

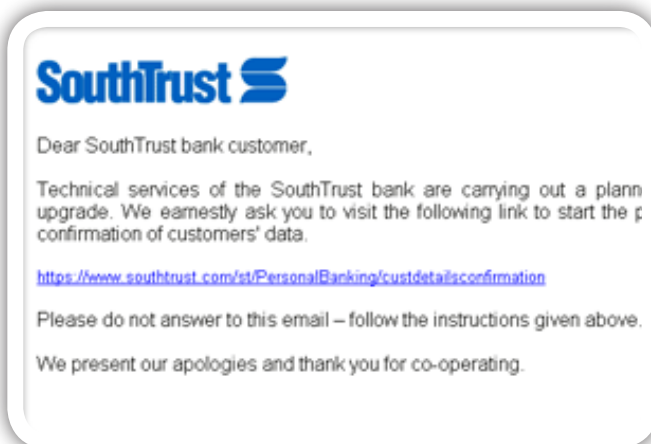
COMPUTER GEEKS
PRESENTS

tech-tips

Survive and thrive in a digital world

Going Phishing and Other Adventures in Internet Piracy: *A Guide to Avoiding Identity Theft and Financial Ruin*

Tech Tip 129 - Kimmy Powell



Surely you've encountered the "Dear Valued Customer", "Verify Your Account" or "If you don't respond within 48 hours, your account will be closed" emails flying across the screen, threatening corrective action unless you take the time to respond. Worse yet, what about those pesky pop-up windows that sporadically appear when you visit your bank's website, urging you to verify account details?

Welcome to the world of Internet piracy and [malware](#), where [phishing](#) for dollars nets more prize money for fraudsters than Bob Barker could ever give away in a single Showcase Showdown. Acting as legitimate business entities, phishers flood your inboxes with emails demanding personal information (i.e., your username, password, social security or driver's license numbers, banking or credit card numbers) in order to mollify some threat of dire financial consequence. They are responsible for the pop-up messages at

legitimate websites, or they can spoof these same legitimate websites, employing official logos (hijacked directly from official websites) and other company paraphernalia as integral parts of their scams. They deploy Trojan [keystroke loggers](#) and viruses to your PC in order to snatch what you type away from your fingertips. They may call by phone, using the same threats and tactics to collect tidbits about your life using "[social engineering](#)". In fact, hackers may even take advantage of backdoor security lapses in broadband routers to change [DNS](#) settings that re-route traffic to their own websites, executing malicious [JavaScript code](#) to mimic legitimate websites and hijack your router. Hackers then have access to any username or password combinations you enter as you surf the web.

Armed with your private information, phishers can wreak havoc on your financial well-being - applying for credit cards and loans, enjoying shopping sprees at Internet merchants, and draining bank accounts at the speed of light faster than you can say "identity theft." Just because something looks and sounds legitimate doesn't mean that it is, and you're not alone;

"It is important to stay vigilant and avoid becoming a victim of identity theft and the financial ruin that can ensue."

even the most Internet-savvy users face the dangers of identity theft if they're not careful.



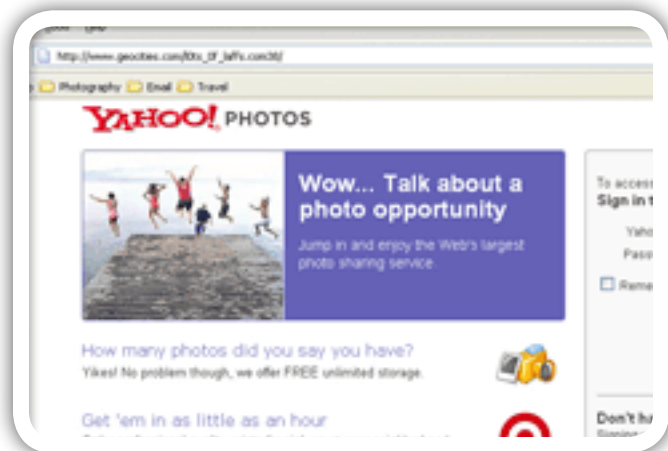
According to a [joint report](#) issued by the US Department of Homeland Security and the Anti-Phishing Working Group, online thievery is a billion dollar industry and growing in sophistication as technology advances. Between March and April 2007 alone, [Antiphishing.org](#) reported a substantial increase (55,643 in April compared to 20,871 in March) of unique phishing expeditions targeting email, social networking sites and voice-over-IP (VOIP) applications.

Protecting Yourself

The best protection against Internet piracy is not disclosing any information. If you don't know the person, don't say anything, and don't click on any links within an email message without first verifying the request with the legitimate entity the messenger purports to represent. A quick search for the company in [Google](#) or [Yahoo](#) will give you the relevant information. If the alleged entity is your bank or credit card institution, use the contact number listed on your statements. As a general rule, reputable companies will not collect personal information over the Internet because of lax security. If the emails are indeed spam, the government

encourages you to forward them to spam@uce.gov, reportphishing@antiphishing.org and to the company being impersonated.

Before entering usernames and passwords, verify that websites are secure by looking for the https:// in the URL and the logo of a closed yellow lock in the lower right corner of the browser window (or just to the right of to the URL field in IE7.) One caveat does hold, however: Hackers hover like hawks over new technologies, and they will resort to forgery of these same digital security measures in the pursuit of wealth. Online job seekers make themselves especially vulnerable to attack by leaving contact information and personal histories on bulletin boards. Always verify the validity of a source before uploading personal information.



Thwarting unauthorized access to your [desktop](#) or [notebook computer](#) should be a top priority as well as creating a barrier between you and the pirates. Use [antivirus](#), [firewall](#), and [anti-spyware software](#) on your system, and update these programs regularly. Internet Explorer and Firefox provide excellent tools to monitor fraudulent sites. [The phishing filter bundled in Internet Explorer 7](#) (located under the Tools menu) warns users of potentially threatening phishing sites by comparing the website against a confirmed list of suspect sites. [Firefox's anti-phishing](#)

feature functions in much the same way as the IE7 filter (access this feature by going to Tools → Options → Security). For an extra layer of protection, download Earthlink's free [Scamblocker](#) tool-bar add-on application, which also warns users of the security risks associated with a website. Finally, change the default password of your broadband [router](#) and/or [Wireless Access Point](#) (WAP), remove access to unnecessary services like FTP and Telnet on servers, and block unused ports to prevent tampering or scanning by hackers. If your wireless network hardware supports it, enable [WPA or WPA2](#) protection, even if you are currently using [WEP](#) which has been inadequate since 2003.

Careful and frequent review of your financial statements will alert you to any unauthorized charges against your accounts. Contact your bank or credit card company and alert them immediately to any suspicious activity. You are not liable for credit card charges you do not authorize. Remember - unless **you** initiate the contact, reject all requests for personal information.

Damage Control

If you suspect yourself to be a victim of identity theft, you can take the following measures to minimize damage to your financial reputation:

01. *Change your passwords. Select passwords that do not disclose identifying details and cannot be associated with you (e.g., your birthday.)*
02. *Contact your financial institution immediately, and close any accounts that have been tampered with.*
03. *If you've disclosed any personal identifying information, contact one of the three credit bureaus to determine whether a fraud alert should be placed.*

04. *Contact the [Social Security Administration](#) to report fraudulent activity.*

05. *Report thefts to the local police.*

06. *File a complaint with the Federal Trade Commission (www.ftc.org) and the FTC's Fraud and ID Theft Division (www.consumer.gov/idtheft).*

07. *If your bills do not arrive on time, receive denials of credit for any unknown reason or find purchases you did not make, call your financial institution immediately.*

Final Words

Internet piracy is very much alive and rearing its ugly head. It is important to stay vigilant and avoid becoming a victim of identity theft and the financial ruin that can ensue. Closing backdoor security lapses, avoiding unfamiliar emails altogether, and maintaining your security and antivirus software will aid in the fight against malicious hackers.