FIRSTSTEPS
ONLINE

Security Module: Protect Your Passwords and Your Privacy!

In this module let’s take a look at one of the best ways to protect your private information and identity – **Passwords!**

One of the easiest ways to create a barrier between a successful information hacker and a failed hacker is to create passwords that discourage them from their hard-core, brute-force attacks to steal your goodies.

Good passwords can be two-edged swords, and it’s impossible to have only one password, or perfect passwords for each situation. You want passwords that are crack-proof, simple to remember, and if you forget them, simple to find. Many folks end up with dozens of passwords scattered over the internet and have a hard time recalling which password goes with where. If your browser has a password manager, your life gets easier, but you don’t want to lose the manager when you’re away from your computer and urgently need you connect to a particular site.

In the first point of his article, **“5 Steps to a Good Password,”** Paul Gil lists the qualities your password should have:

“The objective is to create a password with three qualities:

1. Is neither a proper noun nor a word in the dictionary.
2. Is complex enough that it resists repetition attacks.
3. Is intuitive enough that you can still remember it.”

Finding the balance between these three can be frustrating yet quite rewarding when you have succeeded. That feeling you've done your best to secure your valuable identity and information is worth the peace of mind and worry-free sleep!

A good password should be unique *to you*, have meaning *to you*, but not divulge any clues about something that everyone knows about you. If you had a nickname "Bubba" growing up, don't use it. (If you had a secret name for a high school sweetheart, who disappeared into the universe twenty year ago… maybe.)

Some marketers use special phrases that they shorten or alter in a meaningful way or by adding numbers or symbols (#@$%&?!) as an integral part of the password. You can also scramble different characters – uppercase with lowercase or special characters with numbers – in an odd order only known to you.

Once you've determined your passwords, keeping track of them is critical. Writing them down, though insecure, is a great way to manage your passwords. Where you keep them *after writing them* down is even more crucial! To hide them from prying eyes and unwanted visitors, keep your passwords on a small card in your wallet or purse with your other valuables, credit cards, identification, and money.

Write your passwords on the edges of the pages of your favorite book stored in a bookcase with lots of other books. Ease of remembrance is high since your favorite book is unique to you. (Don't tell your book club members your favorite book. Lie to them! Tell them your favorite book is the original, 1,500-page version of *Les Miserable* by Victor Hugo. They'll leave you alone.)

Tape a copy of your passwords to the bottom of a wastebasket, a hidden shelf, a flower pot, under your toupee, inside the dog house of your Doberman Pinscher, or somewhere not associated with your computer. A home safe or secure filing cabinet is also a viable option for secure storage and retrieval. (Of course, you might lose the key or forget the combination!) Some people store the deed to their home in the refrigerator freezer because it still might be standing if your house burns down. You might be homeless, but you'll still have your passwords.

Seven quick tips to help you choose your passwords

1. Your password should be at least eight letters long. Include upper and lower case letters, numbers and/or special symbols or characters mixed up in the password. And… The longer your password, the harder it is to crack 'n' hack.

2. Make your password memorable by using a non-recognizable word known only to you and have meaning to you. For example, you love Mexican food and when you serve it to guests, you say, "Mi casa, su casa." (My home is your home.) Take the first letters of every word – MCSC – and add some meaningful words, numbers or characters like this: mcsc&tacos4me or McSc14tacos1time.

3. **Never** use your birthdate, anniversary, family members' names, street names, pet names, or other high profile subject or phrase. Stay away from using any personal information for your password.

4. Be careful how many times you use the same password. If a hacker cracks one password, they may have access to numerous secure locations.

5. Instead of using a word with letters and numbers, use a pass-phrase like, "momlikespb&cheese," "bballrulesall," or "cudchewingcow." Add numbers or characters to increase difficulty and confuse the hackers.

6. Change your password from time to time, and make the change significant, the opposite, definitely different from your original password. Some experts strongly recommend changing them every 30-60 days and not to reuse a previous password for at least one year.

7. Make your password more secure by replacing letters with symbols and characters. (This tip comes from another article by Paul Gil: “Examples of Weak and Strong Passwords.”) For example, “ilovemypiano” can be upgraded to “!LoveMyPiano”, or even better, “ILov3MyPianO.” Of if you really want to be obscure, use !@#&$*%0!!^!! so people will run away because they think you’re swearing at them.

Tips on How to Protect your Web Privacy

In the conclusion of this module, I want to share with you eight more vital tips on how to prevent your personal details and identity from being compromised.

It’s impossible to be 100% secure, but with a few guidelines and common sense, you can place yourself in a more secure position. I’ve said this before, but I gotta say it again: the Internet is an exciting place to explore and experience, however ... there’s a cost... and a risk. How you handle this risk and prepare yourself will determine how secure you are in the end (and along the way).

Eight more tips to help you protect your privacy and personal identity.

1. Don’t give out too much information.

Nasty hackers use forms and unnecessary surveys to steal your private information.

2. Clean out your search history often.

Your search history leaves a digital footprint of where you've been and what you've been downloading. Your computer browser records and saves everything you type in your address. Periodic cleaning protects your online privacy and helps your computer run faster and more efficiently.

3. Click the "Log Out" button whenever you finish with a particular site.

Many websites, search engines, or online programs require you to "Log in." Then you might close your browser window and continue other online activities. Not a secure technique. Stop it! This method leaves you vulnerable to hackers and puts your computer security at risk.

4. Pay attention to what you click on and what you are downloading.

Many websites and programs embed a "cookie" which records your online habits, your online searches and history, and reports back to its information gobbling masters. Delete the "cookies" folder and your "Temporary Internet files" from your computer on a regular basis.

5. Common sense are the two operative words of the day.

Stay away from sites on the internet that might cause embarrassment to you, your loved ones, your distant relatives, your coworkers, your neighbors, and the elderly checkout lady at your local convenience store, especially if you happen to be a senator, governor, or president. Adult sites are prone to viruses, hacking, phishing, and worm programs. But if *really like* headaches *and* heartaches, go for it. It's your life.

6. Build a fortress around your personal and private information.

Do not give out information you normally would *not* give out to strangers. That's what entities and people on the web are... strangers. Stranger than most strangers. Beware of sharing personal information on social media, especially details relating to your identity, such as user names, passwords, log on credentials, complete names, email and street addresses and phone numbers. Public access to this information can lead to receiving an enormous amount of spam, unwanted attention, frivolous email, and those stranger than strange strangers showing up at your front door. Or sneaking in the back door of your computer!

7. Watch out when you are on your favorite Social Media Sites.

Review your security settings for any social media site. Weaknesses can lead to exposure of your private and personal information – especially anything of a financial nature.

8. Watch out for online scams.

A myriad of online scammers are constantly inventing new ways to steal your money and your private details. Be aware and be prepared!

Scams! What scams? Don't leave me hanging like this!

(Don't worry. You'll learn about them in the next Security Module. Keep reading...)

Protect your digital valuables-
Your Personal Information and Identity

3E's
2SUCCEED
Educate • Engage • Expand

VIDEO TUTORIAL – Passwords and Privacy

Click HERE to watch

To view and read this module online, go to www.work-with-walt.com

Your purchase of this training tutorial includes free membership to the online version of **First Steps Online** which has more than 20 FREE downloadable resources.

If you have problems with login, please contact walter@firststeps.online