March 2016
Volume 11, Issue 3

Why *Strong, Unique* Passwords Matter

OhioDAS
SERVICE · SUPPORT · SOLUTIONS
DEPARTMENT OF ADMINISTRATIVE SERVICES

Office of Information Security and Privacy

From the Desk of Russ Forsythe, Interim Chief Information Security Officer

Cybersecurity experts continually identify the use of *strong, unique* passwords as one of their top recommendations. However, this is also one of the least commonly followed recommendations because unless you know the tricks, it's difficult to remember *strong, unique* passwords for every login and website.

Why Strong, Unique Passwords Matter

A strong *password consists of at least 10, and includes a combination of uppercase and lowercase letters, numbers, and symbols. A* unique *password is a password that is only used with one account.*

Cybersecurity experts make the recommendation for *strong, unique* passwords for several reasons – the first being that every day malicious cyber threat actors compromise websites and online accounts, and post lists of usernames, email addresses, and passwords online. This exposes people's passwords, and worse yet, they are exposed with information that uniquely identifies the user, such as an email address. That means that a malicious actor can look for other accounts associated with that same person, such as work related, personal social media, or banking accounts. When the malicious actor finds those accounts they can try logging in with the exposed password and if the password is reused, they can gain access. This is why *unique* passwords matter.

Secondly, when malicious cyber threat actors can't easily find or a guess the password, they can use a technique called *brute forcing*. This is a technique where they try every possible password until the correct password is identified. Computers can try thousands of passwords per second, but for this technique to be worthwhile, the malicious cyber threat actor needs the password to be easy to identify, which is why a *strong* password matters. The stronger the password the less likely brute forcing will be successful.

When malicious actors use brute forcing techniques they often try every word in the dictionary because it's easier to remember words than random letter combinations. This technique is not limited to English-language dictionaries, so switching languages will not help. And since many passwords require a combination of uppercase and lowercase letters, numbers, and symbols, the malicious actors rely on human instinct to narrow down the possibilities. For instance, most users when faced with choosing a password that fits these requirements, will pick a word, put the

uppercase letter first, and end the password with the number and symbol. Alternatively, many people will replace common letters with a number or symbol that represents that letter. This changes a common password, such as “password,” into the only slightly more complex password of “p@ssw0rd,” which is still an easy to guess pattern.

Recommendations

Consider using a password manager, which is an application that can run on a computer, smartphone, or in the cloud, that securely tracks and stores passwords. Most password managers can also generate *strong*, random passwords for each account. As long as the password to access the password manager is strong and unique, and two-factor authentication is being utilized, this technique can be affective. However, if the company running the cloud-based password manager is compromised, or a vulnerability in their software is discovered and leveraged by an attacker (which does happen!) it is possible that all of your passwords could be compromised. If you choose a password manager that is local to your computer or smartphone, your passwords may be compromised if malware gets on your computer or you lose your smartphone. When choosing a password manager, ensure it is from a known, trustworthy company with a good reputation.

Another technique to assist in building *strong*, *unique* passwords, is to choose a repeatable pattern for your password, such as choosing a sentence that incorporates something *unique* about the website or account, and then using the first letter of each word as your password. For example the sentence: "This is my January password for the Center for Internet Security website." would become "TimJp4tCfISw." This password capitalizes 5 letters within the sentence, swaps the word "for" to the number "4," and adds the period to include a symbol. The vulnerability in this technique is that if multiple passwords from the same user are exposed it may reveal the pattern. Variations on this technique include using the first letters from a line in a favorite song or a poem.

Further Information

More information on the role of strong passwords in enterprise defense is available in the CIS Critical Security Controls: https://www.cisecurity.org/critical-controls.cfm

Further advice on passwords is available in the MS-ISAC Security Primer available at: http://msisac.cisecurity.org/whitepaper/documents/Security Primer - Securing Login Credentials.pdf

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™