BIZCOMMUNITY

# How to have strong cyber hygiene

By Doros Hadjizenonos

26 May 2020

Cyber threats do not rest and they continue to evolve and bad actors develop new attack techniques. Good cybersecurity hygiene requires more than a strong password to avoid compromise.

Source: www.pexels.com

The most important thing is to know how exactly cybercriminals may attempt to gain access to your data.

They will try the following techniques:

- **Password Spraying**: A form of brute force attack that targets multiple accounts in which adversaries try multiple guesses of the password on a single account that often leads to account lockout. With password spraying, the adversary only tries a few of the most common passwords against multiple user accounts, trying to identify that one person who is using a default or easy-to-guess password and thus avoiding the account lockout scenario.

- **Key logging attack**: By installing keylogging software on the victim's machine through usually some form of email phishing attack, the adversary can capture the keystrokes of the victim such as their username and passwords for their various accounts.

- **Man-in-the-middle**: Adversary insert themselves in the middle of the user and the intended website or application, usually by impersonate that website or application. The adversary then captures the username and password that the user enters into the fake site. Often email phishing attacks lead the unsuspecting victims to these fake sites.

- **Social engineering attacks**: Attacks such as phishing through emails and texts, where users are tricked into providing their credentials, clicking on malicious links or attachments, or going to malicious websites.

- **Brute force Attack**: An approach in which adversaries randomly generate passwords and character sets to guess repeatedly at passwords and to check them against an available cryptographic hash of the password.

- **Traffic Interception**: Criminals use software like packet sniffers to monitor and capture the network traffic that contains password information. If the traffic is unencrypted or using weak encryption algorithms, then capturing the passwords becomes even easier.

- **Dictionary attacks**: Attacker uses a list of common words, called the dictionary to try to gain access to passwords in anticipation that people have used common words or short passwords. Their technique also includes adding numbers before and/or after the common words to account for people thinking that simply adding numbers before and/or after makes the password more complex to guess.

It is necessary to have passwords that are impossible to forget and difficult for someone else to guess. It might seem like a good idea to add numbers and special characters to words, but cybercriminals can leverage a number of attack techniques to crack this.

At Fortinet, we recommend avoid using phone numbers, company information, birthdays, names including movies and sports teams, simple obfuscation of a common word ("P@$$w0rd").
Instead, use the following best practices to secure your information:

- Change your password every three months to decrease the likelihood that your account will be compromised.
- Leverage unlikely or seemingly random combinations of uppercase and lowercase letters, numbers and symbols, and make sure your passwords are at least ten characters long.
- Use a password manager to generate unique, long, complex, easily changed passwords for all online accounts and the secure encrypted storage of those passwords either through a local or cloud-based vault.
- Do not use the same password for multiple accounts, this increases the amount of information a cybercriminal can access if they are able to compromise your password.

As the pandemic is forcing us to increase the amount of time we spend online for work, e-learning and communicating with family and friends, cybercriminals ramp up attacks targeting users. It is important to perform a security posture check across all accounts on updating weak and outdated passwords as needed.

## 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...