

HOW TO GET STRONG! (PASSWORDS)

Lots and lots of people conduct a great deal of business on their computer, and store a great deal of information in the same place. In this column, I'll talk about these wonderful devices, and safeguards we can use to make sure our information is as secure as possible. If you don't own or use a computer, you can probably skip reading this column and go right to the sports page.

We read on an almost weekly basis of breaches of the databases of banks, retailers, government agencies, or celebrity photo storage sites. The term we hear or read of is someone "hacked" into the database. Hacked is a short word that means someone figured out how to bypass a target business or agency's security measures or firewalls. But hackers don't only concern themselves with Home Depot or the Veterans Administration as hacking targets. Individual consumers are targeted every hour of every day by hackers.

These hackers want to gain access to your online information, including your bank accounts, credit cards, email accounts, or anywhere else you store personal information. If you conduct any business online, you already know almost all these types of online accounts require use of a password to access them. This password is your first, and sometimes only, line of defense in safeguarding these accounts. So your password needs to be very strong.

What do I mean by a strong password? Well, let's describe some weak passwords to give you an idea. The Iowa Attorney General, quoting from a security application provider, Splashdata, identified the most common password used in 2013 as "123456". The second most common? "Password". Those are pretty weak, almost comically weak, passwords. Many hackers use password-breaking software, which likely could figure out these passwords in a fraction of a second.

How do you make a strong password? These are the recommendations of the Iowa Attorney General:

- Create passwords unique to each account you access online. That can be a hassle, but consider if you use only one password for all your accounts, how compromised you are if that one password is figured out. It's like giving someone a master key to all the safety deposit boxes in the bank vault.

- Create your passwords with at least eight characters (the longer the more secure). The password should contain upper case letters, lower case letters, numbers, and non-alpha-numeric symbols (those are the symbols above the numbers on your keyboard)
- Don't use names of your children, pets, favorite sports teams, or hobby activities. OK, you might ask, how am I supposed to remember all these passwords if I can't associate them with something familiar to me? Think about this. Your pet cat's name is Tiger. Lots of us might use "Tiger1" as a password. How about this instead? McTh9L@H. That's a shortened version of the phrase "My cat Tiger has 9 lives at home."
- Change your passwords on a regular basis. Many employers require you change your password every 90 days. Government agencies I correspond with require the same. This is probably a good idea for all of us.
- Don't write down your passwords on a sticky note and paste it to your computer monitor. Granted, you'll need to write them down somewhere, but keep those records in a safe place.

OK, so you came up with some dazzlingly complex passwords. Are you safe? That depends on how you react to attempts to pry this information out of you. These attempts are called phishing. It can take the form of a phony email, phony website, or even a phone call. Most commonly, folks get an email which looks like it came from their bank, credit union, or someplace they did business with. The email might ask them to "confirm account information". And to do this, you need to click on a link, which takes you to a website appearing as legitimate, but is not. This website might ask for account information and passwords. A good tip to remember when entering personal information online is to check the web address or URL. If it is a secure website, the address will begin with <https://>. If you don't see the "s", it is not a secure website, and you need to stay away.

Your passwords are important, but you also need to consider the security software installed on our computer. How up to date is it? Does it update automatically? You want to use something which does update on its own.

But you can employ strong passwords, use the latest, greatest security software, and still get in trouble. Because you can fall prey to what is called, “human engineering”. What’s that? Well, keep reading.

A retired Clinton professional contacted me this week. I will call her Amanda. Amanda was always very cautious about doing business online. Recently she received a phone call from a man claiming to work for Microsoft. He said his system detected a problem with her computer, and wanted to remotely access her computer to diagnose the problem. Amanda allowed him access, and he spent half an hour reviewing her files. He said he wanted to sell her a warranty, which she agreed to purchase. She gave him her credit card number. He told her it turned up as invalid. He asked for her bank routing number and bank account number, her email address, and last four digits of her social security number, to process the payment. All this sounded very professional, so Amanda provided the information. The call ended.

Within a quarter of an hour, Amanda received a do-not-reply email from Western Union, asking if she just opened an online account. If she did not, she needed to call a toll-free number. When she called, Western Union told her, someone tried to transfer \$2800 out of her bank account by wire transfer to China. Western Union blocked the transfer at Amanda’s request. With her bank account compromised, she needed to take action to limit access to her account. Naturally, all this caused Amanda distress and anxiety, and it took a lot of her time to set up safeguards on other accounts susceptible to compromise.

This is human engineering at work. Or you can call it slick-talking. Same thing. Keep your guard up!

You can report scams, fraud, exploitation of the elderly, or other concerns to Seniors vs. Crime. Call me at the Clinton County Sheriff’s Office, 563-242-9211 extension 4433, or email me at randymeier@gapa911.us. Most of what I learn, I hear about from readers.

End of column/rmeier