



April 2010

## Check out the new OUCH! Security Information Service at:

<http://www.sans.org/newsletters/ouch/updates/>

### In This Issue:

- **Safer Electronic Banking for Business Users**
- **Patches and Updates Roundup**

[Editor's Note: (Phil Hoffman): Businesses face an expanded set of challenges and threats when using online banking. Many of the consumer protection laws that safeguard individuals and limit their liabilities in the event of loss, theft and fraud simply don't apply to businesses and their bank accounts. In many cases, the only protection that a business has is defined by the bank's terms and conditions of use. That means your

business may be held responsible for any losses incurred prior to reporting suspicious activity to the bank. A chilling account of how quickly things can go wrong for a business has been reported by security expert Brian Krebs. <http://www.krebsonsecurity.com/2010/02/n-y-firm-faces-bankruptcy-from-164000-e-banking-loss/>

Last month we discussed one option for safer online banking that was recommended by the American Bankers Association: using a dedicated computer as your "banking computer." <http://www.sans.org/newsletters/ouch/issue/20100311.php>. This month we discuss two more options for creating an enhanced-security banking computer. These options require more technical know-how, and may be more suited for business users. We recommend discussing all three options with IT at the office or your computer support provider before you make a decision.]

## Safer Electronic Banking for Business Users

---

### Boot Linux from a CD

Many Linux distributions, such as Ubuntu, Knoppix and Fedora, can run entirely from a CD or a USB drive on an ordinary PC. Booting from a CD offers an important security advantage that a dedicated PC does not. Each boot represents a "clean start," so any unwanted or malicious changes made to the operating system or to applications are discarded as soon as the computer is turned off.

Some caveats. While Linux software itself is free and easy to implement, allow yourself time to learn the basics of a new operating system unless you are already familiar with it. Keep in mind that booting and rebooting from a CD can take longer than from a hard drive, and that you'll need to update your Linux CD frequently. Finally, check to make sure your bank's online transaction system will work with Firefox or whatever browser is included in the distribution of Linux you are thinking of using.

## **Boot Linux from a CD**

### **Pros**

- No additional software expense
- Little, if any, additional hardware required
- Linux is a smaller “target” for malware and hacking than Windows
- Automatically restarts from a “known good state”
- Updates easily; just download the newest distribution

### **Cons**

- You’ll have to learn the basics of a new operating system
- Your choice of browsers may be limited
- Loading Linux requires rebooting your computer
- Linux is updated frequently; you’ll need to update (re-burn) your Linux CD often

## **Use a virtual machine**

A virtual machine (VM) is like a computer within your computer. In essence, you’re running multiple computers which share the hardware resources of your single physical machine, all at the same time. The VM’s and the physical host can run different operating systems, and they generally behave as if they were separate PC’s connected by the same local area network.

You’ll need some extra memory and disk space to support it, but most systems purchased within the last few years should have enough of both. Many VM’s can be placed into a standby mode and “reawakened” rapidly. VM’s can be configured easily to reset to their initial “known good state,” so any malicious or unwanted changes made to the operating system or to applications are discarded. If you’re not sure you are up to creating a VM on your own, you can download a free virtual machine “player,” along with a preconfigured virtual “software appliance” for web browsing.

Some caveats. If you use Windows, for example, “inside” your VM, a license for that copy of Windows is required (MS doesn’t distinguish between “physical” and “virtual” installations). Just like a “real” Windows computer, a Windows VM needs regular patching and updating, and good-quality security software is a must.

## **Use a virtual machine**

### **Pros**

- Modest hardware expenses
- Can be configured to automatically restart from a “known good state”
- Faster starts than a normal reboot
- Can be used side-by-side with your “real” machine

### **Cons**

- May involve additional software expense
- Additional patching and updating is required
- Configuring the VM to restart from a “known good state” will remove recent patches and updates



**Caution!** Whether you choose to use a dedicated computer, the Linux-CD-boot solution or a Virtual Machine:

- Keep your banking computer's operating system and applications patched and updated.
- Install and maintain good-quality antivirus, anti-malware and a two-way software firewall.
- Do not use a banking computer for any purpose other than online banking.

### Tips!

- Monitor your bank account activity often. Most fraudulent activity is detected by the account holder first, not by the bank.
- Enable activity alerts. Many banks allow you to set up an automatic email that gets sent when a threshold, such as a specific dollar amount or a number of transactions, is exceeded.
- Disable features and services that you don't use. For example, if your business doesn't involve making international wire transfers, ask your bank to remove that capability from your account.
- Maintain proper division of duties and responsibilities. Email alerts and account statements should *not* be sent to the same person who enters the transactions.
- Know the terms and conditions of use associated with your bank account.
- Review your insurance coverage to determine what losses are covered and not covered.
- Use the advanced security features your bank provides such as requiring multiple approvals for transactions, one-time-use passwords, and anti-spoofing protection.
- If you suspect your bank account has been compromised or spot activity you have not authorized, contact your insurance company, and follow these guidelines from the Federal Trade Commission:
  - Notify your bank and credit card companies immediately
  - Close the affected account(s)
  - Notify the major credit reporting agencies
  - File a report with the Federal Trade Commission
  - File a report with the police.

### More Information:

- <http://blog.paradigmcc.com/2010/01/22/aba-recommends-dedicated-pc-for-online-banking/>
- [http://downloads.vmware.com/d/info/desktop\\_downloads/vmware\\_player/3\\_0](http://downloads.vmware.com/d/info/desktop_downloads/vmware_player/3_0)
- <http://www.vmware.com/appliances/directory/cat/0?k=browser>
- [http://en.wikipedia.org/wiki/List\\_of\\_antivirus\\_software](http://en.wikipedia.org/wiki/List_of_antivirus_software)

## Patches and Updates Roundup

### Operating Systems/Applications

Windows & PC Office: <http://update.microsoft.com> and <http://www.microsoft.com/security/updates/bulletins/201003.aspx>

Mac Office: <http://www.microsoft.com/mac/help.msp?CTT=PageView&clr=99-0-0&ep=7&target=ffe35357-8f25-4df8-a0a3-c258526c64ea1033>

OS X: <http://support.apple.com/kb/HT1338>

iPhone/iPod: <http://support.apple.com/kb/HT1414>

iPod: <http://support.apple.com/kb/HT1483>

Windows Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows>

OS X Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Macintosh>

Flash Player: <http://get.adobe.com/flashplayer/>

Firefox: <http://www.mozilla.com/en-US/firefox/update/>

Safari: [http://www.ehow.com/how\\_2033324\\_update-safari.html](http://www.ehow.com/how_2033324_update-safari.html)

Opera: <http://www.opera.com/>

Chrome: <http://googlechromeupdate.com/updates.html>

Java: <http://www.java.com/en/download/manual.jsp>

Windows iTunes: [http://www.ehow.com/how\\_2016273\\_update-itunes-pc.html](http://www.ehow.com/how_2016273_update-itunes-pc.html)

OSX iTunes: [http://www.ehow.com/how\\_2016270\\_update-itunes-mac.html](http://www.ehow.com/how_2016270_update-itunes-mac.html)

### **Security Suites**

Symantec: <http://service1.symantec.com/SUPPORT/sharedtech.nsf/docid/2002021908382713>

Norton:

[http://www.symantec.com/business/security\\_response/definitions/download/detail.jsp?gid=n95](http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=n95)

McAfee: [http://www.mcafee.com/apps/downloads/security\\_updates/dat.asp](http://www.mcafee.com/apps/downloads/security_updates/dat.asp)

Kaspersky: <http://www.kaspersky.com/avupdates>

Sophos: <https://secure.sophos.com/support/updates/>

Panda: <http://www.pandasecurity.com/homeusers/downloads/clients/>

BitDefender: <http://www.bitdefender.com/site/view/Desktop-Products-Updates.html>

Microsoft Security Essentials:

<http://www.microsoft.com/security/portal/Definitions/HowToMSE.aspx>

Copyright 2010, SANS Institute (<http://www.sans.org>)

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Alicia Beard, Alan Paller.

OUCH! Security Information Service: <http://www.sans.org/newsletters/ouch/updates/>

Email: [OUCH@sans.org](mailto:OUCH@sans.org)

Download the formatted version of the OUCH!: <https://www.sans.org/newsletters/ouch>

Permission is hereby granted for any person to redistribute this in whole or in part to any other persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product. We request that redistributions include attribution for the source of the material.