



Press release

Digital Security: Is it time to move on from passwords?

Source: Asian Age

Find the link of the news below:

<http://www.asianage.com/decaf/010618/digital-security-is-it-time-to-move-on-from-passwords.html>

Mumbai, Jun 1, 2018

According to many cybersecurity experts, the crux of the problem is in weak, guessable passwords and poor password management.

Passwords, once hailed as the de facto standard of digital security, are now being looked at with suspicion. The buzz in the cyberworld is that they aren't enough to secure our digital identity. The two cyber-attacks (WannaCry and Petya) that crippled many computers across the world have shown that, as technology is expanding its footprints, so are the threats associated with it. In such perilous times, is password protection good enough?

A report released by Microsoft titled Security Intelligence Report Vol22 (January-March, 2017), states: "There has been a surge in the cases of site-breaching and phishing attacks as attackers attempt to reuse the stolen credentials on multiple services". While having different passwords for different platforms may help secure digital locks in a better way, a cognitive phenomenon called "interference of memory" points out that we (an average human mind) cannot firmly remember more than five text passwords on an average. As per the RSA Quarterly Fraud Report for the first quarter of 2018 "Phishing accounted for 48% of all cyber-attacks. Canada, the United States, India and Brazil were the countries most targeted by phishing".

According to many cybersecurity experts, the crux of the problem is in weak, guessable passwords and poor password management. Ankit Jain, CEO, MyOperator, explains the susceptibility of passwords to cyber-attacks. He says, "Most security breaches happen because of some sort of human weakness. Although we know how safe our passwords should be, we tend to ignore this knowledge in favour of using easy-to-remember passwords because the fear of forgetting is stronger than the fear of being hacked."

As per the 'Worst Passwords List' compiled by SplashData, the two most commonly used passwords are '123456' and 'password' and surprisingly, both of them have remained at the top of the index since 2011. Kanchan Ray, VP Technology, Nagarro, told this newspaper that the major problem still is that "These are all security measures being added after-the-fact. Unless critical IT systems (both

software and infrastructure) are redesigned with a 'privacy first' or 'security first' approach where user identity and privacy are at the core, the problems will remain."

This underscores the fact that we (most of us) haven't been able to catch up with the fast-advancing technology.

Kartik Mandaville, founder of SpringRole, a machine-learning based recruiting start-up, believes that connecting online accounts with devices is the way out as it will ensure that no one gets through unless verified by the user himself. "The best way to keep your online accounts is to enable two-factor authentication through a physical device which gives you a one-time code to login. Passwords are obsolete and need to be supplemented with two-factor authentication (or 2FA)," he said.

Today, the businesses (and thereby, transactions) have drifted apart from the physical world to the online medium locked with passwords, which act as gatekeepers to an individual's identity. Thus, easy-to-crack passwords are like chinks in the armour for the hackers. Compromised credentials, especially on financial websites, could lead to significant harm.

Avinash Tiwari, co-founder and director pCloudy, told this newspaper, "Password-only protection is permanently broken, and any organisation relying only on it is placing its business and reputation at risk. Alternatives such as multifactor authentication, behavioural analytics, and biometrics are available, but the adoption rate is low." India's payment industry portrays a paradoxical mixture of technology-deficient public sector units and fast-forward online payment providers. Rajesh Desai, CEO of Lyra Network India, believes that "It is better to prevent and prepare than to repent and repair". "While there have been multiple practices, policies and tools developed to minimise the damage, the threat still prevails," he said.

The US National Institute for Standards and Technology recommends users to come up with a password of 16 characters, ideally a mix of letters and numbers. Rajesh Desai suggests incorporating a secure system of multi-biometrics to secure our online accounts adding that Aadhaar can be a great facilitator for the same. Some cyber experts are of the view that distributed identity management can help figure out the issue. "Decentralised identity stores using blockchain, where no single system has the entire identity, is a promising way to ensure security of accounts," says Mr Ray.

Meanwhile, there are many who believe that passwords are symptomatic of how poorly we envisioned computer security. Shailendra Naidu, CEO of Obopay, points out, "The tech world giants like Microsoft, Apple and Google have efficiently put to use several alternative authenticators like voice print, fingerprints, location based identification, mobile authentication but such authenticators are underutilised and still have a long way to go in gaining user confidence."

To conclude, keeping alpha-numeric passwords, regular updation of passwords, and using different passwords for different platforms, using biometrics, and connecting accounts with physical devices are the most feasible methods to fortify one's online accounts from any cyber threat.

About Lyra:

Founded in 2001 by Alain Lacour, Lyra secures e-commerce and proximity payments and develops value-added services to manage transactions and POS equipment on a daily basis. Based in Toulouse, Lyra is present internationally with 10 subsidiaries (Algeria, Germany, Brazil, Chile, Spain, India, Mexico, Argentina, Colombia and Peru). The group has over 250 employees for a turnover of €53M in 2017.

Lyra's key figures:

Over 10 billion payments secured and transmitted in 2017 worldwide

Over 50,000 e-merchants

Over 3,000,000 payment terminals worldwide

Lyra's services are certified PCI DSS, Visa Merchant Agent and approved by GIE Cartes Bancaires.

<http://www.lyra.com>