Commit To Password Hygiene Or Resign To Getting Hacked

(NAPS)—Passwords—they're so ubiquitous, yet are the source of so many online hacks due to poor password hygiene. According to a recent Aware poll, more than 50 percent of people choose to use the same password across multiple accounts, which means that if a hacker has a password to one account, they can likely access several of that person's accounts. In fact, almost 70 percent of people remember passwords by picking those that are easy-to-use, or writing them down on a stray piece of paper.

Currently, there are billions of passwords available on the Dark Web, all aggregated through various attack methods, from malware and phishing to brute force. Passwords are highly prone to being weak, stolen, or lost—which brings up the question: Why don't people adopt more sophisticated techniques?

What is Password Hygiene?

Password hygiene is the practice of ensuring passwords are strong (hard to guess) and not prone to theft or loss. Best password hygiene practices include choosing unique passwords for each account, routinely changing passwords and never storing them somewhere obvious. But with people's attention spans and patience so often stretched, does anyone really do this?

Alternatives to Traditional Passwords

Nearly 67 percent of Aware survey respondents know people who have been victims of account hacks. Unfortunately, the likelihood of those hacks will only continue to grow as cybercriminals get smarter and their methods become more agile. With all the problems around passwords, what are some more sophisticated approaches that could supplement or replace them?

1. Use two-factor authentication: Two-factor authentication requires an additional step before the user logs into the account. It typically is a one-time password via text, phone or email to ensure that only the account owner can gain access. Many websites do let users override two-factor authentication for trusted devices, so be sure not to do this, no matter how convenient it may seem.

2. Leverage a password manager: Password managers help users generate strong passwords and store them all in one encrypted place, alleviating the burden of remembering individual passwords for every account. In fact, you need to remember only one password in order to access that password manager.

Passwords can be a problem, a recent survey found, but one you can easily fix.

Password managers can be a great organizational tool but aren't foolproof; if someone gains access to the password manager account, they have access to all the passwords stored within, which could be disastrous. Additionally, should a password manager company experience a data breach, all of its customers would be in danger.

3. Implement "passphrases" instead of passwords: Many organizations have begun locking sensitive data behind passphrases, not passwords. Instead of a password constructed by letters, numbers and symbols, some organizations require users to type out a whole phrase or sentence to access sensitive data. Again, this isn't a foolproof method, as sentences and phrases can also be guessed, but the length and strength of that passcode definitely supersede that of a password, making it more difficult to guess.

4. Biometrics: Biometric authentication methods are considered the strongest means of authenticating people because they rely on something that can't be stolen or guessed at: their face, voice, fingerprints or iris. In addition to its superior security, biometric authentication is highly convenient, and the widespread presence of cameras on computers and smartphones makes it very easy to implement. The Aware survey also found that most consumers would choose to replace passwords with biometrics for most online services, including shopping and banking.

It's never been more important for users to adopt good password hygiene in both their personal and their work lives. Between those efforts and the growing implementation of biometric security, it's possible to reduce the incidence of cybercrime.

Learn More

For further facts, visit www.aware.com.