You have so many electronic devices capturing data! Whose seeing that data? Even your car has a computer that shows error codes. There are not really any types of electronic devices that don't store information, unless they are manual, like a wind up-watch.

With the large range of devices that connect to the Internet it's important to protect them. Keep in mind almost all data, voice, text, videos, IP, MAC addressing is tracked somewhere is log files. This collected information is a trail of all activity online and accessible; online can be a physical cable or wireless.

Any device that connects to the Internet has a MAC (Media Access Control) number like `00:15:6D:73:45:2E`; this is hard to fake and is unique to the vendor and device. So when you're traveling in cyberspace keep in mind you are being logged and each piece of data you submit is going somewhere for use by something else; could be your just a statistic.

Top 16 ways to help stay secure:

1.) Protect your social security number; be cautious when using it. If mailing in an application see if the number can be called in directly; online be super careful. Never use as a PIN, password, or other electronic access code.
   a. Never provide over the phone to someone who has called you. Always verify the phone number is the legitimate number for the organization, don't simply call a number provided to you on a piece of paper or web site.

2.) Avoid Phishing Scams; this is becoming more common as a popular way to steal someone's identity or fake a website interface. Before you submit any data to someone requesting look up the requester utilizing a search. Sometimes the site clone looks so good you can't tell the real from the fake. Even e-mails look official with logos, colors, and forms.
   a. You can actually trace the IP address and narrow down if the site is known to be malicious. I like to use http://www.dnsstuff.com/. Today's news sources also keep you updated on Internet scams. Researching online will help you become a better online surfer.
   b. Phishing scams can hack into your friend's or family's address book and auto-generate an email to everyone within it to spread automatically. Unsuspecting people, trusting that friend or family member open the email and they get infected. To protect yourself, beware of:
      i. Incomplete email messages that perhaps contain nothing but a link, especially if the link is an address you don't recognize.
      ii. Poor grammar, messages that make no sense or whose subject line isn't something that the sender would write.
      iii. Messages that don't include your name, example ("hi Sally").
      iv. Aren't addressed the way the sender normally addresses you (instead of "hi Sis", do they call you by a nickname but this email includes your legal name?).

3.) Protect what you post on Social Media websites. Social Media has its place on the Internet, but there are times is misrepresented and used for foul plots of deception. Never assume the information is valid or who is being represented. I'm not a big fan of sharing too much information on these sites. Many investigating firms/others like to research you on social media websites; they may not get the correct impression of you.

4.) Do not share Secure Passwords, don't write down; Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary when being hacked, and make sure they are at least eight characters long. There are password cracking programs that stroll the Internet looking for weak or easily guessed passwords. Passwords should never spell any word in the dictionary. I like http://www.random.org/passwords/ for passwords. Hackers can do allot of research on you just by Google-ing your name, so make any password you use secure.
   a. I've seen quite a few e-mail usernames and passwords cracked; then the e-mail address is exploited to send SPAM and other messages. The ISP (Internet Service Provider) has to step in sometimes to correct the problem or block the offender.
   b. Consider changing your password on a quarterly basis.

5.) Never throw a hard drive or other storage device away without destroying the data. Depending on the data being destroyed I often replace the hard drive, and keep the old hard drive. There are a number of hardware and software utilities to do this. It's the same concept as shredding any important document before putting in the trash can.
6.) Be aware of Behavioral Advertising – this is where you visit a merchandise site looking at merchandise, then that merchandise item shows as a ad on other websites you visit. This is big business now, they know what you looked at, and at how many sites. These 3rd party cookies drive many Internet sales.
    a. Most websites are free to you to access because they sell ad space to advertisers to make money. The website tracks your activity and based on what you do, presents ads for products they think would interest you. Website publishers have to make money somehow to pay for the upkeep of the website.
7.) E-mail is one of the more attacked and common communication envelopes. The Electronic Communications Privacy Act (ECPA) tells you how to protect your legal rights regarding email communications. I don't consider free e-mail services secure; they are often loaded with non-solicited information or internal links the just clutter your inbox.
    a. Don't open suspect e-mails; delete them.
8.) Don't allow someone to get on your computer that you have not researched or solicited assistance from. Some scams indicate they any fix any issue online or speed up your computer…well, if your computer is acting up take it to a computer vendor. It's safer, and if your computer/electronic device is acting up you should not be online.
9.) Every MAC address and IP address is tracked. As mentioned above, everything is track-able; and you never really know who/or what you are communicating with.
10.) The safest place for your backed up data –your pocket. The Cloud is a great new technology and Serves a great need; I would not put my stored data there at this point. Attacks against networks are always where the data resides. Remember to protect/secure your storage device. Apply a good routine of backs and secure physically where you have the most control.
11.) Keep your device up-to-date with system updates and intrusion/virus updates. Apply patches to your devices. Know your device, not a fan of automatic updates, sometimes they fail. Check for updates weekly, it easy with a few clicks of the mouse.
12.) If you have a wireless connection you use ensure you change the default password and change the SSID. Allot of users make a trip to the store, buy a wireless router, plug-in-play and never change the defaults on the device. This makes an easy target for someone to get on your network they could even lock you out.
13.) When shopping online always research the company contact information, address, and, return policy. If using a credit/or debit card - The Payment Card Industry Data Security Standard (PCI DSS) applies to any organization that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit credit card/debit card data. Since the end of 2007, any organization that accepts payment card transactions must be in compliance with the standards. The 3-digit security code can never be stored; the credit/debit number is vaulted and tokenized.
14.) Keep an eye on phone numbers, with VoIP (Voice over IP) you never really know where the call originates from. You can always enter the number in a search panel and find the basic information.
15.) Clear my cookies (How users are tracked.) – I like to clean on the cookies installed on my devices. This cleaning can be a little time consuming, but keeps some of my tracking information out of the hands of information hounds.
    a. Common type of cookies: Session, persistent, Secure (HTTPS), Flash Cookies, Zombie (re-spawned automatically).
    b. Knows of the users: Pages visited, time spent, from/referral, name, location, search history, website activity.
    c. Possible Known's: Name, address, favorite music (example), places most visited/habits, tracking across multiple dimensions and properties.
16.) Do an occasional reboot of your devices, router, wireless router, Server, etc. A nice reboot clears out the RAM (Random Access Memory) and other registers. Usually a device that's having issues works better after a reboot; if not there are other problems that need to be addressed.

As long as information can be gathered it will be used. Who gathers the information, stores, and utilizes in the big question. Some data collection is a tremendous help when used positively. Other forms of data collection really nail us down to specifics that we may not want to share with the world.

Domain Registration – You should always ensure the source that is registering your domain (unless you personally register) allows you Administrative Privileges so you can control the domain. If you don't, the person registering the domain has all of the rights to the domain. And it's very tough to gain back the domain.

Compromised Device – If you feel your electronic device has been compromised, power off. Devise a plan to restore; be careful if you restore a backup, the compromised files may be within the backup. If resetting/formatting the device is a option look a closely. Starting from scratch is a good way to ensure the device is back to factory defaults.

Wade LeBeau, VP Fabulous Fiber, Network Operations Director