CampusGuard News

5/1/2020

Educating Remote Employees: Passwords

As employees adjust to their remote working environments and cybercriminals increasingly look to exploit this drastic change, providing continued awareness training and guidance on information security best practices is critical.

As you know one of the most important defenses when protecting systems against unauthorized access is strong passwords. In fact according to the 2019 Verizon Data Breach Investigations Report (DBIR), 80% of hacking-related breaches involve compromised and weak credentials. Even with multi-factor authentication deployed on systems housing sensitive information, typically the first factor is a password so it is critical for employees to understand how to create strong passwords.

Now is a good time to remind your staff of your organization's password policy. You may also want to share the recommended best practices below:

Password Creation:
The biggest problem with most passwords is that, in our attempts to make them easy to remember, we are relying on words that can either be guessed or easily broken through brute-force attacks. Weak passwords include the names of family members or pets, anniversary or birth dates, names of systems or software, or words describing visible items in your work area. Much of this information can be researched on your social media accounts. In an attempt to ensure users are implementing strong passwords, many organizations have policies dictating that passwords meet a particular set of requirements. For example, systems might have requirements to use a minimum of 8 characters, contain at least one upper case and one lower case letter, one number, and at least one special character. Even with these somewhat restrictive requirements, users will typically choose a password that is easy to type and easy to remember. Make your passwords unique for that environment and avoid using personal information.

Password Length:
Longer passwords are cryptographically harder to break than shorter ones. However, if your system supports longer passwords, consider using a passphrase. Believe it or not, a passphrase of at least four words, each at least two characters long, written in lower case is actually harder to crack than an eight-character one as described above. For example, the passphrase "winnie the pooh loves honey" is significantly more secure than 8H6y$7kq while also being a lot easier to remember.

Change Passwords Regularly:

Your organization most likely has periodic requirements for updating passwords, but are you also updating your passwords frequently for personal accounts? When is the last time you changed your password to your Gmail account? By changing passwords often, hackers have less time to try to break the password and you also narrow the window of time in which someone might have access to your account. Change your password regularly and when you believe it may have been compromised.

Never Share Passwords:
Never share credentials with a colleague, even if you both have the same job responsibilities. Your ID and password must be unique to you.

Don't Reuse a Password:
Never use the same password for multiple systems, applications, or websites as the loss of it in one place can allow access to the others more easily. Be honest…is your Facebook account password the same as the one you use for your organizational email?

Strengthen your Challenge Questions:
Make sure your responses to challenge questions (used to reset your password) are unique and difficult to guess. Just because the question asks what city you grew up in, does not mean you have to have your answer be truthful. Come up with a consistent response that only you can remember.

Change Default Passwords:
Default passwords for common systems and devices like wireless routers can be found on the Internet, making it very easy for hackers to gain access. Always change default system passwords and do not allow your passwords to be automatically saved and stored by your browser or PC.

Password Managers:
Given the availability of information via social media and the sheer volume of passwords that you now must maintain, consider using a password management tool. These tools allow for enhanced variation of password generation and you only need to remember the single password to access the tool; you no longer need to remember every password you use.

The password manager encrypts the stored information and protects it with a master password that only you know. When you need a password, you simply type your master password into your password manager to unlock your stored vault of passwords.

If you are not currently using a password management tool, you may want to reach out to your IT department or Help Desk to see if there is an approved solution for your organization.

The best passwords are those that are easy to remember but hard to guess. In addition to establishing a password policy, consider performing periodic password audits to help your organization test for and uncover weak passwords. Using the list of accounts with weak passwords, so you partner with your

staff to educate users on the creation of strong passwords and thereby correct the behavior before attackers have the opportunity to exploit that potential weakness. A robust password audit will help you identify possible issues with your password policy as well.

Some additional guidance from the Offensive Security Services team:

> **[Sullivan]:** *When we are performing password audits, we often find that passwords using current events, the current month, or the current season are the most widely used among organizational accounts. A good password ideally would combine a few random words that are easy to remember but hard to guess when put together. The password '1BatteryEatingCyclops?' is over 15 characters in length, hits all 4 types of complexity rules, is easy to remember, and would be near impossible to guess or crack. Where on the other hand, 'Spring2020!' Is going to be guessed in about 5 minutes.*