SUSAN GUNN SOLUTIONS

Speaker • Author • Consultant • Fraud Examiner

Welcome to the Information Age

By: Susan Gunn

Big Brother is Watching. Or at least, in the 70's, we thought so. The illusion that the government had eyes and ears everywhere was at the forefront of our minds. Somehow, we believed, Big Brother (i.e. anyone in "authority," such as government, law enforcement, etc.) would use a twig to rat out the tree. We never wanted to say very much, as anything we said could be twisted and used against us. The paranoia of the McCarthyism mindset stayed with us.

We now live in an information age, where all knowledge is only a few keystrokes away. What a distance we have traveled in forty years. Without blinking an eye, we have started giving away our personal information to hundreds of "trusted friends" on social networks like MySpace, Facebook and LinkedIn.

After all, anyone that might read it only has our best interest in mind, right?

Without realizing, the personal information we randomly choose as our security questions is the same information readily available on Facebook, or any of the other deep wells of personal information to cull from.

Our lives are driven by remembering passwords to the thousands of "secure" websites and software programs we use daily. In the likely chance we don't remember, we then must remember the answers to our security questions to gain access; but, how secure are those questions, really?

Not to step back in the Big Brother era, but a loud clanging gong needs to be resounded.

Start with Passwords. As a fraud examiner, I am amazed at the lack of strong passwords for bank accounts and financial institutions. Recently, I learned one client's bank account password was "123DmD123!" and only that because of the site's requirements. It should go without being said, but this is *not* a secure password.

The amount of password cracking software now available is staggering. You can learn more about password cracking on Wikipedia than you are probably comfortable learning; however, the information may compel you to strengthen your passwords.

Yet, with websites being attacked and hacked at records speeds, the requirement to begin with stronger passwords prevails, but ends with the website encrypting those passwords to make the hack more difficult.

All Websites are Not Created Equal. For instance, some banks allow an assortment of special characters, while others do not. Some give a range of the number of characters to be used (7-10); while, all encourage, if not require, upper and lower case letters along with a number. Most website passwords are case sensitive.

Amazon, for example, requires a minimum of 8 characters, with a maximum of 128 characters and allows special characters. Baymard Institute conducted a useability study that determined 18.75% of existing Amazon users abandoned their accounts when they could not remember their passwords and then had issues with the "password reset" option. While the study itself was geared towards understanding E-Commerce and checkout processes, it also lends itself to understanding the user and password conflict.

After all, who abandons a checkout process at Amazon?

Don't Become a Hack. With the recent Equifax breach, the call for stronger passwords needs to be shout from the mountain top. Monitoring our finances can begin with strengthening our defense!

At the bare minimum, all passwords need to include upper and lower case letters and numbers. Depending on the site, add more than one special character. Typically allowed are "! * $ # @ ^" but some sites also allow "( ) ~ + { |" as well as others. Become friends with your special characters and explore the options of including them in your passwords.

Never, *ever*, have the minimum allowed characters. If the website allows up to 20 characters, choose 15 as a minimum. If the website allows up to 10, then 10 characters is what you choose. The more characters allowed, the stronger the password.

Create a different password for every site. Most use the same password, knowing full well they are not protecting their information as steadfastly as they should. These passwords must be properly maintained, though. Pen and paper can record them so long as that paper is secured. Password vaults are better. PC Magazine provides reviews on The Best Password Managers of 2018. These vaults can retain your various passwords for a low cost.

Some people treat passwords as an infringement of their personal space. However, if your information is breached, you will most certainly learn a difficult, costly lesson.

Security Questions & Answers. Amazingly, Facebook posters give out information that could be culled for website security answers daily. Look at the list of the security questions on QuickBooks. Most of these answers can be found online with relative ease.

There is a thread throughout Facebook that always intrigues me. It appears innocent enough and usually starts with "Let's have fun!" or, "Where have you traveled?" Beyond the obvious information gathering posts, we can gather favorite sports, anniversary dates, parent's names, your pet's names, the street you grew up on, and the list goes on.

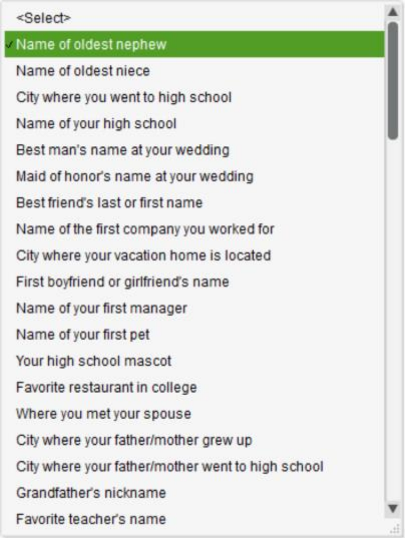
Go on, Google yourself. What information can you glean? I can assure you, every public social media account, like Twitter, Facebook and LinkedIn will appear. In my blog post, Equifax Breach: Part Two, I speak to privacy monitoring. This is an enlightening exercise everyone should undertake. Do not be complacent.

In prior days, this plethora of information was deemed private. It is amazing how that information has been lulled into being declassified, deemed safe to share, and seen as means of connecting with and supporting "friends."

Choose Your Friends Wisely. Are your security settings truly secure? Many colleagues accept everyone as a Facebook friend, then filter their posts accordingly. However, I have a rule to determining a "Facebook" friendship. If I have not shared a meal or conversation with you, then we are not friends.

My personal Facebook page is for my personal friends. I do have a readily open Facebook fan page for business colleagues that want to stay in touch. This goes against the advice of so many social media marketing experts, but stays in alignment with a greater number of security experts.

Of the 19 questions shown below, 10 of the answers are most probably readily available through online public records.



<Select>
✓ Name of oldest nephew
Name of oldest niece
City where you went to high school
Name of your high school
Best man's name at your wedding
Maid of honor's name at your wedding
Best friend's last or first name
Name of the first company you worked for
City where your vacation home is located
First boyfriend or girlfriend's name
Name of your first manager
Name of your first pet
Your high school mascot
Favorite restaurant in college
Where you met your spouse
City where your father/mother grew up
City where your father/mother went to high school
Grandfather's nickname
Favorite teacher's name

Fool Me Once. Continuing Education takes me to security conferences where speakers like Kevin Mitnick take the stage. I first learned of Kevin when I worked for a California corporation that had business relationships with one of his hacks. Possessing criminal records since the '80s, every time I hear Kevin speak, I am strongly compelled to change all my passwords.

Convicted and released, convicted and released, time and time again. How did he do it? Simple, he used social engineering to gain access. Kevin did it for the end game of accomplishment, not for financial gain.

Watch **this 43-minute video** on YouTube detailing the in's and out's of Mitnick's hacking, and tell me you don't agree. Kevin doesn't look or act shady. By all accounts, he is a normal guy with an extremely interesting talent. Skip to 39:09, hear his explanation of why he was a hacker, and be enlightened.

The average person is lead to complacency until they are jarred into a reality they have no desire to take part in. Most believe nothing like this could ever happen to them, that is, until it does.

It is the Information Age, after all.