

## Slick eBay scam aims to steal your ID

By Bob Mims  
The Salt Lake Tribune

From its carefully duplicated eBay logo to subtle manipulation of the online auctioneer's Internet addresses, the message arriving in e-mail inboxes Wednesday looked genuine.

We at eBay are sorry to inform you that we are having problems with the billing information of your account, it reads, providing a link to a security update site. The message warns that if the requested data are not provided, the recipient's eBay membership is in peril.

A mouse click on the link pops up a page and a fill-in form. Along with eBay user identities, passwords and e-mail addresses, visitors are asked for their Social Security numbers, mail addresses, credit card numbers and personal identification numbers (PINs).

But this is no request from San Jose, Calif.-based eBay's accounts management office, as the message states. Rather, it is the latest of so-called e-mail spoof scams to plague not only eBay but numerous other companies -- AOL, BestBuy, Sony Electronics, UPS and Bank of America among them -- heavily engaged in Internet commerce.

If you provided the information, chances are your identity has been stolen, along with the information needed to make purchases on your credit, apply for additional counterfeit credit cards, passports, driver licenses and numerous other official documents.

Spokeswoman Jennifer Chu Caukin confirmed Wednesday that eBay is aware of the latest scam and is investigating.

We treat these e-mails very seriously because our aim is to protect the nearly 86 million global buyers and sellers in the eBay community from threats, regardless of where it happens and to whom, she said.

In the latest case, the e-mail's header contains the bogus SecretService@ebay.com sender address. To learn more about the real origins requires some digging. Members and nonmembers of eBay reported receiving the message, meaning the scam apparently used the shotgun approach to cyberfraud, mass e-mailing the message to thousands if not millions of accounts.

The hypertext eBay Billing Center link within the e-mail provides clues to its origins. The link's counterfeit security form traces it to an Internet service provider in Chonju, South Korea.

However, those investigating the scam could well be no closer to nailing the perpetrator: Such high-tech con artists often use stolen Internet access to bounce from one ISP to another, hiding their origins in multiple dead-end trails.

People have to be very careful with this stuff, said Polly Samuels, an assistant attorney general assigned to the Utah Cybercrime Task Force. Anytime you receive an e-mail asking for that kind of information -- Social Security numbers, PINs, credit cards -- it is almost always linked to some kind of identity theft.

Such messages have become so sophisticated in design that anyone might fall prey. They are easy to fall for, very official looking, Samuels said.

Just use common sense. Don't fill out those forms, especially when they are unsolicited. If you have questions, call the business involved.

It is advice Caukin heartily endorses. Indeed, eBay has so often had to deal with fraud that it provides users an address to forward suspect messages to: [spoof@ebay.com](mailto:spoof@ebay.com).

More information on fraud, how to prevent it and how to minimize damage if you become a victim, is provided at eBay's Security Center site, <http://pages.ebay.com/securitycenter>.

Among other suggestions, the site recommends always using a secure server -- indicated by the prefix <https://> in the Internet page address -- and never send private data via e-mail.

eBay will never ask you to send your account password or other sensitive personal information such as credit card numbers in an e-mail, Caukin said.

If you have already replied to a fraudulent e-mail with sensitive personal information or entered data through a fake Web page, contact your bank and/or credit card companies immediately to prevent identity theft, she added.

While unable to prevent such scams, eBay tries to react quickly to reports of fraud and prosecutes perpetrators.

In June, a Los Angeles man was sentenced to three years in prison for duping 170 eBay users out of \$600,000 for computer parts that were never delivered.

An even bigger case, though, is awaiting trial in Salt Lake City's U.S. District Court, where Russell Dana Smith, also known as John P. Leary, faces 54 counts of fraud for allegedly bilking hundreds of eBay bidders out of \$1 million for nonexistent laptops.