- Computer security

Mind your passwords

Manila Bulletin · 21 Jun 2022 · 7

Passwords have become a vital element of everyone's digital life. Nowadays, each of us manages multiple online accounts in order to fully enjoy the benefits of digital existence.In fact, every online application would require the use of digital identity verification tools such as the use of passwords, thumbprints, facial identity, multi-factor authentication, iris, or a combination of all these tools. The most common of these would be the use of passwords. Data breaches and cyberattacks are becoming to be common today. To ensure that our online identity and private information are kept safe, taking care of our passwords is as essential as ever. But are we serious about it or are we taking passwords for granted? Just one case of passwords being compromised would potentially have life-changing consequences.

Besides our email and social media accounts, we must create an account or register for things like retail loyalty programs, mobile transport apps, online entertainment like Netflix, accessing online resources like reports, and even digital storage apps.If we think about it, we may have created more accounts that we rarely visited because we were required to register in order to access the app. Studies show that the average home user would have around 120 online accounts associated with the same email address while the average business user would usually have around over 190 accounts.

Last year, the cybersecurity world was shocked by the news that about 8.4 billion password entries were leaked on a popular hacker forum. The compilation has been dubbed "RockYou2021" and may be one of the largest collections of leaked passwords which are presumed to be a combination of previous data leaks and breaches. The RockYou2021 leak is almost twice the entire global online population of 4.7 billion people. For that reason, users are encouraged to immediately check if their passwords are included in the leak by visiting the Cybernews Data Leak Checker. The site actually has the largest database of known breached accounts with more than 15 billion compromised accounts.

Obviously, it would be next to impossible for us to remember so many different passwords by heart if we must set up a different one for each account.One of the key elements of a strong password is its uniqueness. But some passwords are anything but that. I have been entertained by what I have heard, and actually have seen, about ridiculous passwords commonly used. During the 90s, it was very common for implemented software applications to initially have a password as the system administrator password. It is not uncommon to discover that, several years later, the initial password provided was not changed at all. You will be surprised to know that among the most common passwords used today are the following: password, 123456, secret, passwordforoldpeople, newpassword, qwerty, and password123.

Today, there is no need to memorize difficultto-remember passwords with the use of Password Managers. They come in both free and paid versions. If you are on a Google platform, you can use the Google Password Manager. Attacks rely on your need to set the same password or similar passwords for multiple accounts. For extra protection, you may want to keep your passwords stored in two separate password managers so have a plan B.

Everyone should set only strong and unique passwords for each online account. Resist the impulse to use the usual go-to password which may hold personal significance. Also, refrain from using default passwords because attackers usually start with those to unlock accounts and devices.

Regular resetting of passwords should be a necessary part of any cybersecurity hygiene policy. Companies would usually require passwords to be changed every six months. They generally restrict their employee's use of work passwords in their personal accounts which is hardly being followed.

As much as possible, it is not advisable to use public wi-fi networks because research shows that these are one of the biggest security risks for any system. If anyone absolutely needs to connect to one, the traffic should be rerouted through a VPN platform. Using a public wi-fi network to log in to an account would, most of the time, result in credentials winding up in a data collection sooner or later.

Most apps today enable the use of two-factor or multi-factor authentication platforms like the use of a one-time pin sent to a registered mobile number or email address. It may not be totally fraud-proof, but it can make it more difficult for cybercriminals to breach online accounts. Multiple layers of security are still better than less when we connect to the internet. With this in mind, everyone needs both an antivirus solution and a shield on top of it. It is always a smart move to keep apps and programs up to date because these updates include security patches.

It is about time that we take the use of passwords or any other digital identity authentication system seriously. As earlier emphasized, the consequences can be life-changing.

(The author is the lead convenor of the Alliance for Technology Innovators for the Nation (ATIN), vice president of the Analytics Association of the Philippines, and vice president, of the UP System Information Technology Foundation.)
mon.ibrahim@aap.ph