Online Security & Privacy 2002

By J.D. Abolins

Introduction: Changing World of Personal Computing

In the early days of personal computing (early 1980's) , personal computers (PCs) were standalone devices. Information security and privacy concerns back then revolved around mainframes and big computer database systems. PC security problems mainly involved direct physical access to the PC.

Then came modems and computer bulletin board systems (BBSs), making PCs connected to other computers. Hacking of BBSes and, sometimes, computers calling to BBSes started to appear. The big privacy issues were over interception of email on BBSes and the possibility of authorities monitoring BBS communications. Law enforcement raids on some BBSs , such as the Illuminati BBS run by Steve Jackson Games, raised some concerns about the confidentiality of information on the BBSs.

This all became tame in the mid-1990s when the Internet became widely available and the Web made it popular. Now, most PCs (and many other devices) are networked to the Internet, a global network of networks. One's computer neighborhood is the world. Also, people started do more things online: buy things, do banking, conduct government transactions, etc. We are getting more done with our PCs but we also have more to lose. Meanwhile, the systems, the networks, and the interactions among them have been increasingly complex, making it harder to discern what is happening on the systems.

On top of all this came the terrorist attacks of September 2001 and the responses to the attacks. The legal and social changes since last fall have had a tremendous impact upon online privacy. [1]

What do all these things mean for the average person using the Internet? This paper will examine selected aspects of online security and privacy as it applies to individual computerists.

---

[1] The legislation and other measures following the September 11, 2002 have affected many existing privacy laws in the United States. The PATRIOT act, for example, has many provisions that apply to computer crime rather than to the type of terrorist attacks that occurred last year. The Electronic Frontiers Foundation Web site offers a good overview of the impact of the PATRIOT act upon Internet users. (See http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html.)

The basic thing to know is that the provisions for surveillance of online users has increased while the checks and balances have been reduced. The other thing to know is that the laws are not going to be as protective of personal privacy nowadays.

First, Is Online Privacy an Oxymoron?

"You have zero privacy anyway… Get over it."
Scott McNealy, Sun Microsystems; January 1999[2]

While most people appreciate some need for online information security and see it as attainable to some practical degree, there is some debate about privacy. One argument is that our online activities leave so much of a trail, we cannot practically control information disclosures. Therefore, there is zero privacy online.

Another argument, usually not overtly stated, is that the future of various businesses and modes of commerce depend upon access to consumers' personal information with minimal challenges. This, however, is not really an explanation of whether or not there can be online privacy. It is more of an exhortation for people to not even seek having privacy.

Online privacy is not an "all or nothing" proposition. Absolute privacy is very difficult to achieve online but much can be done to gain a good degree of relative privacy. Just because there are going to some information disclosures that one might not prevent does not mean one has to live in a fishbowl. Now let's look at some ways of protecting our systems and personal information.

At the PC Itself

The way that a PC is setup can help or hinder security and privacy. One of the basic factors is the physical access to the PC.

An old computer hacking adage is "if I can get to the computer physically, I can 'own' it."[3] If one's PC is safely locked up when one is not around, it is a bit easier to secure. But if the PC is shared with other people or kept in an area accessible to other people, such as shared PCs in libraries and schools, protecting it is a bit more difficult.[4]

Hardware Keystroke Loggers

---

[2] "Sun on Privacy: 'Get Over It':; WiredNews.com; 26 Jan 1999; http://www.wired.com/news/politics/0,1283,17538,00.html

[3] "To own", in hacker jargon, means to gain full control over the system. By the way, "hacker" *as used in this paper* doesn't mean a computer criminal. It means a person who has a passion for experimenting and learning about systems. Some hackers may use their skills and interests for overtly criminal ends but this is a subset of "hackers". There are hackers whose activities can be quite beneficial. Without hackers, we would have things such as the Internet, Linux, etc.

[4] In some cases, it may be best to not use a widely shared computer for any transactions or communications that are really sensitive.

One snooping technique is the use of keystroke loggers. The loggers will capture any thing typed upon the keyboard, including passwords, passphrases, and credit card numbers. The loggers can be software or hardware based. If one's PC has a keystroke logger, most security and privacy measures will be foiled. Some methods of foiling software-based keystroke loggers will be examined later in this paper but we'll look at hardware-based keystroke loggers here.

Hardware keystroke loggers are now sold to the public on the Internet and in some specialty stores as a family and workplace monitoring tool. (Of course nobody would ever buy one of these devices to intrude upon anybody's privacy or to steal sensitive information, right?) One type looks like a little cylindrical plug like the one on the end of the keyboard cable. It goes between the keyboard cable and the PC's keyboard connection. Another type is built into a keyboard.[5]

It pays to familiarize oneself with one's PC. If there's something out of the ordinary, like a new cylindrical "adapter" in the keyboard connection, it should be checked out. It is also good to check for such devices on computers at libraries, schools, and cybercafes.

Operating Systems

Operating systems and their impact upon security and privacy is a vast and contentious topic. For the purposes of this paper, the main things are

1) Some operating systems were designed to be single user systems (even with an apparent "login/password" screens) while other operating systems were designed to be multiuser systems with a good degree of security.

   Windows 95, 98, and ME are good examples of the first category. It is easy to bypass the login screen and access most of the files on the PC. The login really acts as a customization rather than a security feature.

   Windows NT, 2000, and XP, as well as Linux, BSD, and other Unix type of operating system, are examples of the second category. They are much better ones to use where others will have access to the PC. Even if the PC is accessible by just one person, there is a advantage to the multiuser operating systems' security. They protect the system from the user's own mistakes or from programs doing something harmful.[6] (Ever wipe out important system files by an error in deleting files?)

2) Whatever operating system one uses, be sure to keep up with security patches for it. Check with the vendor's Web site periodically. The advice about security patches also applies to other software besides the operating system.

---

[5] Examples of these hardware based keystroke capture devices can be seen at the KeyKatcher.com site at http://www.keykatcher.com/

[6] That protection works if one does not fall into the habit of using the computer as "root" or whatever administrative account.

By the way, be wary of emails with attachments that claim to be security update patches. The attachments should not be run. There is a great possibility that the email could be a fake security alert with a malicious program being presented as a security patch. It is much safer to go directly to the vendor's site and download the current patches.

Home Firewalls

"Who'd want to break into *my* PC?" is common response people have when home firewalls and other security tools are mentioned. There is the notion that the main computer exploitation risk comes solely from people who seek to break into corporate or governmental systems. But there are other risks.

Because home computers are now connected to the Internet round-the-clock just like institutional and corporate computers, they are now more visible on the Internet. Some people are opportunists seeking any connected system to exploit for fun or for practice.

Then there are various programs that can open outbound Internet connections from one's system. Some are trojan horse programs, others are built-into software applications. (If you are interested in seeing what can be seen on your system from the Internet looking in, try the tests at the Gibson Research Center Web site at http://grc.com/.)

Firewalls are one category of tools that help filter inbound and outbound connections. They are not the panacea that some people think they are but they are handy to use in conjunction with other security and privacy tools.

What firewall to use is beyond the scope of this article but one good program to consider is Zone Alarm from Zone Labs at http://www.zonealarm.com. One of the nice things about Zone Alarm is that it detects attempts by software on one's system to connect tot he Internet. It is easy to use and there's free version available.

Among some of the home firewall products are BlackICE Defender and Norton's Internet Security. You can research these and other firewall products at the Home PC Firewall Guide <http://www.firewallguide.com/>.

Anti-Virus and Anti-Trojan Software

Although the anti-virus software have often been hyped as major security tools, they can be useful in countering some of the security and privacy problems from computer worms, virus, and trojan horses.

Anti-trojan software, such as Pest Patrol < http://www.pestpatrol.com/>, is a special type of a security tool that detect various software routines that don't fit the normative virus or worm categories. They can detect things such as "spyware" and "adware" which may be

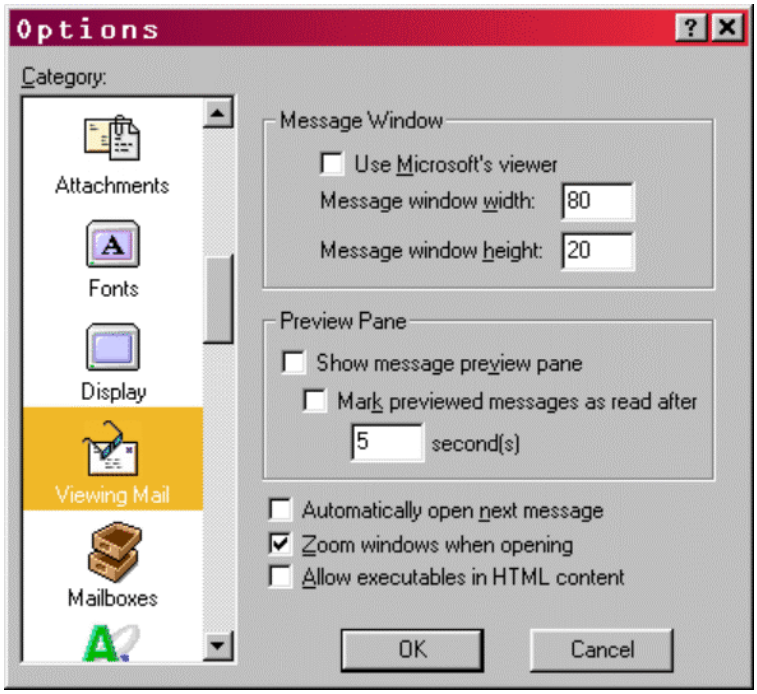
installed by various software products.[7] Often, they can detect programs that act as software-based keystroke loggers.

The Defaults May Be at Fault

A common computer security problem is that many products have defaults that are poor for security. This is often done because of the assumptions that people don't really care about security or that secure settings would get in the way of functionality.

When installing new programs, choose the "Custom Install" option if it is available. Even though one might not change any of the suggested settings, the custom installation menus and prompts will give useful clues about what is being installed onto the PC. Sometimes, one may see programs that aren't really needed and can deselect them.

Once software is installed, take the time to check the settings and preferences. Often a check of the settings can show options that help security and privacy. For example, in some email software, one can gain an extra measure of security by not having the emails automatically hook into a Web browser such as Microsoft's Internet Explorer. Here is an example of a Eudora options menu where such settings can be made:



[7] There has been a trend for some software providers to sneak extra programs having nothing to do with the offered software. Some of these extras serve to pop up advertisements. Others report how the person is using the computer. There are other types of extra programs snuck in. As this paper is being written, a software company has been accused of sneaking in a file sharing program along with its own software. See ZDNet's *Week in review: A Brilliant plan* at http://zdnet.com.com/2100-11-876709.html.

Look Ma', No Cables!: The Challenge of Wireless Security & Privacy

Wireless networking shows in many forms: cell phones, portable data assistants, and wireless network cards for homes and offices. The Wireless networking is very convenient. No wires to run through the building. It's easy to move the computers.

But the wireless networks have a special security and privacy challenge. The data transmission is not along distinct physical wires or cables but via radio waves. Literally, the data is being broadcast beyond one's walls and property lines. The radio waves can be readily intercepted. Security articles talk of "wardriving", a technique where people drive through business areas with a laptop computer equipped with a wireless net card to finding open networks.[8] Although most residential areas might be low yield for wardriving, a neighbor with a wireless net card could gain access to your system.

The interception can bypass the protection of various firewalls. Protecting wireless networks requires tools to make the data hard to interpret if intercepted and to limit the ability of an interceptor to do much to one's system..

Practically Networked's Wireless Security Tips Web page <http://www.practicallynetworked.com/support/wireless_secure.htm> offers a good set of tips for protecting home or small business wireless networks. Among these tips are :

1) Don't use TCP/IP for file sharing among your Windows computers;
2) Limit sharing only to the extent really needed, share folders not entire drives, and use passwords for access control; and
3) Enable Wireless Encryption Protocol (WEP) if it's available.

Speaking of WEP, it is flawed encryption scheme but still better than not encrypting. All too often, WEP is not used, making wireless interception easy.

Finally: The Most Important Security & Privacy Tool: The Human Brain

"Doh!"
Homer Simpson

Often it is the stupid little things we do that can undermine security and privacy.

For example, the proclivity to open attachments without giving them some thought helps to spread various computer worms. How many people opened attachments that came with "I love you" emails without thinking?

---

[8] For an interesting glimpse of wardriving and the use of a snack food can as an antenna enhancer, see the BBC article "Hacking with a Pringles tube" at http://www.practicallynetworked.com/support/wireless_secure.htm.

Then there are hoax emails. Many of them warn people of non-existent computer viruses. There are nastier hoaxes which try to get the reader to do damaging things to their system. One hoax email claimed that a legitimate Windows program was a virus and explained how to delete it. Some legitimate helpful emails circulating online could be modified to give harmful advice. For example, one email tells people how to get a copy of their credit reports. Fine advice but if a crook modified the contact information, the reader might actually disclose sensitive financial information to identity thieves. It is smart to use independent source sources to check contact information before disclosing sensitive information.

Another example is the lack of critical thought when provides information online. Not everything should be posted online. Sometimes, people have posted rants to the Web that came back to haunt them later. The Web has a long memory.

The basic message here is to think before clicking or keying.