

## January 2012 Newsletter

### Can You Spot the Phish?, and Steve Jobs was Right

Internet fraud is one of the biggest for-profit illegal activities, and much of it starts with a “phish” email or fraudulent website. Think you can spot a real website from a phish? Take the Quiz! Also, I explain my take on a controversial thing Steve Jobs did prior to release of the original iPad, and why he was right.

Missed or lost a newsletter? You can always get back issues in Adobe PDF format online at my website - [www.MedOfficeSystems.com/newsletter\\_tips.htm](http://www.MedOfficeSystems.com/newsletter_tips.htm)

---

### Can You Spot the Phish?

Phishing (fishing) is defined as an illegal activity whereby an email or website user is tricked into giving up personal or confidential details via a disguised or forged website similar to legitimate websites.

Typically there are two avenues where you will happen upon a phishing scam. The first is via the breathless email claiming that “your email account will be shut down if you do not act immediately” or “your credit card will be invalidated if you do not re-confirm the details”. The email may look like it came from your email service, bank, or credit card provider, and requests you to “click here...” The link takes to you what looks like a legitimate site, but it is not. If you fill in the data requested, you can be assured it will be used to steal your identity, credit card, bank account, or hijack your email for the purpose of sending spam.

The second avenue is by mis-typing a website address. There are scammers out there who have registered common misspellings of website names in order to create phishing websites. This is a common practice for those who wish to scam credit card companies, banks and other financial institutions.

So, how can you tell what is legitimate or not? One answer is to use your third-grade teacher’s admonitions to spell correctly. Another answer is to always closely examine the actual address in your web browsers address bar. If your browser’s address bar is not visible, you should enable it, the setting is typically found under “View, Toolbar, Address Bar” or “Tools, Toolbars, Address Bar” or similar. When you examine the address the important part is what is to the left of the “.com”, “.org” “.info” or “.net”.

For example ***www.BankOfAmerica.login.com*** is wrong, while ***www.bankofamerica.com/login/*** is correct.

OpenDNS, an excellent internet and website security provider, has created an entertaining quiz of actual phishing websites that have been discovered over the last few years. I took it and got 13 out of 14 correct. I am happy to say my one error was to ID a site as a phish when it was in fact real, so a little paranoia is good!

Take the Quiz: <http://www.opendns.com/phishing-quiz/>

## Steve Jobs was Right

When the Apple iPad was first released in January 2010, one thing was missing that confused, befuddled or angered Apple users, commentators, fans and critics: no Adobe Flash support in the browser.

I wasn't befuddled or angry, but I was very curious to say the least that Apple (actually Steve Jobs) put their foot down about including Flash support. Like Java and Javascript, a very large percent of websites use Adobe Flash to play almost any type of streaming media such as video, audio and even menu buttons. Some websites will not function properly or at all without Flash support. Flash became very popular as the original internet standards in 1993 did not include support for streaming media in any format (anyone remember text-only websites?). As a browser add-on or "plug-in", Flash made video and animations possible on websites as we know them today.

As it turns out, Steve Jobs was right to refuse. Besides his reasoning that Flash requires too much processor time, internet bandwidth, and battery energy on a mobile device, he also objected to Flash security weaknesses.

I can attest to the last part about security: Adobe Flash has become a security nightmare. Just in the last quarter of 2011, the number viruses related to Flash security gaps and infections exploded. I found and removed four computer viruses in one week that I traced back to Flash as the source of the infection.

How does it work? Basically, virus creators look for Flash security gaps in which they can insert their virus code. Then they plant the code in YouTube videos, free games, advertising, music sharing sites, etc. and then the fun begins. The "WinXP Security 2012" and "Windows AntiVirus 2012" viruses were distributed in this method. Because the virus uses security gaps and loopholes, your real anti-virus program cannot detect it, or when it does, it is too late.

The good news is that the use of Adobe Flash will decline quickly on mobile devices, as Adobe has halted future development on mobile platforms. On other platforms, Flash will diminish overall with the growing use of the newest web programming language, HTML-5. HTML-5 has built-in support for streaming media without the use of Flash or any browser plug-ins or add-ons. Building media support into the basic programming code, in place of browser add-ons, is ultimately the best and most secure method to distribute audio and video media.

So hats off to Steve Jobs, he may have taken some heat, but it was the right decision.

Happy New Year!

-John Becker