What is credential stuffing and how can I protect myself? A cybersecurity researcher explains

January 18 2024, by David Tuffley

Credit: Pixabay/CC0 Public Domain

Cyber-skullduggery is becoming the bane of modern life. Australia's prime minister has called it a "scourge", and he is correct. In 2022–23, nearly 94,000 cyber crimes were reported in Australia, up 23% on the previous year.

In the latest high-profile attack, around 15,000 customers of alcohol retailer Dan Murphy, Mexican restaurant chain Guzman y Gomez, Event Cinemas, and home shopping network TVSN had their login credentials and credit card details used fraudulently to buy goods and services in what is known as a "credential stuffing" attack.

So what is credential stuffing—and how can you reduce the risk of it happening to you?

Re-using the same login details

Credential stuffing is a type of cyber attack where hackers use stolen usernames and passwords to gain unauthorized access to other online accounts.

In other words, they steal a set of login details for one site, and try it on another site to see if it works there, too.

This is possible because many people use the same username and password combination across multiple websites.

It is common for people to use the same password for multiple accounts (even though this is very risky).

Some even use the same password for all their accounts. This means if one account is compromised, hackers can potentially access many (or all) their other accounts with the same credentials.

'Brute force' attacks

Hackers purchase job lots of login credentials (obtained from earlier data breaches) on the "dark web".

They then use automated tools called "bots" to perform credential stuffing attacks. These tools can also be purchased on the dark web.

Bots are programs that perform tasks on the internet much faster and more efficiently than humans can.

In what is colorfully termed a "brute force" attack, hackers use bots to test millions of username and password combinations on different websites until they find a match. It's easier and quicker than many people realize.

It is happening more often because the barrier to entry for would-be cybercriminals has never been lower. The dark web is readily accessible and the resources needed to launch attacks are available to anyone with cryptocurrency to spend and the will to cross over to the dark side.

How can you protect yourself from credential stuffing?

The best way is to *never* reuse passwords across multiple sites or apps. Always use a unique and strong password for each online account.

Choose a password or pass phrase that is at least 12 characters long, is complex, and hard to guess. It should include a mix of uppercase and lowercase letters, numbers, and symbols. Don't use pet names, birthdays or anything else that can be found on social media.

You can use a password manager to generate unique passwords for all your accounts and store them securely. These use strong encryption and are generally regarded as pretty safe.

Another way to protect yourself from credential stuffing is to enable two-factor authentication (2FA) for your online accounts.

Two-factor authentication is a security feature that requires you to enter a code or use a device in addition to your password when you log in.

This adds an extra layer of protection in case your password is stolen. You can use an app, a text message, or a hardware device (such as a little "key" you plug into a computer) to receive your two-factor authentication code.

Monitor your online accounts regularly to look for any suspicious activity. You can also check if your email or password has been exposed to a data breach by using the website Have I Been Pwned.

You may be surprised by what you see. If you do discover your login details on there, use this as a timely warning to change your passwords as soon as possible.

Eternal vigilance

In today's world of rising cybercrime, your best defense against credential stuffing and other forms of hacking is vigilance. Be proactive, not complacent about online security.

Use unique passwords and a password manager, enable two-factor authentication, monitor your accounts, and check breach notification sites (like Have I Been Pwned).

Remember, the recent attacks on Dan Murphy, Guzman y Gomez, and others show how readily our online lives can be disrupted. Don't let your credentials become another statistic. As you are reading this, the criminals are thinking up new ways to exploit our vulnerabilities.

By adopting good digital hygiene and effective security measures, we can take back control of our online identities.

Provided by The Conversation

Citation: What is credential stuffing and how can I protect myself? A cybersecurity researcher explains (2024, January 18) retrieved 8 May 2024 from https://techxplore.com/news/2024-01-credential-stuffing-cybersecurity.html