



March 2010

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

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

### In This Issue:

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

[Editor's Note: [Hoffman] Willie Sutton was a very famous 20<sup>th</sup> century bank robber. He is often credited with answering a newspaper reporter's question as to why he robbed banks by patiently explaining, "Because that's where the money is." The same goes for 21<sup>st</sup> century cybercriminals who write malware, send phishing emails and perpetrate online fraud. Your computer may not be where the money actually is, but for many of us, our

computers are an electronic gateway to our bank accounts and other financial services. If compromised, your computer can be used to transfer funds out of your account instantly and without your knowledge.

Any level of security costs more than no security, and secure systems may be less convenient to use than unsecured systems. It's like putting locks on your doors. Every now and then fishing for your keys will make you grumble. It's up to you to weigh the risks, the costs and the benefits. Your computer support provider can help you determine which solutions best meet your needs.

## Safer Electronic Banking for Home Users

---

### Dedicate a computer to online banking

The American Bankers Association recommends using a dedicated computer for online banking. Malicious software often gets into systems through activities such as web surfing or reading email – exactly what most of us do most of the time. Using a computer exclusively for online banking goes a long way toward increasing its security and reliability, and having a dedicated computer is more affordable than ever. Most electronic banking is done using a browser, and a \$500 (or less) low-end PC or netbook will work well for online banking. You could even use that old workstation or laptop that's been sitting in the garage.

### Dedicated computer

#### Pros

- Increased security and reliability through limited exposure to malicious software
- Fewer installed applications means less vulnerability

## Cons

- Increased hardware costs
- Increased software costs
- It's another system to patch and maintain
- Takes up space and uses power

## Get the kids their own computer

Many malicious online enticements target children. One of the simplest ways to increase the security of your computer is to keep your kids (and their friends) from using it. An easy way to do that is to get your children a computer of their own. You won't have to fight them for time on yours, and they'll love you for it.

## Kids' computer

### Pros

- Increased security and reliability through limited exposure to malicious software
- Opportunity to teach your children how to use the Internet safely and responsibly
- More access to your own computer
- Less whining

### Cons

- Increased hardware costs
- Increased software costs
- It's another system to patch and maintain
- Takes up space and uses power

## Tips!

- Keep your dedicated computer out of reach, or even better, under lock and key
- Set a strong password for the Administrator account
- Create a second account that has limited privileges and always use this account for your online banking
- Contact your computer support provider for information about how to add, remove and change user accounts
- Turn your dedicated computer off when not in use to help prevent network-based intrusions
- Keep the operating system secure by applying patches and updates promptly
- Don't scrimp on security software; install a good-quality security suite and keep it updated
- Never use a wireless connection for online banking
- Use a strong password for your online banking account, and do not use that password anywhere else (Strong password tips: <http://www.sans.org/newsletters/ouch/issue/20100219.php>)

## Heads Up!

If you suspect your bank account has been compromised or spot any activity you have not authorized, follow these guidelines from the Federal Trade Commission:

- Notify your bank and credit card companies immediately
- Close all affected accounts
- Notify the major credit reporting agencies
- File a report with the Federal Trade Commission
- File a report with the police

### More Information:

- <http://www.grc.com/sn/sn-231.htm>
- <http://blog.paradigmcc.com/2010/01/22/aba-recommends-dedicated-pc-for-online-banking/>
- [http://www.aba.com/ABAEF/CNC\\_contips\\_idtheft.htm](http://www.aba.com/ABAEF/CNC_contips_idtheft.htm)
- <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>

## Patches and Updates Roundup

Windows & PC Office: <http://update.microsoft.com> and <http://www.microsoft.com/security/updates/bulletins/201002.aspx>

Mac Office: <http://www.microsoft.com/mac/help.mspx?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)

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.