PC BANKING SECURITY Q&A

A *Ciphers By Ritter* Page

Nancy Day
Terry Ritter

A = ritter B = ciphersby
A@BA.com

2010 January 24

N: A friend of mine told me never to bank online. What do you think?
T: Banking online has become increasingly dangerous. But banks depend upon online services to reduce their costs. Your risk depends on which operating system (OS) you use, the browser you have, and how you use it.

N: I use a PC with the Microsoft Internet Explorer browser and Microsoft Security Essentials.
T: Sadly, I no longer believe that Microsoft Windows is secure enough for banking. For my own banking, I use Puppy Linux from DVD, the Firefox browser with security add-ons, and LastPass.com as a password manager. The problem with Windows is malware.

N: What is malware?
T: Malware is deliberately malicious software installed without permission of the computer owner. Malware usually comes from criminal hackers who will exploit their access to your computer however they can.

N: That sounds scary! So how do I know if my computer has malware?
T: There is no way to know for sure whether your computer has malware. Anti-virus and anti-malware packages can find some malware, but not all, and they probably miss the most dangerous kinds. Microsoft provides no tool to certify a Windows installation as clean.

N: What does dangerous malware do?
T: The worst examples become local robots or "bots" controlled by a remote "bot herder." Once in place, they can do anything you can do, and more. In particular, they can monitor your keyboard for account numbers and passwords and send them to a crime syndicate.

N: OK, I have heard enough! How do I prevent this?
T: First, avoid malware by using Linux for on-line browsing. Next, avoid infections and start each session clean by booting Puppy Linux from DVD. Then use the Firefox browser with security add-ons, and the LastPass password manager.

N: That sounds hard!
T: Not hard, just different! It does require you to get more involved.

N: I have heard of Linux, but what is Puppy?
T: Puppy Linux is a free operating system that most ordinary Windows users can use quickly. For best security, Puppy loads from DVD, then runs in memory and the DVD can be removed.

N: What about using some other Linux?
T: Any Linux is going to avoid malware far better than Microsoft Windows. However, most Linux distributions install on the hard drive just like Windows. The problem is that a hard drive is very easy to infect, and recovery involves re-installing the operating system. Even though Linux malware is relatively rare, it can occur, and if it infects the hard drive, we have a problem.

N: Is Puppy Linux the only one that runs from DVD?
A: Many distributions have a "Live" CD form which allows a user to check things out before installing to the hard drive. But most Linux distributions do expect to eventually run from a hard drive and thus do not confront some of the issues involved in long-term operation from DVD.

N: What is the problem with using an ordinary "Live" CD?
A: Browsers are frequently updated for security reasons and most "Live" CD forms do not handle weekly updates very well. Puppy seems unique among Linux versions in allowing new files, including security updates, to be automatically identified and burned to a new "session" (directory) on the existing boot DVD. The next time Puppy comes up, it loads the new files instead of the old ones. It is the ability to write security updates to the boot DVD which makes DVD operation practical and, currently, only Puppy Linux has it.

N: Do I have to get rid of Windows to use Puppy?
T: Not at all. Puppy loads from DVD and generally ignores Windows on the hard drive. And you will still need Windows for your software and hardware that runs only on Windows. Puppy Linux supports the Firefox browser and most Firefox add-ons, thus delivering a browsing experience similar to Firefox in Windows.

N: Firefox? I do not use Firefox!
T: The Firefox browser with security add-ons is an important part of the solution. Firefox gets patched quickly when problems are found and has an easy update system for itself and add-ons. No other browser has all the security features produced by these add-ons.

N: How do I get Firefox?
T: Firefox is free both for Windows and Puppy. For Windows, we go to mozilla.com and download the package for Windows. Install it, and you have a new browser! For Puppy Linux, there is a special .PET file organized to install Firefox. Then you should update Firefox. Then install various security add-ons from Tools / Add-ons / Get Add-ons in the browser.

N: So, are those security features like extra locks on your door?
T: Sometimes they are like warning you when your door is unlocked. Other times they are like keeping packages outside, when we know that every once in a while a package contains a bomb. Yet other times they show us whether we are sending something by postcard or secure courier.

N: That sounds great, tell me more!
T: Sometimes these security features can be annoying. But most people do not understand the level of risk generated by Internet technology. Hundreds of millions of PC's are online, and the Internet allows direct communication between any two computers anywhere in the world. We do not see this much on the Web, where we visit specific websites, but the capability is there for every criminal on the Web to directly touch your computer if they can get through. Firewalls prevent unrequested connections from outside, but can do nothing about connections the criminals can get you to request by trickery, either technological or psychological.

Criminals on the Web want to make a profit, and they prey on users to do it. The annoying security stuff is less of a problem than exposing your passwords and having your funds wired to another country.

N: I absolutely agree! Would these security features slow me down online?
T: In most cases you will not notice any computing slowdown. On some sites, the security systems may detect potential problems you will never see. On newly-visited sites, Flash and JavaScript will be stopped until you specifically approve them. Then you may have to think about it, which will take a few moments. But what do you want, fast, or secure?

N: Good point. But if Firefox is so good, why do I need Puppy Linux?
T: Firefox can only do so much. The single most important security improvement is to not use Microsoft Windows online. Modern hackers are out to make money, but their attacks hit users mostly at random. Over 90 percent of browsing is done from Windows computers, so most attacks are aimed at Windows. Even Flash and PDF attacks generally need Windows to run. By not using Windows, we get out of the line of fire.

N: Doesn't malware just stay online? And then what difference would it make using Windows or Puppy Linux?
T: Malware may come from online, but it invades your computer. Malware designed for Windows generally cannot work in Linux. For security, Puppy Linux boots from a hard-to-write DVD, while Windows boots from an easily-written hard drive. When malware starts working, one of the first things it does is to change the boot files on the hard drive. After that, the malware is always in charge.

N: So everything on my computer can be affected?
T: Yes. During a malware infection, you cannot trust anything on your computer. Any and all information on your hard drive is no longer private. You cannot even trust a directory window to show all the files which are actually there. And the malware will re-install itself on every new computing session until Windows itself is re-installed from CD.

N: How does Puppy Linux help?
T: For security, we boot Puppy Linux from DVD. Not only does Linux prevent most malware from running, a DVD boot starts clean on every session, avoiding any infection already on the hard drive.

N: How do I use Puppy Linux?
T: Puppy Linux is free. In Windows, we download the .ISO file to our hard drive. An .ISO is designed to make a bootable disk. We use DVD burning software to burn the .ISO to the DVD. We can boot from that DVD and Puppy will come up instead of Windows.

Some computers will need a one-time edit in their BIOS (Basic Input-Output Operating System), to make sure that the optical drive will be checked before the hard drive. Then the computer will boot from DVD if there is one, and from the hard drive otherwise.

N: Does my computer have a DVD burner?
T: Most recent computers do have DVD burners. It is possible to put Puppy on a CD, but that has much less storage for updates. It is important that you be able to update your Puppy boot disc, and doing that requires a burner, which is not an expensive upgrade.

Puppy can install itself on the hard drive, or on a USB flash drive, but these options are not good security. Even Linux can have malware, and it is easy for malware to take over the hard drive or a USB flash drive. In contrast, if malware tried to write to the DVD it would take much longer, should be apparent to the user, and can be prevented entirely by removing the DVD after Puppy has booted.

N: Does Puppy have frequent updates?
T: Linux is a free operating system, which means people work on it as a hobby or avocation. Typically, there has been a new version a few times a year to correct errors or provide some advance. Puppy is open-source software anyone can download to change or extend. Various modified versions become available as people make them. Linux has no formal "Patch Tuesday" for updates like Microsoft Windows.

N: I guess I get updates on line, so do I write them to the same old DVD?
T: The main update problem is the browser and add-ons, which Firefox handles beautifully. The main advantage of Puppy is to not be Windows, and that does not need updating. Occasionally, security flaws are found in the Linux kernal, and a new version is eventually included in a new Puppy. Probably the best way to update Puppy is to get another DVD, download and burn the new .ISO file (use Menu / Multimedia / Burniso2cd), then click on the "save" button on the Puppy desktop. Then your current environment will be saved to the new DVD along with the new Puppy system.

N: Once I start using Puppy and Firefox, can I use easier passwords?
T: You probably need *harder* passwords! Hard passwords are the way we protect our online accounts. We need to make and use a different long random password for every device and every site and every account. We cannot hope to remember these passwords, so we use a password manager, and LastPass.com seems like the best choice. All our passwords are collected and saved as an encrypted file that only we can decrypt and use.

N: Where do I get LastPass?
T: LastPass.com is a web site where we each establish an account. They have a remarkable range of free options to work with almost every modern browser and operating system, along with "one time" and "multifactor" authentications for use away from home. Probably easiest to use is the Firefox add-on, which is available from Mozilla just like other add-ons.

N: Will you tell me how LastPass works?
T: A little password database is encrypted locally, then saved as a local file (which is written to the DVD when a session update is saved), and uploaded to LastPass.com. Passwords are only decrypted locally, and then only when you supply your master password. Even the people at LastPass cannot expose the passwords. Since an encrypted copy is kept on the LastPass site, we can access our passwords from any secure computer, without carrying around the password file. And it is easy to add new sites from different computers (or different boot DVD's) without producing password files with different sets of passwords, which really can be confusing.

N: Can we use LastPass in Windows?
A: Yes and no. On the one hand we know that Microsoft Windows often is infected with password-sniffing malware, and on the other hand we have no way to certify that a particular Windows installation is clean. For security we are forced to assume the worst and ask whether it makes sense to do anything sensitive on a potentially infected computer. Normal LastPass fill-in-the-blanks operation may or may not defeat high-tech sniffing of account passwords. But nothing can protect the account numbers or other private information inside accounts after they have been unlocked.

N: If all my passwords are on my Puppy DVD, can someone get them if I lose my DVD?
T: No. Without your master password no one can expose your passwords. Do not forget your master password.

N: Could Puppy Linux be helpful in a family with kids online?
T: Definitely. Everyone can have their own DVD, which means the adults have their own clean OS unaffected by the kids. Even if the kids get Microsoft Windows infected with malware (and they will), the adults using Puppy Linux get a clean OS on every session, even on the infected computer.

N: Suppose I am on a business trip with my laptop, can I take Puppy?
T: Sure! The ideal solution is to take out the laptop hard drive, leave it at home, and put Puppy in the DVD drive. Now your private data cannot be lost and your hard drive cannot be infected. You can still browse as well as usual, and use your browser for email and banking.

N: Is that all Puppy Linux will let me do on a laptop?

T: Of course not. You can edit documents and spreadsheets online using Google docs or other sites. Various sites allow you to edit or develop graphics. You can save files as attachments in email to yourself. If you use Gmail, the email to yourself will be encrypted by SSL, thus protected from snooping in transit. (Email probably is fairly secure if it stays within Gmail, but not when sent through other providers or a website re-direct.) Or you can save files to various online backup sites, also through SSL. Some sites have games, and so on. Most things a Windows machine can do with a hard drive, Puppy can do without a hard drive.

N: Since Puppy Linux is so good, why don't I just quit using Windows altogether?
T: Now I have a question for you: Do you play games?

N: Yes. I have a suite of card games and a couple of others.
T: Remember, 90% of computer users operate under Microsoft Windows, so most games are programmed to run with Windows, not Puppy Linux. You may have an old Windows word processor you like, or a program for work which does not have a Puppy Linux version. Any special device you may have, like a scanner or fancy audio card, may not work under Puppy Linux. Anything especially new and different may not work under Puppy Linux, but it usually has Microsoft Windows support.

N: You mean there is no way to use Windows programs in Linux?
T: Well, not with good security. Linux does have a software package called "wine" that can be installed to run many simple Windows programs. But wine also makes Linux vulnerable to some Windows malware! For banking security use, wine must not be installed in Puppy! But one could have an "insecure" Puppy DVD with wine, not for browsing but for running such Windows programs as will run. In that case, Linux itself will cause most malware to fail, and the DVD is difficult to infect, so subsequent sessions should load clean, for a big advantage overall.

N: Will my bank be OK with Puppy Linux?
T: If you access your bank through a browser, Puppy Linux and Firefox should do fine, and LastPass can be programmed to sign you in.

N: Do I just go make myself a Puppy DVD and sign on to my bank?
T: Make yourself a Puppy Linux DVD. Add Firefox and update it. Add security add-ons, including LastPass. Configure to taste. Eventually you will need to create new long passwords for your banking and other sites. Then you will be much better off than you were, and more secure than almost anybody.

N: Thank you for answering my questions. What if I have more later?
T: It has been my pleasure! I have written several articles about PC security and Puppy Linux and the other programs we've discussed. Check my website. You should find answers to most of your questions in these articles:

- PC Security for Banking (47K)
- Basic PC Security (150K)
- Simplified PC Security (26K)