August 2015
Volume 10, Issue 8

The Harm in Password Reuse

ENTERPRISE INFORMATION SECURITY PROGRAM
Keeping our organization's data safe.

Enterprise Information Security Program

Tacoma

From the Desk of Ron Jimerson, Chief Information Security Officer

Every day malicious cyber actors compromise websites and post lists of usernames, email addresses, and passwords online. While this can be embarrassing, such as when thousands of government employees email addresses and passwords were exposed during the recent Ashley Madison breach, it also leaves users open to follow-on potential attacks due to password reuse.

Password reuse is when someone reuses the same password on multiple websites or accounts. This is a vulnerability when the password is exposed in coordination with other information that identifies who is using the password, such as first and last names, login names, or email addresses.

How Password Reuse is a Threat

Password reuse is a threat because malicious actors can take advantage of a reused password if there is other associated information that identifies you. This typically occurs through one of two potential scenarios:

NEVER use your work email address when signing up for and accessing personal web sites.

In the first, and most common scenario, the malicious actors can search for other accounts you use and try to login with the same password. In some cases the actors might try to find personal accounts such as Facebook, Twitter, or banking websites. If they can identify those accounts, and you reuse your password, they can login as you. In other instances the malicious actors may try to determine where you are employed and attempt to use for remote access, such as through a remote email or timecard access.

A second scenario involving a malicious website is much less common, but still poses a threat. In this scenario the malicious cyber actor sets up a website that spoofs a legitimate web site, that requests you enter an email address, password, and potentially other information to gain access. Once you have done that, they know who you are and can search for your other accounts where you used the same password.

Avoiding Password Reuse

Avoiding password reuse can be challenging because of the number of websites and accounts that require passwords, some of which require updating your password every 30 days There are two ways to both avoid password reuse and to ensure any password meets the recommended password complexity requirements.

The first technique is to use a password manager to remember each unique password.

Password managers are applications that can be stored on a computer, smartphone, or in the cloud, and will securely track passwords and where they are used. Most password managers can also generate complex random passwords for each account if you choose to do so. As long as the password to access the password manager is sufficiently complex, this technique can be affective. However, if the company running the password manager is compromised (which does happen!) it is possible that all your passwords will also be compromised. If you choose a password manager that is local to your computer or smartphone, that information 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.

The second technique 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 August password for the Center for Internet Security website." would become "TimAp4tCfISw." Since a strong password is complex, and includes upper and lower case letters, numbers, and a symbol, this password keeps the capitalization within the sentence, translates the word "for" to the number "4," and adds the period to include to add a symbol. The vulnerability in this technique is that if multiple passwords from the same user are exposed it may reveal the pattern.

Regardless of how a unique password is chosen, it is critically important that every password is unique. Some companies, such as Facebook, have begun programs to identify password reuse. Facebook's program to identify password reuse involves monitoring for lists of compromised usernames, emails, and passwords, and attempting to match those to the usernames or email addresses of existing Facebook users. If a match is found Facebook asks the user to reset their Facebook password.

Further advice on choosing a strong, complex password is available in the MS-ISAC Security Primer available at: http://msisac.cisecurity.org/documents/SecuringLoginCredentials.cfm

---

Provided By:

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

STOP | THINK CONNECT™