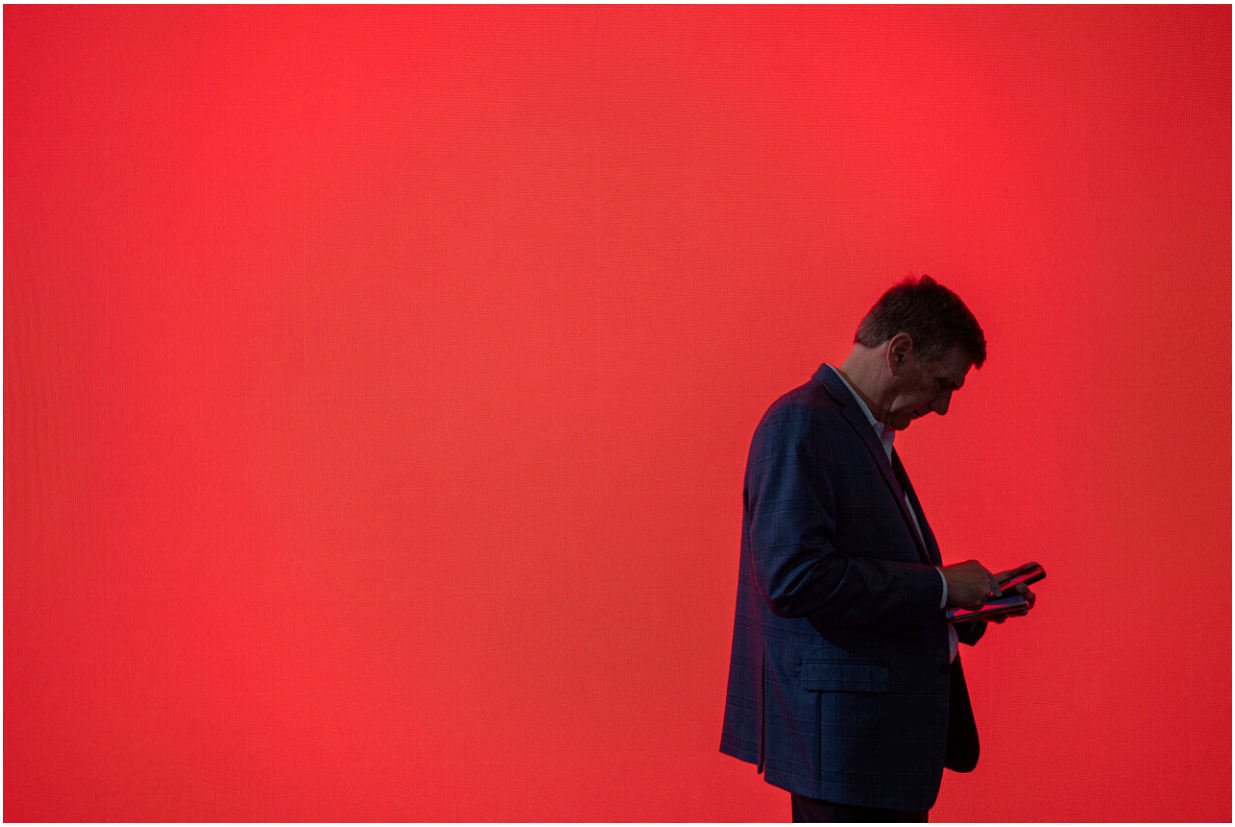
One Tech Tip: Too many passwords to remember? Try using a password manager

June 27 2024, by Kelvin Chan



A visitor looks at his phone at the Mobile World Congress 2024 in Barcelona, Spain, Feb. 27, 2024. According to some un-scientific studies, the average person has hundreds of passwords to their name. Credit: AP Photo/Pau Venteo, File

Everyone has too many passwords. The credentials we need to remember

to navigate online life keep multiplying, not just for frequently used email, banking, social media, Netflix and Spotify logins, but also, say, the little-known e-commerce site you're not sure you'll buy from again.

According to some unscientific studies, the average person has hundreds of passwords. That's a lot to keep track of. You might be tempted to recycle them, but it's one of the bad password habits that cybersecurity experts warn against.

Instead, use a password manager. They've been around for a while and can be useful tools to keep on top of your credentials. But they can also be intimidating for those who aren't tech-savvy.

Here's a guide on how to use them:

Why should I use a password manager?

Many people just use the same password for all their online accounts, mainly because it's the most convenient thing to do.

Don't!

If your credentials are caught in a cyber breach, the hackers could try using the stolen passwords to get into other services.

Other no-nos: Using easily guessed information like birthdays, names of family members, favorite sports teams, or simple phrases like abc123.

The best strategy, experts say, is to use a different password for each account, the longer and more complex the better, backed up by two-factor authentication where possible.

But it's impossible to remember all those various codes. So let a

password manager do the job.

How does a password manager work?

The basic concept is simple: Your passwords are stored securely in a digital vault. When you need to access an online service, it auto-fills the login and password fields. The only thing you'll need to remember is a single password to open the password manager.

Most password managers have a smartphone app that works with mobile browsers and other apps and can be opened with a thumbprint or facial ID scan. If you're using a computer, you can also log in to your password vault through a browser plug-in or by going to a website.

A good password manager should also be able to generate complex passwords with letters, numbers and symbols, for whenever you're setting up a new account. And it should also recognize that you're signing into an online service for the first time and ask if you want to save the credentials you've entered.

Password managers can also help you avoid falling prey to phishing scams. Those deceptive emails from fraudsters trying to trick you into clicking a link to a phony website designed to harvest login details? A password manager won't automatically fill in the details if the web address doesn't match the one linked to the saved password.

They don't just store passwords. You can save bank and credit card PINs, for example. Many also support passkeys, a new technology that companies like Google have been rolling out as a safer alternative to passwords.

How do I choose the best one to use?

There are dozens of password managers on the market, so it can be hard to figure out what's best for you.

Better-known platforms include 1Password, Bitwarden, Dashlane, Bitdefender, Nordpass, Keeper and Keepass.

Check out the many tech review websites that have conducted in-depth testing and compiled rankings of the most popular services. If you want to nerd out, users on Reddit have drawn up spreadsheets with side-by-side comparisons. Britain's National Cyber Security Centre has a buyer's guide.

Most services have free and paid versions. The paid options typically cost a few dollars a month while the free offerings tend to have restrictions like allowing only one device to be logged in at a time or limiting the number of passwords you can store.

If cost is a factor, Bitwarden's free service gets top marks from reviewers, though it's less polished and not as immediately intuitive to use.

A good password manager will work across different devices and platforms, with apps for Windows and Mac computers and iOs and Android devices, and plugins for browsers like Chrome, Safari, Firefox, Edge, Brave and Opera

There are also basic browser-based password managers as well as Apple's iCloud Keychain for Macs and iOS devices. The iPhone maker is aiming more directly at the market with a new Passwords app that will roll out in the fall.

But are they secure?

Cybersecurity worries around password managers flared up after one service, Lastpass, reported a security breach, leading experts to recommend avoiding it.

Don't let that put you off. For one thing, experts advise that saving credentials in a password manager is much safer than letting, for example, e-commerce sites do it.

Good password managers use strong encryption that prevents anyone else from seeing your data.

Many services use AES-256 encryption, which is considered the most secure type "and impossible to be brute-forced by today's technology," said Pieter Arntz, senior malware intelligence researcher at cybersecurity company Malwarebytes.

Strong encryption "ensures that even if your computer or your password manager is compromised, the attacker cannot simply read all your passwords, because they are stored encoded and the attacker will need the master password to decode them," Arntz said.

A good password manager should also hold regular security audits and inform users quickly if there's a breach.

Many services store data in the cloud. If you're worried about that, some let you store them only on your local device, but it can be a complicated process.

Citation: One Tech Tip: Too many passwords to remember? Try using a password manager (2024, June 27) retrieved 7 August 2024 from https://techxplore.com/news/2024-06-tech-

passwords-password.html