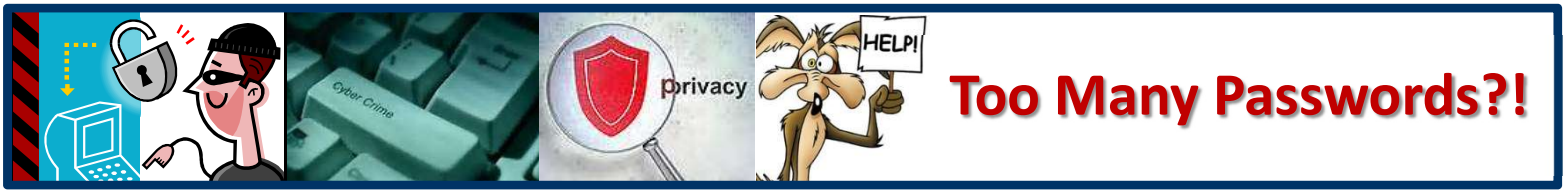

Too Many Passwords?!

Phishing: Reduce your risk!

Cyber criminals are EXPERTS at connecting the dots. They can easily guess where you might have online accounts elsewhere through e-mail contents, social media and publicly available information.

One of the best things you can do to protect yourself is not use the same password at multiple sites: if you are unknowingly tricked into providing a credential, your risk is limited to that site, not everywhere else you have used it. In practice, however, that is easier said than done without writing them down.

Consider this suggestion to manage multiple passwords and safely write them down in "hint form":

1. Think of a word, phrase or character sequence that nobody would easily discover such as the street name of your childhood home, elementary school, first car, etc.
    a. *Don't use information easily discovered through social media or public records such as current address, nicknames, high school, maiden name, pet's name, etc.*
    b. *Consider information from when you were a minor…most is not public record.*
2. For this example, we will use "gremlin". Create a strong password by adding special characters, such as a '#' to the front and '*1' to the end: #gremlin*1.
3. A password hint of **#car*1** can be written down anywhere because it is meaningless to others and only YOU know what "car" means. Your e-mail contacts can be a convenient place to store all of the hints, but use a unique password structure (different from your base word and character sequence above) for your e-mail account where your contacts are stored in case it is compromised.
4. For each online account, use a different variant. For example: *gremlin%4 (hint would be *car%4).
5. Obviously, never write the full password or base word down anywhere, only the hint.
6. Better: Use a combination of upper and lower case to further strengthen the password (!BlueGremlin%4) and change the base word on all accounts annually (immediately if you think you got fooled by a phish).

Remember! Cyber Criminals are not interested in simply embarrassing you. They are looking for ways to steal your money or sell private information they have obtained…it is a billion dollar industry of epic proportion. They are successful because it is much easier to exploit human behavior and trust than it is to circumvent most IT security systems! Once they have a valid credential, they can access that account freely without being noticed because computer security systems only know what kind of access a set of credentials should have…not who is really behind the keyboard typing them in. Be suspicious and be vigilant to be safe on-line! -M. Zimmerman, CIO