NEED TO KNOW NEWSLETTER | MAY 2022

World Password Day (May 5th)

World Password Day aims to educate and remind people how to create strong passwords to secure their personal information, accounts, and data. It brings awareness to new technologies that impact our journey to creating strong security practices, such as Multifactor Authentication apps and Single-Use code messages. This month's newsletter will highlight the ever-evolving use of passwords and how we should best be protecting ourselves today.

Password security is constantly evolving — with more work to be done

The password first made its appearance in the early 1960s when Fernando Corbató, a computer scientist at MIT, wanted a way to secure private files by users as they all completed research on one shared system.

This newly created system of passwords was only used in the research and academic field. As computers became more popular, hackers started finding their way into computer systems with the weaknesses of using and creating passwords.

The first password breach happened just a few short years after the password became used. A Ph.D. candidate wanted more than his given 4 hours a week to work on the MIT computer system, so he found a way to print the system's password file and log into the system using other people's accounts.

In 2020, according to Verizon's Data Breach Investigation Report, it was reported that over 80% of data breaches were because of lost or stolen credentials. This proves that we still have a long way to go in securing our passwords.

Implementing security measures such as using a passphrase instead of a password is one way to increase protection against lost or stolen credentials. A passphrase is a "short combination of words that mean something to the user. It can make the user more likely to create unique logins for every account they own instead of reusing a single password on multiple accounts."

Also, enabling Multifactor Authentication (MFA) is key for password protection. MFA adds a layer of security by making you use another device or code to access your account, even after putting in your password.

Try out a password manager — LastPass

You're always hearing about creating a secure password, but how do you keep your secure passwords secure? Using a password manager app can help you remember (or forget) passwords and keep them safely stored.

There are three different tiers of the LastPass service: a free version, a premium version and a family version. You can purchase these through any app store or their website. The free version of LastPass offers:

1. Storage of unlimited passwords, documents, SSNs etc.
2. Autofill passwords
3. Multi-factor authentication
4. Access with fingerprint
5. Strong password generator

How passwords get hacked

Hackers use a variety of different ways to hack passwords. As technology improves, hackers have found different methods of breaking and entering.

Dictionary attack: The computer generates every word possible as a password until it finds the right word. Using a solid passphrase is what can stop this type of attack

Brute force attack: This attack finds all possible password combinations possible. Having an account that blocks multiple missed password attempts can stop this type of attack.

Credential stuffing: Once a hacker has access to someone's password, they try that password with other accounts. Having a different password for each account is key to stopping this type of attack.

www.etechcloud.ca | 647-361-8191 | contact@etechcomputing.com

E-TECH