THE GLOBE AND MAIL

Online password overload making your head explode? A cyberfraud expert has the answer

ROB CARRICK
PERSONAL FINANCE COLUMNIST
PUBLISHED JULY 16, 2019 UPDATED JULY 17, 2019
22 COMMENTS

Technology's most epic fail of the past two decades is arguably that passwords are still being used for internet security.

Passwords were manageable 20 years ago, when we frequented a small number of websites at most and few or none of them involved money. Today, many of us have half our lives online. Bank and investment accounts, social media, subscriptions and accounts at online stores, various utilities and the Canada Revenue Agency.

We have more passwords than ever to keep track of it, and they're getting harder to remember. Many websites are prudently not letting people use easy-to-guess passwords such as 123456 or, yes, password. You've got to mix in upper and lower case letters, numbers and sometimes keyboard symbols such as @ and *. On your own, you're supposed to upgrade old passwords to this higher standard.

Help is coming slowly for the password-afflicted. More and more mobile apps, including some for banking, can be opened by using the fingerprint reader on your phone or tablet, and some smartphones can be unlocked by using an eye-scan or facial-recognition software. But until these measures are packaged in a way that makes them available for computers as well as mobile devices, passwords will continue to be a part of our lives.

That means you either play it fast and loose with passwords and hope your computer isn't hacked, or you create long, cryptic passwords for each of your accounts and commit them to memory. Open to a third option? Consider the password manager, which is a secure virtual vault where you store the login and password for all your online accounts on all your devices.

You can create the most brutally complex password ever for your password manager because it's the only one you'll need to remember. Log into the password manager and it looks after everything – passwords for the website of your bank, your investment firms,

the account with your water utility, the company where you buy concert tickets, your Spotify account and more.

Sandy Boucher, a specialist in fraud investigations at Grant Thornton, made the switch to a password manager after deciding that his own personal system of keeping track of passwords wasn't secure enough.

"I'm very confident that this is a great big step up in my personal password security from what I was doing before," he said.

As part of his job, Mr. Boucher has observed how people manage their passwords. He's seen people keeping passwords on sticky notes attached to a computer monitor, or on virtual stickies on the computer screen. He's also seen people store passwords in Microsoft Word documents, sometimes with "passwords" used as the file name.

One of the riskier ways he's seen people manage their passwords is by activating the auto-fill function on their web browsers (browsers typically give you the option of using auto-fill to remember passwords). He said he was told by the forensics people at his firm that these passwords are easy to find if someone hacks their way into your computer. "They'll have the laundry list of all your logins stored on the browser."

There's a good variety of password managers available either for free or with a monthly or annual cost. To compare, try googling "best password manager." Mr. Boucher says he tried a free product and, after he found it lacking, asked the techies at his firm for some suggestions. He ended up choosing LastPass, which is available with a free 30-day trial and then costs US$36 a year for one user and US$48 for families.

The obvious risk in using password managers is that they offer one-stop shopping to hackers seeking access to your financial accounts. LastPass uses strong encryption and says it has no access to the data stored in a client's vault of passwords. Still, online security experts have found potential flaws in password managers that could conceivably make them vulnerable to a hacker who has access to a computer.

Mr. Boucher acknowledged the risks associated with password managers, but believes they protect passwords better than the measures taken by so many internet users. "There's no question in my mind that by using a good quality password organizer, you are significantly reducing risk."