Password Management

Most of us use passwords every day, to log onto the systems we use at work, access e-mail, bank or shop online, or access smartphones. However, passwords are also one of your weakest points; if someone learns your password, they can steal your identity, access ePHI or intellectual property at work, transfer your money or access your personal information. Using a stronger password makes it less likely that an individual will be able to guess your password and gain unauthorized access to your accounts.

What Works – You need to create a password that is difficult to guess but easy to remember. It should be at least ten characters long, and contain a mix of upper and lower case letters, numbers, and special characters. Consider the following when creating a password:

- Use a pass phrase. A pass phrase is a complex password based on a memorable song, line of poetry, line from a movie, or any other phrases that have personal meaning to you that you can easily recall. Pass phrases make it easier for you to remember the password. Here are some examples:
  - 4s&7yAT!!! – Four score and seven years ago today.
  - Ga&mmd…. – Go ahead and make my day.
  - J&Jwuth??? – Jack and Jill went up the hill.
  - 2Bon2b!!!! – To be or not to be.
  - Mmilirn!!! – My mother in law is really nice.

- Use the license plate rule. Pick a very short phrase or one or two words and try to squeeze them into at least ten characters, similar to a vanity license plate. Some examples include:
  - 00Gravty!! – Zero gravity.
  - 10Sne1!!!! – Tennis anyone.
  - Bkeepr11.. – Bee keeper.

What Doesn’t Work -

- Using a word, whether spelled backwards or forwards, or a word preceded or followed by a number.
- Using personal information such as family names, pet names, birthdays, or anything else that could be associated with you.
- Using slang words.
- Using common keyboard sequences such as QWERTY, or abc123.

Use Passwords Securely – Using a strong pass phrase won’t help if it can be easily copied.

- Don’t use the same pass phrase for personal ‘private’ accounts, e.g. work, financial, and personal ‘public’ accounts, e.g. Facebook, Twitter.
- Don’t share your passwords.
- Don’t use a public computer, e.g. hotel, library, to log on to a work or bank account.
- If available, use two-factor authentication. Using two factor authentication:
  - You would enter your pass phrase, which is something you know.
  - You would then enter a passcode, which is something you have. The passcode would typically be sent to your smartphone after you enter your pass phrase.
- Finally, if you are no longer using an account, be sure to close it.

Remember, security won’t work without you. YOU are the key to security at PSOM.

Please refer all information security comments or concerns to David Wargo at:
Tel: 215.898.9678 | E-mail: David.Wargo@uphs.upenn.edu