RE-ISAC Weekly Cybersecurity Report

Real Estate ISAC Information Sharing and Analysis Center

Serving the Commercial Facilities Sector

09 May 2019

This report is **TLP AMBER**. **TLP AMBER**: Limited disclosure, restricted to participants' organizations. Sources may use **TLP AMBER** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share **TLP AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

Find RE-ISAC on Social Media!

FOCUSING ON FUNDAMENTALS: PASSWORD HYGIENE

IN BRIEF: The first Thursday of May is annually recognized as World Password Day. And in celebration of that day, it is appropriate to look at the ways to increase individual and enterprise level password security. Many RE-ISAC Weekly Cybersecurity Reports focus on the various threats, their continued evolution, and malicious actors – and good cyber hygiene, and especially password management, is a key pillar to ensure employees are not unwittingly opening the door, or increasing the attack surface, to an organization. Despite the best efforts of security teams, there do not appear to be an end to the number of data breaches and other cyber-related incidents, with new ones popping up virtually every day. World Password Day also comes on the heels of the UK's National Cyber Security Centre's first UK Cyber Survey in which over 40% expected to lose money online from fraud, and yet over 23 million accounts still used "123456" on their account. With the number of ways cyber-criminals can exploit users, adhering to fundamental cyber hygiene principles, and adding strong authentication can help individuals and organization protect their finances, email, and critical and proprietary information amongst others.

KEY TAKEAWAYS & RECOMMENDATIONS:

- Despite the overwhelming evidence that supports strong passwords, users are oversaturated and continue to exhibit poor password security practices.
- These poor habits not only have a direct impact on the users, but also have an impact on organizations that have to contend with and protect against fraudulent identifies and transactions.
- Organizations can help enforce strong passwords, including implementing two factor authentication, but also need to be on guard against adding unnecessary complexities that only exasperate poor behaviors.

DISCUSSION. When President Skroob of Planet Spaceball was told that the combination to the air shield was the same as the combination on his luggage – 12345 – it was meant to draw a laugh; *Spaceballs* was a comedy after all. However, we are continually reminded that it's not so funny when it happens in real life. World Password Day serves as an annual reminder of the need to protect individual and organizational data and information with strong passwords. With cyber-criminals evolving their attacks to commit any number of crimes ranging from identity theft, to theft of sensitive information or finances, it is important for individuals to practice good cyber discipline and hygiene. Coincidentally, the UK's National Cyber Security Centre's first "UK Cyber Survey" released in April revealed several concerning online behavior

and an overall lack of personal security knowledge and awareness of their online footprints. Additionally, in concert with security expert Troy Hunt, security expert and creator of the "Have I been pwned" website which tracks exposed usernames and passwords from data breaches, the NCSC released the Global password risk list published to disclose passwords already known to hackers from previous data breaches. It would come as no surprise that many of the 100,000 passwords on this list include sequential numbers, common words, a variation of "qwerty" and "password" (see callout box for a sampling). Other password-related findings in the survey include, "70% always use PINs and passwords for smart phones and tablets" but "less than half do not always use a strong, separate password for their main email account."

What are some of the reasons that may contribute to poor password hygiene?

- Too many websites with too many different logins.
- The password complexity makes it too difficult to remember.
- Malicious actors aren't interested in anything I have.
- If they haven't gotten me yet they won't get me in the future

What users do not always appreciate is that when attackers steal their username and passwords, **the attack is not always designed to target them and steal from them, but rather to use for larger attacks or to sell on the dark web to other malicious actors who will use to create false identities**. So, while not directly impacting the user at that point in time, it can have longer, far-reaching consequences. Troy Hunt further stressed the impacts of this point. "[when discussing] how terrible passwords are and the impact this then has on individuals and organizations alike, one of the big problems I've seen really accelerate over the last year is credential stuffing. In other words, bad guys grabbing huge stashes of username and password pairs from other data breaches and seeing which ones work on totally unrelated sites." **Because users are using the same username and passwords on their sites, if they are able to gain this information then then could conceivably use it elsewhere to create fraudulent transactions which could impact the business and create a mess with the user to resolve / contest the transaction.**

Ultimately, most experts agree that the most effective solution involves the transition to multi-factor authentication (MFA) often meaning two-factor authentication (2FA), and is simply adding a second layer of protection above simple username and password. The second factor promotes three requirements, such as something you know (password), something you have (such as a one-time password/passcode (OTP)), and something you are (biometrics – fingerprint or FaceID). Some MFA even uses USB tokens. MFA is now often seen with financial institutions, and social media applications. For example, some banks now require MFA for "high risk" transactions such as transferring money, adding additional accounts, or paying bills. Other platforms will use it if the user is logging in from an unfamiliar platform or location. Of course, one of the negative aspects to MFA is the perception of all the extra time incurred by adding another level, but the reality is that this extra step takes less than a minute to activate. There is even a movement - #layerup - to help encourage individuals to protect themselves and their identity by enabling MFA.

So, what does good cyber hygiene look like for passwords? For starters, it's important to remember that these passwords are protecting you and your data. They are designed to prevent someone from getting in so effort has to be made to ensure they are not predictable or easily guessed by random crooks, complex algorithms, or easily applied in credential stuffing attempts. The UK's National Cyber Security Center (NCSC) promotes the idea of using, "Three random words or #thinkrandom." While incorporating MFA is seen as a recommended path, some platforms have not

Global Password Risk List Sample

123456
123456789
qwerty
password
111111
12345678
abc123
1234567
password1
12345
1234567890
123123
000000
iloveyou
1q2w3e4r5t
qwertyuiop
monkey
dragon
123456a
654321
123321
666666
1qaz2wsx
myspace1
121212
homelesspa
123qwe
a123456
123abc
1q2w3e4r
qwe123
7777777
qwerty123
target123

adopted it completely so there are other steps organizations can take to ensure they have good password hygiene also includes:

- **Never give out your password to anyone. Period.** Seems obvious but you never know. And if there is a time when you have to reveal your password, make sure you change it immediately thereafter.
- **Don't use just one password**. This is becoming harder and harder especially since most platforms require a unique username and password that it can be hard to keep track of. **Password Managers are always helpful in these instances.** As noted by Consumer Reports, "Earlier this year, researchers discovered a treasure trove of more than 2.2 billion stolen email addresses and passwords posted online. The data didn't appear to stem from a massive new data breach. It was more likely an aggregation of consumer information stolen over the years from companies such as Dropbox, LinkedIn, and Yahoo. So, if your login credentials for your favorite blog get swiped, it could threaten your online banking account if you used the same email and password for both."
- **Make the password or pass phrase at least 12 characters long and use numbers, capital letters and symbols**. One of the best and easiest things to do is to create a long password out of an easy-to-remember phrase, then throw in some special characters.
- Consider using a $ instead of an S or a 1 instead of an L, or including an & or % – but note that $1ngle is NOT a good password. Password thieves are onto this. But Mf$J1ravng (short for "My friend Sam Jones is really a very nice guy) is an excellent password."
- **Don't use dictionary words**.
- **Don't post it in plain sight**. Hint, under your keyboard is not a good idea.
- **Don't fall for "phishing" attacks**. The strongest password is immediately undermined if click on a link or open an attachment loaded with malware.
- **Make sure your devices are secure**. Use a password, pin or fingerprints for your phones or tablets too. The UK survey found 70% do, which also means 30% don't.
- **Consider using multi-factor authentication**.

Or it can be as simple as what's listed on the Microsoft Support page:

- Is at least eight characters long;
- Doesn't contain your user name, real name, or company name;
- Doesn't contain a complete word;
- Is significantly different from previous passwords;
- Contains uppercase letters, lowercase letters, numbers, and symbols.

In 2018, security firm LastPass reviewed whether data breaches or security incidents had any impact on improving password security. There findings may be somewhat surprising, or maybe not:

1. We keep using the same password again and again.
2. Our brains are oversaturated.
3. We treat work and personal accounts with the same indifference.
4. Breaches don't faze us.
5. Oh wait, we were breached. Still not fazed.
6. We think Instagram posts are for friends' eyes only.
7. We love a good old-fashioned spreadsheet (for tracking our passwords).
8. We don't think we are hack-worthy.
9. We're a little lazy.
10. We'd rather clean the house.

With the global marketplace moving almost exclusively online, and the ability to access sites using other accounts and platforms, the need to practice good password security is at an all-time high. However, the challenges and complexities of creating a password used by some organizations contribute to poor practices. **By adhering to the principles outlined above, and if organizations begin to implement and enhance 2FA or MFA, it may not prevent all password issues, but it can help lower the risk and may enable the other elements of the security plan to stop a more complex attack saving an organization from the larger impacts of a full breach.**