INNNOVATE

SHOULD YOU BE USING A PASSWORD MANAGER?

BY HEATHER REMER, CEO, COMPUTERCARE, LLC

Last month, I talked about the coming "password apocalypse," which was basically my way of getting your attention so you protect yourself from the perils of a compromised password.

In keeping with the theme of password security, this month, I would like to dig more into the use of password managers. As I mentioned in my last article, using short passwords, using predictable passwords and reusing passwords are all things many of us do that are inherently risky. Password managers are used to help mitigate those risks. Basically, a password manager generates complex passwords for you and then stores and organizes them (usually in an encrypted format). You have to remember only one master password that allows you access to the vault where all your passwords are kept. You can set your password manager to log in to sites automatically and automatically fill out forms as well. These applications can be cloud based or stored locally on your machine(s). Let's take a look at the advantages and vulnerabilities of this approach to password management.

ADVANTAGES

- There is so much less to remember, and you save time! No more having

to go through the process of resetting your password every third time you log into a site because you've forgotten it.

- The passwords generated are random and much more secure than pretty much anything that can come out of your head.
- Each website has its own unique password.
- You can synchronize your information across multiple computers and devices.
- Your password manager can automatically fill in not just passwords but common web forms as well.
- You can store notes specific to the website or password with the password information in the application itself.
- You can use your password manager regardless of the browser you are using.
- Speaking of browsers, independent password managers are better than using the integrated password managers in your browsers that are not always encrypted and don't sync well between devices (depending on the browser used). There are more weaknesses to browser password managers, but in summary (and in my opinion), browser-based password managers are more about saving time and less about overall password management.
- Password managers can help protect you against phishing because they can scan the URLs you are at before auto-filling the form and giving away your login information.

DISADVANTAGES

- While you have the benefit of only having to remember one password, if that one password is compromised, everything is compromised. I'll address this more in the conclusion.

- If someone has access to your computer, they could have access to your passwords (for example, if you leave your password manager application open on your desk and walk away for coffee).
- A virus or malware could gain access to whatever is stored on your computer (this is less of an issue if you are using a cloud-based password manager).
- If a keylogger gets installed on your computer, then all bets are off because your keystrokes would be logged.

So, yes. If someone gets your master password, you are in trouble. But, here is the thing: As blogger Neo Notenboom puts it, "Avoiding technology specifically designed to keep passwords secure doesn't increase your security. When you factor in human nature, it actually significantly decreases overall security." What's more, if you are doing the things that you absolutely should be doing anyway (which include ensuring you have a high-quality, up-to-date anti-malware solution running on your devices and ensuring your computers are up to date with all necessary patches and fixes), then you are much safer going with a password manager than going it alone.

So, which password manager do I recommend? Personally, I use LastPass, which is cloud based. But, there are others like RoboForm, KeePass (KeePass is locally housed on your computer) and SafeWallet out there, all with their own pros and cons.

Remember: Make your master password super secure, and keep it that way. Use multi-factor authentication whenever possible, and keep your computers and antivirus up to date. Security and convenience really do live on opposite ends of a continuum — it's all about risks and trade-offs. In my opinion, if used properly, password managers are the way to go and sit right where I want to be on the convenience-security continuum.

HEATHER REMER is co-owner and CEO of ComputerCare LLC, an IT services company providing a full spectrum of IT solutions and services to small and medium businesses.