

Have You Been Phished, Skimmed or Dumped?

What CPAs and financial executives can do to avoid being defrauded by cyber criminals.

September 3, 2009

by *Sukanya Mitra*

How often have you received e-mails from legitimate companies such as Bank of America or JP Morgan Chase or PayPal, asking you to update your account information, only to see that mousing over their link does not link you directly to their Web site? And if you didn't mouse over and clicked and started updating your information as requested ... guess what, you were phished!

You're not the only one who has been scammed by these cyber criminals who are very creative and are experts at recreating Web sites that look like the real McCoy. Even the Internal Revenue Service (IRS) has been victim.

Chris Neighbors, assistant to the director of Office of Privacy, Information Protection and Data Security at the IRS, says that some of the most common methods of identity theft in cyberspace include skimming, phishing, dumpster diving and e-filing phishing sites. Dumpster diving, though not part of cybercrime, he noted was the easiest to keep in check. When you "dump" your old bills or unwanted credit card solicitations in your dumpster, anyone can plough into it and retrieve your bills and take up your identity. Imagine the fun shopping spree that person can go on having applied and received a new credit card in your name without your knowledge! Yes, it's that simple, and Neighbors strongly advises you shred every piece of mail you receive, no matter how frivolous it may seem.

Phishing

And what about the crimes that *are* cyber-related, such as phishing? "This is a huge problem. Not a day goes by that one of our staff doesn't e-mail the helpdesk with a copy of an e-mail received 'that appears to be legitimate' and asks 'What should I do'?", said James C. Bourke, CPA.CITP, partner at Red Bank, N.J.-based WithumSmith+Brown, PC. "From a CPA and financial exec perspective, the easiest solution is education. Educate your end users and customers about these types of fraudulent requests. Companies should NEVER send e-mail requests to their customers/clients asking them to update their personal information." Bourke strongly suggested instructing your customers and clients to not only never respond to such requests, but also having them forward such e-mails immediately to your company's attention, "no matter how legitimate the request may appear."

Skimming

Skimming is a growing cyber problem in which the scammer duplicates your credit card, debit card and can even do so with your driver's license. "This high-tech scam is done by swiping

your card into a device that records your card's information for later use. The *skimmer* — which is the name this device is called — can be bought online and is usually sold for under \$50," said Roman Perez, MCSA, MCT, CTT+, A+, VCP, an IT consultant for Queens, NY-based ITPro4me.

Perez said that there are two main types of machines used by skimmers. While one version is placed near a bank's ATM machine, the other type is used by dishonest store employees and is a "portable version" that is kept under store counters.

How are these transactions conducted? Often the scammers swipe your credit card information twice, said Perez, once for the actual transaction and the second time to record your information into the skimmer. While it is not always easy to keep a watchful eye on the person doing the swiping, especially at restaurants, Perez had the following additional suggestions:

- Always keep carbon copies of transactions, should manual credit card scanners be used;
- Keep low limits on credit cards you use for everyday purchases;
- Check to see if the front of the slot in which you place your credit/debit cards at ATMs look altered because that is where the skimmer is often placed;
- Cover your hand when entering PIN codes at ATM machines as "tiny cameras hidden inside a speaker shell are sometimes placed at ATMs to capture your PIN number while you type it in"; and
- Use common sense and be aware of your surroundings.

Virtual Surroundings

Time and again, we are reminded that plugging into virtual offices in hotels, airports and other business centers (at conferences) are not safe. What precautions can CPAs take to ensure that there are no security breaches in such situations?

"This is also a big problem. Connecting to such sites come with the risk of breach of customer/client private and confidential information that may be shared and accessed while connected to such points," said Bourke. He reminds financial execs to "NEVER-NEVER connect to 'free-WiFi' connection that may be floating looking for victims [because] every keystroke can be tracked and retained by these points for later attempts to commit fraud." Randy Johnston, M.C.S., M.C.P., executive vice president at K2 Enterprises, advised always using a broadband attachment and placing an IT policy of "no public access use." Agreeing that this policy may not be possible for all companies, he suggested, "consider SSL encryption, as well as two- or three-factor authentication."

Perez agreed with Johnston and also pointed out how important it was for users to not only have strong passwords that include capital and lowercased letters, numerals as well as special characters, *and* to change their passwords often. "When you are not using the Internet, disconnect the Ethernet cable and if on wireless, simply disable or turn off the wireless," said Perez. "When using a public PC, make sure that if asked to save your passwords by the system always click no, clear the browser cache when you are done and log out," pointed out Perez.

Behold, BlackBerry, Fuze, Surge Oh My ...

Most financial executives won't be caught dead without their BlackBerrys. Today's Smartphones make life easier and simpler and yes, you can get through many e-mails during that long one-hour commute. Hey, even the president can't live without his PDA. As Bourke remembers, "President Obama, like most of us, rely heavily on Smartphone access to communicate and quickly respond to the needs of our clients. The White House security staff was extremely concerned with the ability to not only electronically track the whereabouts of the president electronically (via the unique serial number known as an International Mobile Equipment Identity (IMEI) or Mobile Equipment Identifier (MEID) assigned to every phone), but also the ability to gather sensitive information that may be sent or received on such a device."

Yes, size matters and unfortunately as the size of PDAs keep getting smaller, it gets easier to lose or misplace them, and with that all your important documents. As with your laptops and PCs, Perez suggests thinking of your PDA the same way as you do your PC/laptop, making sure it has a 128-bit encryption. He also suggests synchronizing your workplace desktop/laptop with your PDA on a regular basis so you don't lose too much of your data. And finally, "use an antivirus program and keep it up-to-date with the most recent virus definitions, only download from reputable sites, and when your device is connected to your home or office network via your laptop or desktop, disable wireless," Perez said.

Bourke agreed completely and added the following suggestions:

- Don't connect your PDA to unknown WiFi connections;
- Don't retain more information that necessary on your device. In other words, after viewing e-mails, delete them;
- Don't use memory cards to store e-mails, e-mail attachments or other forms of confidential information. Such cards sometimes fall out of the scope of many protection programs when they are engaged to secure such devices;
- Remote wipe technologies should be in place allowing the organization to remotely remove all information and disable such devices regardless of type or location; and
- Report it to your IT group when a device is lost or stolen immediately, and such devices should be immediately remote wiped.

Last Thoughts

The name of the game is to be alert and make sure your company's employees are educated on how to use their devices — whether laptops, desktops or PDAs — properly, safely and cautiously.

Phishers and skimmers do not discriminate. And even if you are your company's president, you are more than a blip on their radar. "It is a good idea to establish a policy on the usage of these devices as part of your IT policy," advised Perez. "For example, what type of information can and cannot be stored in the device, what sites are allowed to download from, etc. The BES or Blackberry Enterprise Server from RIM for example, allows IT administrators to create security policies that can be enforced and pushed down to the Blackberry handheld devices."

It is better to be over-cautious, than be phished or skimmed. “Mobile devices are hot items for thieves of business-critical data,” quipped Perez, “so be mindful of your device and store it in a secure place.”

Rate this article 5 (excellent) to 1 (poor). Send your responses [here](#).

[Sukanya Mitra](#) is Managing Editor of the Insider™ e-newsletter group.

CUSTOMER SERVICE

- ▶ [Contact Us](#)
- ▶ [Order Tracking and History](#)
- ▶ [Access Online Subscriptions](#)
- ▶ [Forgot Password](#)

CORPORATE INFORMATION

- ▶ [About CPA2Biz, Inc.](#)
- ▶ [Advertising](#)
- ▶ [Visit AICPA.org](#)

GENERAL SITE INFORMATION

- ▶ [Site Map](#)
- ▶ [Terms & Conditions](#)
- ▶ [Privacy Policy](#)

**Current Published Version : 2301**

© 2001-2009 CPA2Biz, Inc. All Rights Reserved.

CPA2Biz and the CPA2Biz logo are trademarks and service marks of CPA2Biz, Inc.
100 Broadway 6th Floor, New York, NY 10005

All other trademarks are the property of their respective owners.

To place an order by phone or for other assistance, please call 1-888-777-7077.