6 Tips for creating secure passwords

By Doros Hadjizenonos

13 May 2019

Passwords are like toothbrushes - you want to choose a good one, never share it, and replace it quarterly.

Doros Hadjizenonos, Regional Director – SADC at Fortinet

Earlier in May, World Password Day was celebrated. The goal is to promote better cybersecurity hygiene by upgrading easy-to-guess passwords or refreshing older passwords that may have been compromised through some data breach. Think of it as the cyber equivalent of testing and replacing the batteries in your car's key remote.

Weak passwords create security risks

According to the Verizon Data Breach Investigations Report, 81% of breaches leveraged either stolen and/or weak passwords. That problem is compounded because one of the biggest risks to data security is the reuse of passwords across accounts.

If one of your accounts is compromised and your user name and password are posted on the dark web, cybercriminals who know how often passwords are reused will simply begin to plug that information into other possible accounts until they unlock one that uses the exact same credentials.

This is a common risk, as 83% of people have admitted to reusing passwords across multiple sites. Even if you think it is safe to reuse passwords on accounts that don't house sensitive data – a breach there can be used as an entryway to move laterally across networks in search of critical business data or personally identifiable information (PII).

What constitutes a weak password?

Short, simple passwords take fewer resources for hackers to compromise. In fact, hackers maintain databases of the most common words, phrases, and number combinations that they can run your password through to find a quick match.

Some of the most common passwords are baseball and football team names, any variant of 123456789, and QWERTY. Avoid using common password themes when creating a passphrase, such as the following:

1. Birthdays
2. Phone numbers
3. Names including movies and sports teams
4. Simple obfuscation of a common word ("P@$$w0rd")

How to minimise password-based cyber risk

When creating new accounts or updating well-used passwords, keep these six best practices in mind to minimise password-based cyber risk.

1. To add an extra layer of security, use multi-factor authentication wherever possible. This confirms your identity by utilising a combination of multiple different factors, such as something you know or something they have, such as a token generator on your smartphone.

2. Never repeat the same password for different accounts.

3. Change your passphrase at least every three months. This will lock out cybercriminals who may be using your account, protect you from brute force attacks, and remedy the issue caused by cybercriminals who purchase lists of usernames and passwords obtained through data breaches.

4. Ensure no one is watching as you enter passwords.

5. Be cautious when downloading files from the internet as they may contain key loggers as well as password grabber malware variants that will compromise your password. A good practice is to regularly scan for the presence of such malware.

6. Use a cloud-based password manager to enable you to create and store strong passphrases. This is especially

important if you require strong passwords for dozens of accounts. Password management tools allow you to securely store an encrypted list of passwords in the cloud that can be accessed from any device. Not only will you only need to remember one password to access your password locker, but the passwords you store there for your various accounts can also be even stronger because you don't have to remember them.

Final thoughts

When it comes to password security, everyone has a role to play in the protection of PII and corporate data. IT teams and stakeholders should review the common risks of weak passwords with their organisations, as well as remind everyone of these best practices. This simple practice can help employees better protect their data while minimising unintentional insider threats to the organisation.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet
- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...