Password Best Practices

Best Practice suggests that employees should not use their organization's logon password for anything other than logging on to their organziatonal account, i.e. do not use it for other email accounts, social media or accounts such as LinkedIn, shopping, banking, etc.

Why?

Imagine if one of your accounts was breached and your password exposed? By using a different password for each account, you eliminate the risk of compromising confidential information within secure accounts. Here are some ways unsecured passwords could be exposed:

- Passwords may be sent over the internet in clear text (i.e. not encrypted) when logging into a public site or commercial service.
- There are frequent breaches of retail and online services. If the database containing your password becomes exposed, all accounts using the same password become vulnerable to attack as well.

How do I create a strong password?

Employees are asked to create and manage lengthy and complex passwords. Short length passwords (even complex passwords of 8 characters in length) are relatively easy to break as the attack technology for password guessing has dramatically improved . Large complex passwords may seem daunting, but they can be quite easy to create, and more importantly, easily remembered without the need to write them down.
These steps will help you create a secure and easy to remember passphrase:

1. Think about a phrase that you can easily remember (titles, famous quote or something that means something to you). For example:
   - **M**y **o**ne **p**et '**S**am' **i**s **s**o **f**at **h**e **e**quals **t**hree.
2. Take the first letter from each word, this is easy to do while you say it to yourself:
   - **Mopsisfhet**
3. Substitute capitals, numbers and symbols for some of the words:
   - **m1pSi%Fh=3** (capitalize the important words like Sam and Fat, substitute % for small s)

From a simple sentence, you now have a 10 digit password that cannot be recognized by any dictionary attack, add some symbols and numbers and it could take nearly 1,000 years for a criminal to crack (see chart).

Other tips are:

- **Longer is stronger.** For each additional word you add in a string of words, you increase difficulty exponentially. A long, unrelated string of words with substitutions is the most difficult to guess.
- **Don't use personal information.** Personal facts may be discovered from one of your online profiles.
- **Change them regularly.** You may not know if one of your passwords are breached.
- **Increase complexity.** Always substitute or insert symbols, numbers and/or capitals into your text.

- **Consider using two-factor authentication.** A secondary authentication (a biometric, code sent to your phone, smart card or token) makes it nearly impossible to breach your credentials.

Some Interesting Facts:

How much time is needed to crack a password by brute-force?

It has become far more complicated to estimate the length of time to crack a password than a few years ago. There is now an algorithm based upon the size of the space (***T***), the length of valid characters (***A***), the number of characters (***N***), the number of hours to try every combination of characters (***D***), the number of years that will have to pass before the space can be checked in less than one hour (***X***) based on Moore's law of computer capacity doubling every two years and the fact that a computer can process more than a billion possibilities per second, the formula is:

$T = A^N$
$D = T/(10^9 \times 3{,}600)$
$X = 2 \log_2[T/(10^9 \times 3{,}600)]$

If this boggles your mind, here is a chart from the National Institute of Technology in Warangal to give you some idea:

Number of Characters	Numbers only	Upper or Lower case letters	Upper or Lower case letters mixed	Numbers, Upper & Lower case letters	Numbers, Upper & Lower case letters, Symbols
3	instantly	Instantly	Instantly	instantly	instantly
4	Instantly	Instantly	Instantly	Instantly	instantly
5	instantly	instantly	instantly	3 secs	10 secs
6	instantly	instantly	8 secs	3 mins	13 mins
7	instantly	instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1 qt years

Some Other Resources:

Passwords Best Practices Video: https://www.gov.bc.ca/informationsecurityawareness
Wikipedia on password cracking: http://en.wikipedia.org/wiki/Password_cracking
Canadian Centre for Cybersecurity: https://www.cyber.gc.ca/en/publications (search passwords)