Online Safety

Last year, there were 5.4 Billion internet users, and there were 5.5 Billion malware attacks, according to statisca.com.

What you can do:

- *use secure passwords*
- *be careful what you click on*
- *be careful what you post online*
- *know who you are giving your personal information to*
- *know who you are getting advice from*

Did you know that you can get lists of commonly-used passwords online. You can! So can the people who write viruses and malware!

These days, it's easy to do high quality graphics work to make your emails look nice. So, anyone can fashion an email to look like it's coming from a bank. Your bank will never ask you what your account number is, or what your pin number is, in an email or text message. Your bank already knows them, so they don't need to ask. You can, and you should, call your bank and verify that they sent an email that 'doesn't look quite right'.

Are you going out of town? The Facebook world doesn't need to know that. Post your pictures and experiences <u>after</u> you come home.

Hey, when's your birthday? Well . . . how young are you going to be? Thanks, you just gave me your birthdate. With that, and one or two more facts, I can now pretend that I am you! That's another thing that social media doesn't need to know.

Do you have aches and pains? Ask your doctor about it! If you do Google it anyway, be careful which answers you read. Is it from an organization you recognize and respect? Many doctors will accept and answer emails from patients between visits, and

some insurance companies provide a nurse you can call, anytime. Find out whether these options are available to you.

***Password Safety**:*

If you make up a password of 4 lower case letters, then there 4^{26} (or 4,503,599,627,000,000) different possible combinations. If you also include the upper case letters, then there are 4^{52} (or 2,028,240,960,000,000,000,000,000,000,000). Add numbers into it, and it's now 4^{62} (just trust me, it's a large number). If you add 8 special characters to the mix, then there are 4^{70} possible combinations. If you make your password longer, say 12 characters long, that makes for 12^{70} different combinations (3.4 followed by 74 zeroes).

Is this a problem for a bad actor with a modern computer running modern software? Not necessarily. Sure, a perfectly random, 12 character password might take years for his computer to figure out, far longer than the bad actor is going to wait. Most people don't use passwords like that, they use passwords that are much easier to remember, and also worlds easier to figure out.

So . . . let's see what this bad actor might do. First, he my try his list of 5000 most-often used passwords. That will take him a handful of milliseconds. Then, how about things that are important to the the user, like his anniversary, the names of his children, his zip code, local sports teams, naughty words, and other familiar things that the password might be fashioned after. A few more milliseconds. The bad actor just might've been successful, by then. If you have a shorter password, trying all of the combinations might take just a few seconds or a few minutes.

Computers are getting faster. Perhaps what would take years, today, will be short enough to be worth the wait for a bad actor. Also, some gate-keeper computers have been found to take a different amount of time to evaluate a correct character in a password than the time it takes to evaluate an incorrect

character, and that time difference can be measured. Knowing whether an attempted character is correct or incorrect can reduce the password-cracking effort considerably.

And, of course, there is also the old-fashioned good guess. Someone could still guess the one out of 12^{70} possibilities that will be successful. Not likely, but still possible. It's also possible that your randomly-created password turned out to be a common 12-letter word. Also unlikely, but still possible.

A bit of good news . . . it has become fairly common that the gate-keeper computers will only accept 2, 3, maybe 5 bad password attempts before locking an account out. That's a good thing. Frustrating, perhaps, but its really good security.

Let's say you lost your phone, and a bad actor is using it. Amazon wants you to put in the number that they just texted to you. That bad actor can just read that text message himself, and feed Amazon that number. That might be something to consider, when deciding what kind of business you should do on your phone. Maybe your bank, Amazon, and other online shopping sites are best to not have a place on your phone, particularly if you tend to misplace it. Your phone's lock screen is probably fairly easy to get past (4 digits, maybe 6, and a number combination that has a special meaning to you, like the year you graduated? Fairly easy for even a stranger to find out).

You play a big part in your online security and safety. Watch out for yourself and be online-safe.

Credits:
Statista.com
www.youtube.com/@Computerphile

These articles are available online at youfoundterry.com