SANS OUCH!
SANS Institute Security Newsletter for Computer Users

June 2010

Get security advice you can use at:

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

In This Issue:

- Safer Online Shopping
- Patches and Updates Roundup

[Editor's Note: (Hoffman): This article focuses more on protecting you as opposed to your computer. One of the driving forces behind the rapid and widespread adoption of the Web was online shopping, or e-tailing. Today, just about anything that you can purchase or rent is available on the Web. Just as earlier generations were initially suspicious of mail-order purchasing, you should also apply a healthy dose of caution to online shopping and familiarize yourself with the rules of the road.]

Safer Online Shopping

The Basics

Keep your computer secure and protect your identity. Utilize good-quality anti-virus and anti-malware products, anti-phishing filters or a security suite, as well as hardware and software firewalls. Keep these tools and your browser up-to-date with the latest security patches. Never use unsecured networks (such as public wireless networks) or public computers for making online purchases. If the vendor requires you to create an account, use a strong and unique password.

Know your vendor

Almost all reputable vendors have registered domain names that match their company name, like http://www.<*companyname*>.com/. But make sure you spell it correctly, since subtly different misspellings are often snatched up by Web impostors seeking to lure you to bogus websites. Locate and type in website addresses directly, or use your own bookmarks.

When considering new vendors, do some homework. Are they accredited by the Better Business Bureau [1]? Do they comply with privacy policies from TRUSTe [2]? Be sure to click on accrediting logos to verify that they've not been lifted from another vendor's site, or are not just passive images--two sure signs of fraud.

Check what other people have to say about the vendor. Look for positive and negative comments from other consumers on sites dedicated to searching online retailing [3]. Get recommendations from friends and colleagues. Don't assume that prominent placement on a search engine's hit list means that the vendor is legitimate and trustworthy. The Bad Guys are skilled at manipulating the system to artificially

enhance the position of their websites on the results page.

Always use encrypted websites (shown in most browsers with an https address and a padlock icon) for sending a payment or personal information to the vendor. But don't assume that an encrypted website alone is sufficient evidence of a merchant's integrity. Encryption helps protect information in transit, but it doesn't say anything about a merchant's business practices. Legitimate-looking certificates can be obtained or created fraudulently.

Know your product

Be sure that the vendor is selling the current model and not last year's overstock. Is it new, used, returned, cosmetically defective, or refurbished? Pay careful attention to how the vendor uses a term like "refurbished." Ask what was wrong with the product and what's been done to make it right. Shop around to determine a reasonable price for the item; deals that are too good to be true often are. Make sure that you're buying a version of the product with a valid, local warranty. This is particularly true with cameras and electronics sold in the U.S. where there's an extensive "gray market."

Understand the true cost of your purchase

Determine the bottom-line price before committing to your purchase. If you can't calculate the total cost in advance, choose another merchant. The merchant's website should tell you if the product is in stock, give you a choice of shipping methods, and state when you will receive your purchases. Many people assume that buying online exempts them from paying sales tax – probably not. If your state has a sales *and use* tax, you are required by law to report purchases you make in other jurisdictions and pay sales tax on them voluntarily. Failure to do so could be regarded as tax evasion.

Select your payment method carefully

Avoid using personal checks, bank checks, money orders or debit cards for purchases, and NEVER send cash or cash equivalents. Credit cards provide some protections by law, and the issuer may provide others spelled out in the terms of service. If a vendor will not accept a credit card, find another vendor. The safest way to make a purchase, especially if you are dealing with a smaller vendor, is to use a third-party payment service, such as Paypal [4], AmazonPayments [5] or Google Payments [6]. These services act as middlemen so you don't have to give your credit card information to the vendor.

Fees for the payment services mentioned here are the responsibility of the seller, but that may not hold true for others. Prospective buyers should consult the details in the terms of service ("the fine print") and verify who pays for what before making a purchase. Reputable payment services provide information about their member merchants' standing, and whether or not complaints have been filed against them. Consider dedicating one credit card to making all of your online purchases. Monitor your credit card account activity frequently, and report unauthorized charges promptly. Using a prepaid credit card and a gift card can limit your losses if the card number is stolen or intercepted. Some card companies offer one-time use credit card numbers.

Good karma

Many people do research as part of their shopping in brick 'n mortar stores where they can examine products firsthand and ask questions of the sales staff, but then proceed to make their purchases from an online retailer at a lower price. If a salesperson or a company has been particularly helpful to you, consider

rewarding them with your business, even if it does cost you a bit more. Information adds value.

What to do if you're dissatisfied

Before you make your purchase, understand your rights with respect to returns, exchanges, refunds, and credits. These should be readily available on the merchant's website. Understand whether you can obtain support from the merchant, or if repairs and replacements are handled by the original manufacturer. Are there shipping and restocking charges associated with returning a product?

Problems with online purchases should be handled in the traditional way. Start by contacting the vendor or the manufacturer about it. If the issue remains unresolved to your satisfaction, contact your credit card company and file a dispute regarding the purchase. If things still aren't right, contact your local consumer protection authorities. If you feel you've been defrauded, file a complaint with the Federal Trade Commission and your local police department.

More Information:

[1] Better Business Bureau http://www.bbb.org/online/

[2] TRUSTe http://www.truste.com/

[3] Vendor ratings

- **BizRate http://www.bizrate.com/**
- **Epinions http://www99.epinions.com/**
- **PriceGrabber http://www.pricegrabber.com/**
- **Google Product Search http://www.google.com/products**

[4] PayPal https://www.paypal.com/

[5] Amazon Payments https://payments.amazon.com/sdui/sdui/home

[6] Google Payments https://checkout.google.com

Patches and Updates Roundup

Operating Systems/Applications

Windows & PC Office: http://update.microsoft.com and http://www.microsoft.com/security/updates/bulletins/201004.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

iPad: http://www.ehow.com/how_6256127_update-restore-apple-ipad.html

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

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

Chrome: http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95414

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

Windows iTunes: http://www.ehow.com/how_2016273_update-itunes-pc.html

OSX iTunes: http://www.ehow.com/how_2016270_update-itunesmac.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

McAfee: http://www.mcafee.com/apps/downloads/security_updates/dat.asp

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

AVG: http://free.avg.com/us-en/download-update

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

PC Tools: http://www.downloadatoz.com/pc-tools-internet-security/smart-update.html

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

Avast: http://www.avast.com/download-update

Webroot: http://support.webroot.com

Trend Micro: http://esupport.trendmicro.com/Pages/How-to-update-Trend-Micro-Internet-Security-Pro-2010.aspx

Microsoft Security Essentials:
http://www.microsoft.com/security/portal/Definitions/HowToMSE.aspx

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Alicia Beard, Alan Paller
Email: OUCH@sans.org
OUCH! Security Information Service: http://www.sans.org/newsletters/ouch/updates/
Download the formatted version of the OUCH!: https://www.sans.org/newsletters/ouch