Choosing a smart password

As part of Cyber Security Awareness, UGCERT would like to take this opportunity to remind you about smart password practices. This is to ensure that you're protecting your computer, website, and personal information.

Creating a new password is often one of the first recommendations you hear when trouble occurs. Even a great password can't keep you from being scammed, but setting one that's memorable for you and that's hard for others to guess is a smart security practice since weak passwords can be easily guessed. Below are a few common problems we've seen in the past and suggestions for making your passwords stronger.

Problem 1: Re-using passwords across websites
With a constantly growing list of services that require a password (email, online banking, social networking, and shopping websites — just to name a few), it's no wonder that many people simply use the same password across a variety of accounts. This is risky: if someone figures out your password for one service, that person could potentially gain access to your private email, address information, and even your money.

Solution 1: Use unique passwords
it's a good idea to use unique passwords for your accounts, especially important accounts like email and online banking. When you create a password for a site, you might think of a phrase you associate with the site and use an abbreviation or variation of that phrase as your password — just don't use the actual words of the site. If it's a long phrase, you can take the first letter of each word. To make this word or phrase more secure, try making some letters uppercase, and swap out some letters with numbers or symbols. As an example, the phrase for your banking website could be "How much money do I have?" and the password could be "#m$d1H4ve?" (Note: since we're using them here, please don't adopt any of the example passwords in this post for yourself.)

Problem 2: Using common passwords or words found in the dictionary
Common passwords include simple words or phrases like "password" or "letmein," keyboard patterns such as "qwerty" or "qazwsx," or sequential patterns such as "abcd1234." Using a simple password or any word you can find in the dictionary makes it easier for a would-be hijacker to gain access to your personal information.

Solution 2: Use a password with a mix of letters, numbers, and symbols
There are only 26^8 possible permutations for an 8-character password that uses just lowercase letters, while there are 94^8 possible permutations for an 8-character password that uses a combination of mixed-case letters, numbers, and symbols. That's over 6 quadrillion more possible variations for a mixed password, which makes it that much harder for anyone to guess or crack.

Problem 3: Using passwords based on personal data
we all share information about ourselves with our friends and co-workers. The names of your spouse, children, or pets aren't usually all that secret, so it doesn't make sense to use them as your passwords. You should also stay away from birth dates, phone numbers, or addresses.

Solution 3: Create a password that's hard for others to guess
Choose a combination of letters, numbers, or symbols to create a unique password that's unrelated to your personal information. Or, select a random word or phrase, and insert letters and numbers into the beginning, middle, and end to make it extra difficult to guess (such as "sPo0kyh@ll0w3En").

Problem 4: Writing down your password and storing it in an unsecured place
Some of us have enough online accounts that we may need to write our passwords down somewhere, at least until we've learned them well.

Solution 4: Keep your password reminders in a secret place that isn't easily visible
Don't leave notes with your passwords to various sites on your computer or desk. People who walk by can easily steal this information and use it to compromise your account. Also, if you decide to save your passwords in a file on your computer, create a unique name for the file so people don't know what's inside. Avoid naming the file "my passwords" or something else obvious.

Problem 5: Recalling your password
when choosing smart passwords like these, it can often be more difficult to remember your password when you try to sign in to a site you haven't visited in a while. To get around this problem, many websites will offer you the option to either send a password-reset link to your email address or answer a security question.

Solution 5: Make sure your password recovery options are up-to-date and secure
You should always make sure you have an up-to-date email address on file for each account you have, so that if you need to send a password reset email it goes to the right place.

Cyber security
Starts with
YOU!

Do Your
Part....Educate
Yourself, Educate
Others
&

Be Safe Than
Sorry!