Computer Privacy and Security

This has always been important, but has recently become more important. In February 2017 the President and Congress rescinded rules that limit the security that telecoms must exercise on the transmissions of their customers. Worse, telecoms may now sell any and all data transmitted by their customers, regardless of customer consent (I expect the telecom to require my consent to this before I can continue to use their service). As revealed by the Snowden NSA surveillance documents, HTTP web traffic can also be collected and searched by government agencies without notice to users or webmasters.

Computers are ubiquitous these days and many users have little-to-no understanding of computer technology. This article intends to explain computer privacy and security so that the non-tech users can protect themselves. For the most part it applies to personal computers, but some of this can apply to smart phones and tablets. This article applies to home users, which are one or more people who share the same computer at home. This article does not address the issues that are uniquely applicable to offices with several computers, each with one or more users.

Technology changes. The basic concepts usually persist through several generations of technology. Which is to say, what exists today may not exist a year or more from now.

Vocabulary

We must start here, as there are a number of terms that apply.

Privacy. This applies to access by others to your personal data. The basic concept here is that only people, organizations, and businesses that you explicitly authorize should have access to your personal data. This data can be subjected to unauthorized access when it is "downloaded" from your computer or from records of your Internet activity. Personal data can include:

- Name, address, telephone number, birth date, social security number.
- Current geographical location.
- Email address.
- User id, password, security question and answer.
- Credit card number and expiration date.
- Account name and number.

Whereas most of this article is focused on personal data that is embedded in network messages (see below), it can also apply to personal data on the computers of firms you do business with, like a bank, securities broker, and retail store.

Security. This applies to access by others to your computer, in particular to the computer's configuration and your data files. This data can be subject to damage by external agents who access your computer directly from the outside. Typically these agents "upload" programs that corrupt your files and/or download your files — all without your knowledge and permission.

Connection. Personal computers are typically a collection of devices that are connected directly to each other with cables. The monitor used with a desktop computer is connected to it with a special cable, while laptop computers have the monitor built in, and the capability to connect a second, standalone monitor. A computer is often connected to a printer. Other devices that may be connected to a computer include a mouse, a graphics and/or pen tablet, an external hard drive, and external speakers. This collection of devices represents a "system," not a network as described next.

The nature of the connection has traditionally been cables. Cables are linear bundles of wire encased in a cover with a special connector at each end. Some types of connectors have special uses, such as the one that connects a separate monitor to a computer. More recently, wireless data transmission technologies have been developed and widely adopted. They go by names like Wi-Fi, Bluetooth, and RFID.

Network. A network connects two or more computers with each other. This allows several computer users to communicate with each other and share files. There are a number of ways to "type" a network, but what is most relevant to this discussion is that home users are the primary audience. A local network only connects computers within your home. An extra-local network connects your home computer with external networks such as the Internet.

Computers can be connected to a network with cables and/or with wireless data transmission. The network cable is called an Ethernet cable.

Home networks typically have one computer designated as the network host. All the computers in the home are connected to the network host computer, which is connected to the Internet.

Smartphones have several wireless network connectivity choices; 2G/3G/4G (choice may depend on the capabilities of your phone and your phone service), Wi-Fi, Bluetooth, and RFID.

Upload/download. Upload refers to the situation where a program on/from an external network location sends data or file(s) to your computer. Download refers to the situation where data and/or file(s) are sent from your computer to an external network location.

Telecom. This is the abbreviation for a company that provides telecommunication services. Telecoms started out as telephone companies. With the entrance of the Internet into common home use, they added network access to the Internet. AT&T's first product was telephones and telephone networks. When you needed a home phone, AT&T sold you the phone (with its telephone cable) and ensured you had an operative telephone access point in your home. Cable companies later entered the scene, offering cable-based television service (CATV) and, eventually, CATV-based telephone service in which the internet traffic is routed over the cable television line; note this "cable" is a specialized kind of cable as discussed above as Connection.[1] Other American firms include Verizon (which provides only wireless phone service) and dishNET (which provides only satellite-based service).

Most telecoms provide you with an external wired access point, hardware, and cables. Typically, the wired access point is already installed in a wall of your home, its outlet may look like a telephone outlet; it is connected with cable to the telecom's wired Internet network (DSL or CATV), which is external to your home (and perhaps half a mile away). The hardware typically is a network router (sometimes called a gateway). The installer connects the router to the wired access point (with a cable) and to your computer (with a cable). "Modern" routers offer wireless connection as well; your use of this is optional.

ISP. This is the acronym for Internet Service Provider. A telecom that provides internet access is also an ISP. Every website is hosted on the computers of an ISP; "hosted" means the site files are resident on the computers. Your telecom assigns you an email address when your service is started. (You can always have different email accounts on different hosts, such as Google Mail and the ISP that hosts your website.)

[1] Technical details of CATV-based internet access for those willing and able to follow them: The typical CATV-based system used throughout the USA consists of (1) video collected from local TV stations and cable TV programming suppliers via satellite, (2) fiber-optic cable to neighborhood nodes that then (3) distribute the signals to homes with RG-6/U coax cable. The CATV network was primarily designed for downstream transmission of television signals, most of the existing networks are being refitted to support two-way data transmissions.

All telecoms are ISPs, but not all ISPs are telecoms.

Webform. This is a web page on which you enter text. You may also upload files on the page; often these files are text documents and photographs. Webforms have text boxes and buttons (that mimic what you will find on standalone applications that are installed on your home computer).

Webmail. This is a functionality of viewing received and composing-and-sending email messages on a web page. Typically the web page belongs to the provider of your email address. For example, if you have a Gmail account, your webmail has a URL that begins **https://mail.google.com** . Webmail pages contain webforms (which may be hard to recognize); certainly the area of the page in which you type a new email message is part of a form.

Network Message. From the technical perspective, any single conglomeration of text and images that is sent or received over the Internet (or any external network) is a "network message." Incoming network messages include a web page received with your browser (which may include hidden items), an email message received with your local email client program (I use Microsoft Outlook), or a request (such as for a help topic) sent by a local program on your computer. Outgoing network messages include your browser's request for a new web page, webform data that you completed entering (only the form data, which does not include all the content of the web page), and an email message sent by your local email client program. The network message contains the network address of the destination and that of the origin. Of particular value to this discussion is that the contents of the network message are accessible by your telecom (including the incoming hidden items); as such, your telecom can store the messages "offline" for future examination, analysis, and eventual sale.

Encryption. This is the process of encoding a message or information in such a way that only authorized parties can read it. The original message is encoded with a special algorithm, commonly called a key. Once encrypted, a message must be decoded in order to be read in its original state; decoding requires a special algorithm (key) which may be the same as or different from the key used to encode the message. Theoretically it is possible to decrypt a message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources, skills, and time are required. There are two types of keys. A symmetric/private key scheme uses the same key for encoding and decoding. A public key scheme uses a publically-available key to encode messages, but a private key for decoding. This second scheme is the one primarily used today over public networks.

SSL. This is the acronym for Secure Sockets Layer, which is the standard security technology for establishing an encrypted link between a web server (which hosts websites and email) and a browser. Netscape developed the original SSL protocols, the earliest one was published in 1995. the latest version is SSL 3.0 which was defined in 1996. All SSL versions were found to have insecurities and have been deprecated (prohibited); SSL 3.0 was deprecated in June 2015. They are, however, still in use awaiting a better method that has been approved.

TLS. This is the acronym for Transport Layer Security, which replaced SSL. The first version was defined in 1999. The latest finalized version, TLS 1.2, was defined in August 2008. It was modified in 2011 to remove backward compatibility with SSL. Note that all three versions of TLS have been defined as proposed Internet standards, but have not been formally accepted/approved. Before a client and server (the network endpoints) can begin to exchange information protected by TLS, they must securely exchange or agree upon an encryption key and a cipher to use when encrypting data.

HTTP. This is the acronym for Hypertext Transfer Protocol. HTTP is a protocol for data communication for the World Wide Web (Internet); as such it is the foundation of Internet networking. It is the technology for sending, over a network, requests for web pages from your computer and receiving those web pages on your computer.

HTTPS. This is a form of HTTP with added security. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security, or its predecessor, Secure Sockets Layer.

HTTPS provides three security guarantees:
1. **Server authentication** allows users to have some confidence that they are talking to the true application (web) server. Without this guarantee, there can be no guarantee of confidentiality or integrity.
2. **Data confidentiality** means that eavesdroppers cannot understand the content of the communications between the user's browser and the web server, because the data is encrypted.
3. **Data integrity** means that a network attacker cannot damage or alter the content of the communications between the user's browser and the web server, because they are validated with a cryptographic message authentication code.

HTTP provides no privacy guarantees, and applications that use it cannot possibly provide users any privacy. When using a web application hosted via HTTP, people have no way of knowing whether they are talking to the true application server, nor can they be sure attackers have not read or modified communications between the user's computer and the server.

Web browser. This is the program on your computer that you use to access websites on the Internet. It is also referred to as a "browser." Current web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari, and Opera.

URL. This is the acronym for Uniform Resource Locator. It is commonly and informally termed a web address, although this is not strictly accurate. Browsers have a text area into which users type the URL of a web page they want to access and view (Firefox and Internet Explorer call this the Address Bar). An example of a URL is: `http://www.example.com`

Domain name. Every website and web page is "owned" by a domain. The domain name is a part of the URL. In the example above, the domain name is `www.example.com` .

VPN. This is the acronym for Virtual Private Network. It is a virtualized extension of a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to a private network. A VPN encrypts all data traffic to and from your phone, tablet, or computer by routing it through the VPN provider's server. Using a VPN won't stop apps and ads from collecting and transmitting your personal data, but it will make it much more difficult for spies or hackers to eavesdrop on those transmissions. A VPN is not a completely foolproof solution to privacy, but it can be very helpful.

IP address. Every device on a network has a unique (network) address that is represented by an IP address. IP stands for Internet Protocol. The original form of the address (called IPv4) had 4 segments of numbers and used 32 bits); when the limit of the available numbers began to be exceeded by the demand for addresses, an 8-segment form was adopted (called IPv6) which has 128 bits and eight groups of four hexadecimal digits with leading zeroes omitted. Common IPv4 addresses look like **10.48.29.12** . Common IPv6 addresses look like **2001:db8:85a3:0:0:8a2e:370:7334** . Your computer's IP address is actually the IP address of your internet router, and that address is assigned by your telecom.

Firewall. A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network (such as your home computer) and an outside network, such as the Internet, that is assumed not to be secure or trusted. They are considered by network engineers to be appliances. There are *hardware*-based firewall computer appliances and *software* appliances running on general purpose hardware (such as your computer). Firewalls are generally categorized as *network-based* or *host-based*. Network-based firewalls are positioned on the gateway computers of networks (local, extra-local, and internet). Host-based firewalls are positioned on the network node itself, e.g., your computer or, if you have a home network, your home network's network host.

Internet Privacy Issues and Methods

In light of the ability of telecoms to sell your Internet activity, the most important thing to remember is that every network message that you send and receive can be stored, examined, analyzed, and sold—piecemeal or in its entirety. When you are viewing a web page, everything you see on your monitor can be saved by your telecom. When you enter data in a webform, that data can be saved by your telecom. When you download email messages to your local email program (like Outlook), the contents of every email message can be saved by your telecom; likewise every email you send from your local email program can be saved by your telecom.

Using Wi-Fi instead of an Ethernet cable to connect physically to the internet is especially hazardous to your privacy. Wi-Fi messages can be monitored remotely without your knowledge.

Some websites require you to use an account to interact with their site. Such an account consists of, at a minimum, a user id and a password. When you access that website after your account has been created, you must login. You login by entering your user id and password (on a webform!). Often times as you type the password, the characters are replaced by asterisks; for example, you enter "BoatsRUs" but what appears on the monitor is "********". This technique only works to hide your password from someone standing near you and looking over your shoulder. The actual password is what is sent to the website and included in the network message, which your telecom can read and save. In conclusion, the asterisks do not offer you any privacy with your telecom.

You may be able to specify that a web page open with security. To do this, you enter into the browser address bar a URL like `https://www.example.com` . The presence of the "s" in "https" directs the website to use security when it returns a web page to you. You can verify this by examining the contents of the address bar when the requested web page is displayed.

Some web sites will automatically return web pages with security. You can see this when your web page request began with HTTP (if that was entered at all[2]) and the address of the returned web page begins with "HTTPS." You can install a third-party "tool" (plug-in) to automatically use HTTPS security on many sites; for Firefox, I installed **HTTPS Everywhere** (a program developed by a collaboration between The Tor Project and the Electronic Frontier Foundation); it also works on Chrome and Opera. It works by automatically requesting most web pages as HTTPS.

[2] Modern browsers rarely require users enter **http://** or **https://** in the address bar. Nor do they require users enter **www.** When those components of the URL are missing, the browser automatically adds them. Hence, when you want to access **http://www.example.com** you need only enter "**example.com**".

Your browser may not require you to enter a web address that begins with "HTTP." In that case, the browser automatically adds the "HTTP." If you have been relying on this, you may have to deliberately change your practice.

Not all web sites support HTTPS. When that is the case, if you request an address with "https", you may get an error message from the site or from your browser. At that point you have to decide how risky that page might be to your privacy.

In any case, if you are presented with a web form on which you are asked to enter personal data, do not do so if the web page address does not begin with "https". When you encounter this situation, contact the site as soon as possible and complain — let them know you need to be assured of the privacy of your data.

Use passwords that are not obviously you, and change them frequently. Use a different password on different sites. Remember, people trying to access your personal data use software, often with random password generators, to guess your password. Once they find a password that works on one site, they will try to use it on other sites.

For each email account that you have, find out what type of protocol the ISP or email host uses for mail transfer. This is not necessary when you use their webmail program.

For each email account that you have, configure the email program, be it a standalone program like Outlook or a webmail program, to encrypt the email message. You may be able to configure the program to encrypt all emails, or just one at a time. You can likely find directions on the internet: search for something like "encrypting email outlook 2003." Frankly, this can be easier said than done. I can do this with Outlook, but it requires I get a "digital certificate", which is not free and involves some challenging installation—I decided to wait.

Another way to protect your privacy is to use a VPN, which means you access websites and email via the VPN. You have to buy the VPN and then undergo an installation which may tax your patience and technical knowledge. Not all VPNs are created equal, so if you are considering this option, research them carefully.

You may be able to get a dynamic IP address for your router; such an address changes every time you log on to your telecom. It is advantageous in that transmissions from you cannot be associated with your geographical location and you cannot be addressed directly by your IP address (as it will be different during a subsequent session). The alternate scheme is a static IP address, so that all transmissions by you will be associated with the same IP address.

Log off websites, including webmail and social media, when you are through using them.

Turn off your computer when you are done using it each day. That will keep intruders out.

Don't post on social media accounts while connected to cellular data networks.

Turn off Wi-Fi, GPS and geolocation on your smartphone. They can all be used to quickly pinpoint your location.

Social media also has the ability to track your browsing. Look for information about that and how to block the browsing. If you use Facebook, log off every time you leave it. That will reduce the site's ability to track your browsing.

If you use your smartphone to interact with “apps”, they can track you afterwards, including your geographical location (through the GPS function). The built-in method of the cell phone to organize which cell tower to connect you to also provides a history of your location; the only way to stop this is to turn off the phone.

On your smartphone, turn off cellular data connections. If you don't need to receive constant email updates when on the go, turn off cellular data and go online only when connected to a secure, password-protected Wi-Fi network. You'll still be able to get text messages and voice calls, and your battery life will probably improve.

The National Security Agency (NSA) and police departments have devices with which they can tap into cell phone usage directly from cell towers and eavesdrop on your activity. The only way to protect yourself from this spying is to not use a cell phone.

Internet Security Issues and Methods

Security of the files on your computer, including the individual applications and the operating system, are at risk from programs installed without your knowledge. These dangerous programs are installed on your computer in two ways: (1) by agents that send messages to your router (these are often called hackers or intruders) and (2) by programs that download themselves when you click a link in an email or on a web page. Once installed, these dangerous programs (generically referred to as “malware”) start up and do what they were programmed to do. Malware can corrupt your files, delete them, and copy them to any internet address. The malware may remain on your computer until you find and remove it.

It gets worse: some web pages contain malware that can be automatically downloaded to your computer when you open the page— unless you deliberately block it.

Malware has been used to collect ransoms: typically you have to pay the owner of the malware to restore your files and/or your access to them. Ransom malware has been used on commercial websites that hold medical records: the site and the medical records are only made accessible after the site owner pays a ransom.

Best practices:

a) Use a firewall. This blocks most agents trying to access your computer. The best firewall is a hardware firewall, and likely is a part of your router. The next best is a software firewall, which may be bundled with your operating system or which you may have to buy and install. If you take this path, be sure to research the functionality of each choice carefully (expect exhaustion).

b) Periodically check your router’s records on suspicious access. Your router’s configuration is typically accessed with a browser and with an IP address like **192.168.1.254** The Settings section will probably contain the logs, of which there may be a firewall log.

c) Configure your browser to block automatic downloads. The directions for this are specific to your browser. So you will have to search the internet for a solution. Search for “block automatic download Firefox” or “block automatic download Chrome”, et cetera.

d) Be very cautious about clicking a link in an email; links are typically rendered in a different color and may be underlined — which is to say, there is no standard formatting to rely on. Some email programs and webmail programs will show you the actual domain name (e.g., `www.example.com`) in a tooltip when you hover the mouse pointer over the link. If this happens, compare the actual domain name with the link text or the domain name of the sender; if they are different, do not click the link. If your program does not show you the actual domain name, there are ways to find the URL for the link, but they are complicated and technical. If you use a webmail program, it likely has a tool you can use to discover the URL: try right-clicking the link to open a context menu, then select an item like "Copy link location," then paste whatever it is into a new browser window/tab address bar. Again, compare it with the domain name of the sender.

e) Be very cautious about opening email attachments. They often contain malware agents, and just opening the file may be enough to install them. Never open attachments on emails from people (identified by their email address, <u>not</u> their name) you do not know — these are usually classified as "spam."

f) Install virus protection software. Some such software interrogates every transmission (which can add considerably to response time). Other software can scan your computer's hard drive periodically and/or on demand. Do scan weekly.

g) Backup your data periodically. You backup files to an external data storage device, like an external hard drive or a thumb (USB) drive. Backing up your data to cloud storage is no guarantee of security or privacy.

h) Do your part to protect other users from spam by forwarding spam emails to the Federal Trade Commission (FTC), which is the federal agency tasked with putting spammers out of business and behind bars. The email address for the FTC is **spam@uce.gov**

i) Periodically clear your browser's history, especially cookies. These can be accessed by intruders who can use them against you.