CYBERRISKS&LIABILITIES

Credential Stuffing

If and when you get hacked, it's easy to think cyber criminals used some high-tech program or code to gain access to your accounts. The truth is, however, that data breaches aren't always this sophisticated, and all malicious parties need is a little trial and error to steal your personally identifiable information. This tactic is known as credential stuffing, and it's becoming a common tool for cyber criminals of all kinds.

Simply put, credential stuffing attacks are when a malicious party takes a stolen username and password and tries it on a variety of different websites. For example, a hacker may have purchased your Google username and password from the dark web.

Assuming that you use the same password for multiple accounts, the hacker would test these credentials on other platforms (e.g., banking or social media websites) using botnets (groups of computers tasked with various commands). Essentially, by using information from one account, criminals can potentially access data from a variety of platforms, draining bank accounts or gathering information they can sell to other malicious parties.

Credential stuffing can affect everyone, from individual users to the biggest companies. In fact, a Yahoo breach that impacted approximately 500 million users was largely carried out using credential stuffing.

Thankfully, because credential stuffing relies on victims having the same password for multiple accounts, there are some simple ways to protect yourself:

- **Avoid using the same password for multiple accounts**—Credential stuffing works because many users use the same password for multiple accounts. Be sure to change your passwords often and never use the same password across different accounts.
- **Use two-factor authentication**—While complex passwords can deter cyber criminals, they can still be cracked. To prevent cyber criminals from gaining access to your accounts, two-factor authentication is key. Through this method, users must confirm their identity by providing extra information (e.g., a phone number or unique security code) when attempting to access corporate or personal applications, networks and servers. This additional login hurdle means that would-be cyber criminals won't easily unlock an account, even if they have the password in hand.
- **Create strong password policies**—For employers, ongoing password management can help prevent attackers from compromising your organization's password-protected information. You'll want to create a password policy that requires employees to change their password on a regular basis, avoid using the same password for multiple accounts and use special characters. Long passphrases are becoming increasingly popular as well, and may be a good option for your organization.
- **Provide security training**—Even the most robust and expensive data protection solutions can be compromised should an employee click a malicious link or download fraudulent software. As such, it's critical for organizations to thoroughly train personnel on common cyber threats and how to respond. Your employees should also know your cyber security policies and know how to report suspicious activity.

For additional cyber risk management guidance and insurance solutions, contact us today.

SCS AGENCY INSURANCE