.com/watch?v=nuYpoqkbxSs&feature=youtu.be&t=115

Until you are entirely on board with setting up a password manager; at a minimum, we suggest you follow these password best practices:

> Length: Longer passwords are much harder to force their way into.

> Complexity: Use symbols and numbers in your password.

> Non-Obvious Passwords: Don't use your birthdate, kids names, pets names, or any personal information in a password.

One of the most important password rules that is often very overlooked is very simple:

DO NOT USE THE SAME PASSWORD FOR EVERYTHING YOU DO

If you use the same password for everything it makes it all very much less secure. If you use the same email for everything, it allows attackers to work their way back through everything you own, all the systems you use, and can turn into a very large mess for you to deal with.

Follow these rules, or even better, use a password manager, and you'll be as safe as you can be.

How do Passwords Work?

While passwords are by far the most common type of authentication, there are actually many other different types:

> **Something you know:** A good old fashioned password, a bank PIN, or a safe-word when the alarm company calls your house
>
> **Something you physically have:** A literal hardware key, a phone to complete two-factor authentication (example: you're texted a code to your cell phone to verify your identity), or the keycards you use to get into a building
>
> **Something you are:** This is where biometrics hang out; fingerprint data, retina scans, or iris scans. While these are secure they also can't be changed, so if your biometric data gets hacked, you could be at risk for the rest of your life.

When computers first came out, passwords were stored in plaintext (text that is not computationally tagged, specially formatted, or written in code), so if your password was 'Password' (PLEASE don't use this as a password!), it would be stored in a database exactly like that and an application within your computer would check what you type into your login screen against the text that is stored. As you might imagine, this wasn't very secure…and they quickly found a way to do it much better..hashing.

Hashing is the process of running a password through an algorithm that turns the password into a seemingly random string of numbers and letters. So when a user types their password into a computer, it is run through a Hashing algorithm and then that hash is checked against the hash database. One interesting thing about Hashing is that by running the same input (password) through the same algorithm, you will get the same output (pseudorandom string of numbers and letters) every time. For example, you could put the entire Harry Potter series of books into a Hashing algorithm 3 different times and it would spit out the same output each time. Hashing makes it much more difficult to break passwords, because even if a hacker steals an entire password database, he/she would still have to have the correct Hashing algorithm to convert them back into plain text passwords in order to gain access to your information.

There are also other layers of password security that help prevent hackers from gaining access to important systems, but they are incredibly technical and not relevant to most.

Here's an example of how using the two main concepts of Hashing works…

1. Psuedorandom:

> GreaterIowaCUIsAwesome → database assigns characters that appear to be random that are associated with the password as a whole → 17cbe272bfec635169364c32a7acc257

2. Deterministic: Any change in the password characters will drastically change the output. Hashing associates with the whole password, not a specific character or letter/symbol.

> GreaterIowaIsAwesome → see the characters completely change even with just a change in two letters → 8b4d0b85802481ac092532c49cc71633

See for yourself how Hashing can scramble any sort of input: https://www.md5hashgenerator.com/

What does all of this mean? Hashing makes your password more secure because it's not stored as plain text. However, hackers are becoming smarter and more savvy every day, making it even more crucial to create a strong password to further prevent these hacks from taking place.

See how different companies are protecting passwords for everyone! https://www.youtube.com/watch?v=cczlpiiu42M

Article written by Kyle Hauswirth (IT Support Specialist) of Greater Iowa Credit Union