2022 SedonaASP User Security Audit

02/08/2024 5:28 pm EST

We are auditing the Hosted users [not dedicated] for accounts that do not meet security standards.

- Test accounts will be disabled
- Users with pw set to never expire will now need to change every 90 days
    - Exceptions are only able to be reviewed by SecurityOperations [SecOps] if the company is using Duo Multi Facto Authentication [MFA/2FA].
- Users that have not logged in beyond 6 months will be notified in list to company admin

Below is a sample email that will be sent to company admins with any users that are found in the audit.

Good Day,

We are reaching out to you because during a recent audit, our Security Operations team found that you have one or more users that have a password that do not meet our Hosted Security Policy. Below are our current password security policy mandates.

- Passwords should be rotated at a length not to exceed 90 days
- Minimum 10 Characters
- Must have at least 1 special and at least 1 numeric character
- Must have both upper and lower case characters
- Must not contain more than 5 consecutive characters of your username/company/dictionary word

**All complexity rules can be bypassed if your password length is 20 characters or more

These measures are designed to protect your Data and your users [see info below] We are supplying with a list of current users that have access to the system. Any users highlighted in yellow will be required to enroll on the Password Portal and change their password by 10/15/22. Feel free to return the list with any users that should be removed. We have enhanced the password portal recently to accommodate both security questions *and* emailed reset links to users that are enrolled with a valid email address for your convenience. Let us know if you have any questions.

Additional Info on Password Security

The benefits of changing your password often cannot be underestimated. Your computer stores and provides access to a lot of sensitive information. Even more so when connected to a network that houses the information of your clients. Keeping all of this data safe and secure must be a priority. It is wise for organizations to have a password policy that requires employees to change their passwords regularly. Passwords should also be unique for each account. Most Security/Data Loss Prevention Firms recommend changing passwords every 90 days (about 3 months).

According to recent studies, 80% of all cyber security attacks involve a weak or stolen password. Changing your password quarterly reduces your risk of exposure and avoids a number of IT Security dangers. Unfortunately, passwords are often neglected. We have enough to worry about without thinking of changing our eleventy-million passwords, right? However, the problem is hacking and security breaches are constantly on the rise.

Protecting your data starts with securing passwords. Passwords are your first line of defense against cyber-attack. So, let's look at why you should change your password often, when you should change it, and some best practices for choosing a password.

Why Should You Change Your Password Often?

LIMITS BREACHES TO MULTIPLE ACCOUNTS

If you use the same password for all your accounts, if one gets hacked, you should assume the others will be as well. Each account should have a unique password. For example, you should not use your Facebook password as your work password or your Target password for your mobile banking password.

PREVENTS CONSTANT ACCESS

A hacker may attempt to access your account more than once over a period of time. Changing your password often reduces the risk that they will have frequent access.

PREVENTS USE OF SAVED PASSWORDS

If you lose or change computers, it is possible for someone else to gain access to your passwords. Regularly updating your passwords means that even if someone finds an old or saved password, it will no longer be useful, and your data will be secure.

LIMITS ACCESS GAINED BY KEYSTROKE LOGGERS

A keystroke logger is surveillance technology use to record keystrokes. It is often used to steal credit card information as well as login credentials. Regularly changing your password makes it less likely that passwords obtained this way will be useful for any length of time.

When Should You Change Your Password?

1. After a security breach. If you have been subject to attack or have been made aware of a breach like the Capitol One of Target breach, you need to change your password. When a company tells you that they have experienced a data breach, it is safer to assume that your password is no longer secure.

2. If You Suspect Unauthorized Access. Do not wait until there is glaring evidence that you have been hacked. By that time, it is usually too late. If you suspect someone has attempted access or if you receive an email that an unauthorized user has logged into one of your accounts on a new device, change your password as soon as possible.

3. If You Discover Malware or Other Phishing Software. A virus can put your computer and your entire network at risk. If you discover such software after a scan, change your passwords immediately, preferably from a different device than the one upon which the virus was discovered.

4. Shared Access. Lots of people share accounts like Netflix, Hulu, Amazon. If you share your login information with someone that you are no longer in contact with, change your passwords as often as possible. This is especially true if you have a change in family status, such as a divorce.

5. Logging in at Public Places. If you visit the library or use a public network, change your password afterwards. This will help you keep track of your digital footprint more securely.

6. If You Haven't Logged in for A While. You should always change passwords on accounts that have not been used in over a year. The more often you change your seldom-used passwords the better you will be. Especially if you are not using Multi Factor Authentication.

Password Creation Best Practices

1. Multi Factor Authentication is your friend. This means that to access any account, anyone trying to access it will face a second hoop to jump through. This usually looks like receiving a prompt on your phone and then acknowledging that notification to login.

2. Audit Your Passwords. Do you use the same password in multiple places? Time to stop that. Do you include things like your name in them? Series of numbers in a sequence? Time to stop that, too.

3. Choose passwords that are long and varied. Passwords should have at least 10 characters that utilize uppercase and lowercase letters, as well as numbers and special symbols. Does this seem hard to do? Try to spell a word that is important to you but with numbers and characters replacing letters so that you can remember it. For example, L0v3!5ummer$ Would be an easy way to say you Love Summer or try unique ways of spelling a pet, friend, or family member's name.

Managing your passwords can seem daunting, but it truly is your first line of defense against security breaches. Remember the adage. Passwords are like underwear, change them often. Do not share them or leave them on your desk, and they feel the best when no on else has the same pair.

Additional Resources

https://www.mcafee.com/blogs/tips-tricks/how-often-should-you-change-your-passwords/

- BoldGroup Support