Tips for a Strong Password

Your password is like the lock on the front door of your house. You never want to use a lock that can easily be broken. If someone knows your password, that person has the ability to see your messages and respond to messages pretending to be you.

Below are some tips to aid creating strong passwords.

1. Passwords should be as **long** as possible, with 8 being the minimum number of characters needed. Using a password with 14 or more characters is more secure.
2. Avoid using easy to guess passwords like your name, birth date or your pet's name as your password.
3. Use a combination of upper case and lower case characters, numbers and special characters [like !@!#$%^&*()-+], randomizing the sequence as much as possible. "**password99**" is a terrible password, but "**P@s$W0rd!99**" is much better.
4. Avoid any words that can be found in a dictionary, even if numbers and symbols are added. If your password can be found in a dictionary, it would take less than a second to crack it.
5. Avoid using passwords that use sequential keyboard characters like "qwerty".
6. Do not use the same password for different services. For example, do not make your work email password the same as your personal account password. In case an account is compromised, the damage will be isolated to one account.
7. Change your passwords on a regular basis. Even if you have a strong password, it is only a matter of time before a determined person can crack it. Changing your passwords on regular basis mitigates that risk.
8. NEVER give your password to anyone via email or phone. Immediately delete any email messages that ask you to provide your login credentials, no matter how legitimate the requests seem. Use a password manager app on your smart phone to keep track of your passwords. These apps let you create, store and manage all your passwords and logins. One such app is 1Password by AgileBits https://agilebits.com/onepassword [Use at your own risk]

Emails

Email has evolved into an essential tool of our daily routines. However, most people do not know how to protect themselves from most spam and phishing attacks.

Most spam and phishing attacks prey on your trust and usually try to emulate a friend, coworker, employer, or recently used vendor. In order to protect yourself from these scams, you have to be a little paranoid with your incoming email.

- Do you recognize who the message is from, both name and email address?
- Are there strange attachments (i.e. files ending in ZIP/zip, EXE/exe, JS, VBS)?
- Does the recipient list include lots of other address that you've never seen?
- Did the message come from someone at a really weird time when you know they shouldn't be sending email?
- Does the subject line match the message?
- Is there a hyperlink and when you hover the mouse pointer over it (without any clicks!), does it appear to go to someplace totally different?
- Is the content offering something too good to be true or threatening?
- Does the content look like a child from another country wrote it, including poor spelling and grammar?
- Does the message ask for personal information, like SSN's or banking related?
- Does message ask you to SCAN your machine for viruses or tells you that you have some that needs to be cleaned?

There is a helpful PDF located at:

https://s3.amazonaws.com/knowbe4.cdn/SocialEngineeringRedFlags.pdf

to remind you of these harmful characteristics to be wary of in emails. As a general rule, if the email looks suspicious, it probably is!

So, with that in mind, what can you do to help your inbox?

- Personalized block lists
- Email filter rules
- Avoid clicking unsubscribe links in emails
    - ***These links generally take you off of one list and add you to multiple others.***
- Avoid clicking ANY attachments that you don't recognize the sender