

Net scammers grow savvier in 'phishing' for private data

 Mail this page

E-mail messages trick users into offering info

By **CAROLINE LYNCH**
 clynch@courier-journal.com
 The Courier-Journal

Tina Hollar and Sherri Logsdon Cottongim make their living selling on eBay, so when they got an e-mail message last month saying that they needed to confirm their information or their account would be suspended, they were worried.

They clicked on the eBay link in the e-mail message and a familiar site came up.

"It looked exactly like eBay," Cottongim said. "You couldn't tell the difference."

But it wasn't eBay. It was a copycat site, made by "phishers," or people who send out fraudulent e-mail messages trying to trick users into giving them personal or financial information.

Security tips

The AntiPhishing Working Group offers some tips for how to avoid falling victim. For a full list, visit <http://www.antiphishing.org/>

- Be suspicious of any urgent request for personal or financial information. Phishers often ask for user names, passwords, credit-card or bank-account information or Social Security numbers, telling recipients, for example, that their accounts will be shut down in 24 hours if there's no response.
- Don't use the links in suspect e-mails to get to a Web page. Many of the scam e-mails include links that take the user to a page identical to the one they're pretending to represent. Try calling the company or typing in the Web address yourself.
- Don't fill out forms in e-mail messages that ask for personal or financial information. That info should always be put into a *secure* Web site or given over the phone or in person.

To report suspected fraud:

Phishing is one of the fastest growing Internet scams, targeting people worldwide and getting more professional with each new message. According to The AntiPhishing Working Group, an informal organization that includes computer security companies, banks and law-enforcement agencies, 1,125 phishing scams were reported in April. New phishing attacks doubled between March and April.

"It's growing fast because it works," said Dave Jevans, chairman of the antiphishing group. "It's more profitable than sending spam."

Though Hollar and Cottongim, who own Webay4you, did not fall for the trick — they got nervous when they typed gibberish into the blanks and then couldn't erase it — others do fall victim.

If the attackers dupe only a small percentage of the millions of recipients each scam e-mail message is sent to, they still get several thousand bank account numbers and other highly



Sales Marketing
 BOB MONTGOMERY
 CHEVROLET needs 4...

Engineering
 ARCHITECT A regional "Top 500"...

Other
 PROJECT MANAGER-
 Capable of...


Transportation
 DRIVERS Missing home?
 Looking for a...

Sales
 WANTED ENERGETIC,
 CAREER DRIVEN...

All Top Jobs

[About Top Jobs](#)

Subscribe!
 Click [here](#) to get the C-J delivered to your door each morning.




GET GROCERY COUPONS HERE!



[Click here](#)

to print coupons.

- Forward the e-mail to reportphishing@antiphishing.com, and the Federal Trade Commission at uce@ftc.gov and the Internet Fraud Complaint Center at www.ifccfbi.gov/.

- Contact the company that supposedly sent the e-mail.

- If you've entered your information somewhere and think you might have been scammed, also report the fraud to your bank and credit-card companies, and get credit reports from all three major credit reporting agencies: TransUnion (<http://www.transunion.com/> or 800-888-4213), Equifax (<http://www.equifax.com/> or 800-685-1111) and Experian (<http://www.experian.com/> or 888-397-3742).

— *The Courier-Journal*

valuable information.

Phishers steal information by pretending to be Internet service providers, banks or other companies. Through e-mail, they provide a link to a fraudulent Web site that looks exactly like the bank's or the company's site and then ask recipients to update or confirm bank account information, credit card numbers, Social Security numbers, passwords, etc.

Hollar and Cottongim forwarded the message to eBay, and were told it was a fraud and not to respond. eBay is investigating. Since then, they have received about 10 more e-mail messages that pretend to be eBay or PayPal, the online pay system eBay uses.

Tim Moore, technology director for Semonin Realtors, also reported a phishing attempt in April. He received an e-mail message that was supposedly from U.S. Bank, asking him to update his account.

But he has never worked with U.S. Bank.

He said, "All the stuff that would be normal security questions — it asked for every single one of them."

Moore, who had heard of phishing, forwarded the e-mail message to Tom Troutman, president of Louisville's Network Advocates, which hosts and protects networks for businesses.

Troutman said any e-mail message that asks for personal information is suspect. Users should not go to a link in a suspect message to contact the company. Instead, they should go to the site by opening a new browser window and typing in the address independently. He said new phishing tactics are still emerging and the scammers are getting more professional.

"As good as they are today," he said. "They're going to be better tomorrow."

^^ [Back to top](#)

[Home](#) · [News](#) · [Sports](#) · [Business](#) · [Features](#) · [Scene](#) · [Velocity](#) · [Classifieds](#) · [Jobs](#) · [Cars](#) · [Homes](#) · [Marketplace](#) · [Contact Us](#) · [Search](#)

Copyright 2006 The Courier-Journal.

Use of this site signifies your agreement to the [Terms of Service](#) (updated 12/18/2003).
Send questions and comments to [The Webmaster](#).