Online Safety

The early internet gained massive popularity, in part because it was nearly anonymous and nearly free. In many respects it still is. However, it is also anonymous and free for those who have the worst of intentions.

Be careful what you put out there:

- Once you post something, you lose control of it. This is just as true for personal information as it is for silly cat photos.
- Facebook, Twitter, and any other social media is pretty much the same as the conversation in the corner bar, or gossip at the laundromat. You really shouldn't talk about **everything** there.

Know who you are talking to:

- If you get a text or an email, look at who sent it to you. If in doubt, contact them, by phone, email or in person, and ask whether the sent it to you, and what it's about.
- Do not click on something without knowing what it is and who sent it. Find out where the link goes to (your browser and email program often will display this information)
- Is the grammar good? Are there spaces where they shouldn't be spaces? Does it sound like something that your bank or your acquaintance would send?
- Be aware that malicious links can look very legitimate. Our good friends at Google just started selling website addresses like example.zip, which is all too similar to a legitimate, popular file type that also uses the 'zip' designation. Several technology experts have agreed with how UTTERLY STUPID it was for Google to start doing this. Bad actors have already started exploiting the ugly vulnerabilities this has created.
- Are you being asked for information the sender already should have? Your bank, for example, will **never** ask what your account password is, or what your debit card pin number is. When in doubt, contact them (by another method) and ask about it.

Do you want what they're offering?:

- Did you ask for what they're offering to you? If you didn't already ask about something, there is a real good chance you shouldn't go any further with it.
- Adopt a policy that if you didn't invite someone, they are not welcome. This works online as well as someone knocking at your door.

- Consider resisting everything that you haven't already asked for. You probably know whether your carpets are dirty more than that person who sent you that text message, or the guy standing on your doormat.

Does it sound right?:

- If it sounds too good to be true, then it probably is. Really!
- Does it make sense? Can you see the mutual benefit between the seller and the customer? No business can or would give away something for nothing. If it's a good deal, everyone should walk away satisfied.

Your Personal Information and your Privacy:

- Your passwords, personally identifiable information (like social security numbers and birth dates), address, and family information are things you need to guard.
- Many of these things are used by businesses to determine the identity of the individual using them. If a person just typed in the correct password, then they must be the correct person. If you don't guard your passwords and personal information, you are making it easy for someone to pretend that they are you.
- A growing number of places are using what's called 'two factor authentication', and you will receive a text message to answer, after typing in a password. Since **you** are likely to be carrying **your** phone, this is another assurance that the person who says they are you, is actually you. Use two-factor authentication.
- If something seems to be not right, ask and verify it.

Apps on Your Phone:

- Consider the apps you choose to install on your phone **carefully**. Do you need it? Do you use it? If not, uninstall it.
- Nothing comes for free. Those 'free' apps get reimbursed somehow, and so much of the time is making you an outlet for advertising, or to get information about you, which they then use or sell.
- Do not install apps that access your bank account unless you really need to have that app, and you trust the company behind it. If you also have a home computer and can opt for doing business there, rather than on your phone, it is well worth considering.

Let's Talk About Google:

- Google gives the appearance that they give away tons and tons of stuff! Their search engine is free, and their email service is free, and their GPS navigation service (Google maps, android auto) are free, Google translate is free, Google office is free, and there are tons of other services that are free or very low cost . . .
- . . . no, No, NO! - none of it is free! Google is one of the world's biggest money-making companies. What they take, in trade for all these services, is what they learn about YOU, while you use those free services, and then they sell what they've learned about you to companies willing to buy that information.
- You tell Google what your interests are by using Google search. You tell Google where you go by using Google maps, you tell Google who you know when you use Gmail. And on, and on, and on. Google collects that stuff and sells it. So does Facebook, so does twitter and pretty much any company offering any technology for 'free', including smartphone app makers. **Nothing comes for free**.
- Like most everyone, I use several Google services (both the consumer and software development services they offer), and I am a Facebook user, and I have accumulated a few other accounts I no longer use (like twitter and myspace). I am aware of the trade-offs, and I am also aware that any of this can backfire, at some future time (face it, the rich always want to get richer). Keep in the back of your mind, that just because it's available and it's easy, doesn't mean it's automatically a good thing.

Arm Yourself With Knowledge

- Include some technology news with local, national and weather news that you listen to or read. They talk about online safety concerns on the news.
- Be willing to ask about any concerns you may have. You can always go to technology people with technology questions, and the companies you do business with should be able to answer questions about how their companies do business online.
- There are online technology newsletters out there. I get a newsletter from an organization called Kim Komando (komando.com), every morning, which discusses a lot of online safety issues, how-tos and hints. There are also others, some more technical and some not.