ResponsiveEd®

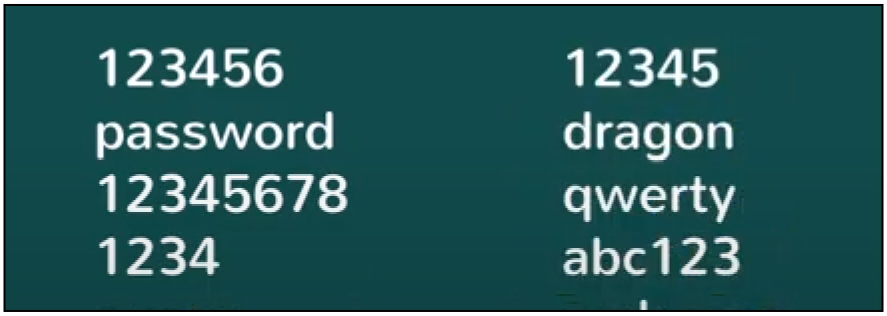
Password Security Awareness

Last Updated: 2024.01.19

Disclaimer: This document may be printed, downloaded, or shared. However, a printed or saved job aid may not be accurate as updates are made to online documents. Please be aware of the date this document was last updated (noted above).

Like keys to your home but online, you should do everything you can to prevent people from gaining access to your password. You can also further secure your accounts by using additional authentication methods.

Dictionary programs are one of the many tools frequently used to crack passwords. A hacker will launch a dictionary attack bypassing every word through a dictionary which can contain foreign languages in addition to the entire English language, to a login program hoping that a word will eventually match the correct password. Some passwords can be cracked instantly by a computer software. Here is a list of the worst passwords. They will be cracked instantly.



123456
password
12345678
1234

12345
dragon
qwerty
abc123

Passwords become more secure as you add more layers of security to them. For example, if you use a password like “Man Carter” it will take about four minutes to be cracked.

If we had an extra layer of security to our password such as numbers or special characters, we get passwords that take much longer to crack.

Secure tips

Tip 1: Don't use the same password repeatedly.

Passwords should be changed on a regular basis at least twice a year *(RES I.S Password Policy)*. Primary reason is that if someone cracked your password without you being aware of it, it makes them have to start all over again. A strong password is one that's never reused.

Tip 2: Categorize your passwords.

Categorize your password in order to minimize the number of passwords you have to remember but also to provide a barrier between systems or sensitive information and those with non-sensitive information. For example you can use the same password for Gmail and Hotmail but you should not use the same password for your online banking program. Passwords you have for your hotmail or other internet email services should be different from the passwords you use on any work-related systems.

Tip 3: Change Password Often

It is important not to reuse passwords and to change your passwords on a regular basis

Tip 4: Avoid using words found in dictionaries.

Instead of people guessing passwords, now computers are guessing passwords. For this reason, if your password is made up of words found in a dictionary it is very easy for a computer to guess it and gain access to your account.

Tip 5: Make Passwords Long

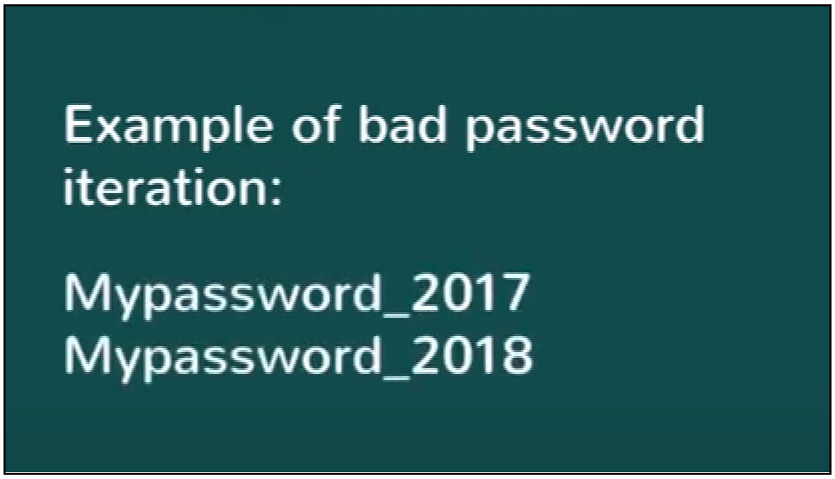
(RES IS Password Policy states: Have a minimum of at least 10 characters.)

Tip 6: Make passwords complex

Moreover, Use uppercase, lowercase, special characters and numbers in your password.

Tip 7: Don’t reuse passwords

Try not to reuse one of your last five passwords in any form of iteration.



Example of bad password iteration:

Mypassword_2017
Mypassword_2018

Tip 8: Make password Non- personal

Avoid using things like your name, birthday, current year, current season, address, phone number, pet’s name or other information may be on the social networking profiles public records or otherwise easily found or guest.

Tip 9: Watch where you store your passwords

If you absolutely need to write down a password, never store it in obvious places such as address books, rolodex files, and drawers or keyboards or behind pictures. At worst but all too common location is a post-it note near the computer. Better locations are a safety deposit box or a locked file cabinet. Software is available for popular handheld computers that can store passwords for numerous accounts in encrypted form. An example is **Last pass.**

Tip 10: Be cautious when using public PC's

Public computers may not always be securely configured and can pose a threat to your privacy by storing the password or web cookies. Think twice about going to a secure site if you cannot verify the security of the computer.

Tip 11: Be cautious when asked for passwords.

Don't forget that getting passwords by manipulation of users is an example of social engineering. An attacker might telephone a user and say "Hi! This is IT here, we're doing a security test can we have your password so we can proceed. Know that any reputable company you do business with will never ask you for your password and rarely if ever need to know your password in order to perform the work, keep your data safe and be cautious.