CREDENTIAL CARELESSNESS CONTINUES TO BE ONE OF THE LARGEST PROBLEMS FOR CYBERSECURITY IN PRACTICE. MAIN SECUREAUTH 2020 STATE OF IDENTITY REPORT'S FINDINGS AND PERSPECTIVES.

SERGIO GUIDA

Independent Researcher, Sr.Data/Information Governance Mgr.

Key-words: World Password Day - biometrics - security - strong authentication

Category: Technical Area

On May 7, 2020, World Password Day is bringing us to a critical reflection about our credential habits. In principle, everyone knows how passwords are critical gatekeepers to our digital identities, allowing us to access online shopping, dating, banking, social media, private work, and life communications. In his 2005 book 'Perfect Password' security researcher Mark Burnett first encouraged people to have a "password day, where they update important passwords. Inspired by this idea, Intel Security took the initiative to declare the first Thursday in May World Password Day in May 2013.

Your privacy, at its core, relies on your data being secure.

In a cyber-world, secure passwords are essential, so SecureAuth conducted a research investigating our approach to safely and responsibly use applications, portals, systems, business tools, and online accounts in our everyday life. The objective is "to gain a better understanding of the psyche of the average person - from Generation Z to Baby Boomers and beyond - when it comes to security and personal privacy, and the habits that are contributing to the challenge of protecting and securing our online privacy".

With nearly 50% of respondents in 2,000 U.S. general population consumers, the 2020 State of Identity Report provides an objective data set with respect to the security and privacy habits consumers apply in both their personal and professional lives.

Here are the main findings:

1. despite all cyber experts always remember it, "bad password habits" are confirmed as "a large problem for our personal and work lives".

Many people are using the same password for more than one account and most are using it across 3-7 accounts (62%), while 10% say they are using the same password across more than 10 accounts. More,“44% of people have admitted to using their personal passwords at work”.

2. The real problem is that “people are predictable due to truly unique passwords being a headache to remember”.

In workplaces, often management behaves “worse than junior staff at password hygiene”, since only 38% of those occupying leadership positions report they utilize unique work passwords. And “34% of employed people in a director level + role admit to having used one of the most common passwords”.

3. Sharing is not valued as an issue when it comes to passwords.

Video “streaming services accounts have the most shared passwords or login credentials, followed by online gaming accounts and cell phone passwords. The type of account with the least shared credentials passwords” relates to work emails, although 34% reveal that they have “shared their password for the work email”.

4. Most consumers are sharing passwords in ways that facilitate hacking.

20% of consumers admit sharing a password using a text message, 19% a phone call, 15% a written note and 10% by email.

That’s why at the end of the Report we find a Bil Harmer (CISO & Chief Evangelist, SecureAuth)'s statement saying that “it’s important to remember, even if passwords are encrypted, hackers can use brute force against them and find out what they are. Ultimately, the victim will have no advanced warning which is why passwords need to disappear and an elevated form of continuous authentication needs to be implemented”.

So prospectively, **“**the future of identity lies in biometrics” (voice recognition, fingerprint reader, facial recognition, or retina scan) to gain access to secure resources. But “more education must be done to increase appetite and willingness among average consumers”.

At this time, only less than 1 in 3 consumers confirm” they are comfortable sharing some of their biometric data with either a company they purchase goods and services from, or the government”.

Conversely, “despite high levels of discomfort” when specifically asked about (“57% of people say it feels to personal, while 43% believe their data could get hacked”), “data shows people are already using biometrics in multiple contexts” without particular problems. In detail, “51% of consumers are already using biometrics” and they “are willing to share their biometric data to save time: i) 13% will share to save 30 sec or less. ii) 12% will share to save 5 min. iii) 10% will share to save 10 -30 min”.

It appears “the future of protecting our identity and improving security lies in biometrics. For now however, more education and awareness is needed to ease the minds of the average person to improve their appetite and willingness to embrace the potential of biometrics”.

In the meantime, the research clearly identified “that people inside or outside the office are not complying with password best practices which is unfortunately putting our personal data and privacy at risk”.

So, while awaiting for future developments it is worth to summarize the relevant password tips to be followed in this turbulent time:

- change an old password to a strong, unique alphanumeric password that is at least in the double-digits of characters for each account you have.
- Change our passwords every few months or any time we think our accounts could have been compromised.
- Turn on two-factor authentication for your important accounts.
- Password-protect your wireless router.
- Don’t store passwords on your computer or phone.
- Log off when you’re done with a program.
- Periodically remove temporary internet files.
- If you know you have an account that you never use, delete it. Holding onto these old accounts may expose you to greater hacks or intrusions down the line, even if you long forgot about them. But remember, if that account is still linked to other sites and services (like your social networking account or two-factor authentication) an attacker could log into those accounts by resetting your passwords sent to your old email address.
- Each time you install an app, it will ask you for permissions to your phone's features or data, like your contacts, photos, camera, or even the phone dialer itself. Be mindful of apps that you install, as a single rogue app can punch a hole in your privacy protections.
- Using ad-blockers can prevent ads from installing tracking cookies and even malware.
- If you ever use a public network (like a Wi-Fi hotspot, be extremely careful, as every page you visit will expose your personal information, including your usernames and passwords.
- It's not only wise to be careful with what you store in the cloud wherever possible, but also to ensure that your various clouds are secure.

Source: The SecureAuth 2020 State of Identity Report

Link: https://www.secureauth.com/blog/secureauth-2020-state-identity-report.