
# Security Awareness / Trends August '17

PASSWORD REUSE

## Password Reuse

### User Account Attacks

In Microsoft's latest Security Intelligence Report (SIR), researchers detected a 300% increase in user accounts attacked over the past year, and a 44% growth in the number of account sign-ins attempted from malicious locations. Looking closer at the data researchers found this increase could be due to large data breaches that had occurred (Adobe, LinkedIn, IRS, etc.) and password reuse. Password reuse is when users use the same password across multiple accounts, which leaves them vulnerable to an attack known as credential stuffing. What happens with credential stuffing is that hackers utilize stolen account and password information from one web site or system, and use it in an attempt to gain access to another that the user has an account on. The reason this technique works so well is a majority of users reuse the same credentials on multiple accounts. What is worse is the availability of tools that allow hackers to automate this attack in a bulk fashion.

What is the best defense? Of course using unique passwords across various sites is the most effective defense. The difficulty of this is the adoption of single sign-on and identity federation. It is still a best practice to keep personal and business usernames and passwords unique. Do not use the same password for your College, social media, online banking or credit card sites.

How can I tell if my credentials have already been exposed as part of a data breach? Given that 1 in 4 Americans have been impacted by a data breach, the odds are pretty good. However, not all data breaches affect passwords. There are some good online resources to do your own checking. These sites use your email address to check their database to see if the email address has been part of a data breach and when. The two major sites for this are "BreachAlram.com" and "HaveIBeenPwned.com". Here you simply enter your email address and a list of breaches and dates will be displayed associated with it. After reviewing the data that was compromised along with the date you can take appropriate action, such as changing passwords. Some services even provide proactive monitoring of accounts at no charge.

What is the College doing to protect against these sorts of attacks? For privileged identities and access the College is looking to implement multifactor authentication (MFA). Multifactor authentication will require certain services to ask for an additional authentication mechanism such as something you have like a cell phone text message or biometric factor like fingerprint or facial recognition. You may hear more about this as the College continues evaluating this technology.

### Password Management

To help maintain good password hygiene and keep unique passwords for various sites and services, you might want to use something other than a post-it note or whiteboard. Password management software is one way to do this. A password manager stores your login information for all the websites you use and helps you log into them automatically. They encrypt your password database with a master passphrase. The password management tool can also identify the password strength and when it was last rotated. Several free software packages can help you manage your accounts and passwords. Here are three free options that you can evaluate:

LastPass: https://lastpass.com

Norton Identity Safe: https://identitysafe.norton.com/

Password Safe: https://pwsafe.org/

Microsoft Global Security Intelligence Report, https://www.microsoft.com/en-us/security/Intelligence-report (accessed Aug. 2017)