Research on Phishing Uses Tricky Technique

by Jonathan Sidener

It looks like you won the auction for the DVD player on eBay but haven't paid the seller yet. It says so right there on the e-mail with the official eBay logo. Of course, you didn't bid on a DVD player, so it must be some kind of misunderstanding. All you have to do is click on the link, sign in with your account name and password.

The vast majority of Internet users will recognize this and similar messages that purport to be from eBay, CitiBank or the Internal Revenue Service as phishing scams, attempts to trick you into revealing passwords and other personal information such as Social Security and credit card numbers.

Most people simply delete them. A few gullible souls respond and become victims of identity theft. And the parasitic phishers will repeat the cycle.

Phishing -- it gets its name and oh-so-clever spelling from the hacker culture -- has been around for years. But here's a new twist. A couple of guys sending out fake eBay e-mail have gone public. And it turns out that they're university researchers.

Two scholars from the Indiana University School of Informatics wanted to measure how many people respond to these scams, so they sent out about 1,000 phishing e-mails.

I'm sure these guys meant well, but my initial reaction was, "What a couple of jerks." Studying phishing by phishing seems to me to be a lot like studying fire suppression by pouring gasoline on a blaze.

Researchers Markus Jakobsson and Jacob Ratkiewicz went to great lengths to measure responses without giving themselves access to respondents' personal information. People who clicked on the fake phishing e-mail were actually sent to eBay, where they could answer a question posed in the e-mail. The researchers had their experiment approved by the school's Human Subjects Committee, which is supposed to ensure that no one is harmed by an experiment.

But imagine someone's grandmother receiving the researchers' fake e-mail. She clicks on a link that she shouldn't but ends up at eBay. Gullible Granny gets the message that it's OK to click on a link in an e-mail from a financial site. Isn't she more likely to click on the next phishing attempt that lands in her inbox?

Obviously they lack a cynical journalist on their Human Subjects Committee.

Despite these objections, you have to love the idea of fake phishing. If done right, it might jolt some sense into the small number of people who respond to these things.

It would be like an inoculation.

Here's my suggestion: In every family, every circle of friends, there's one or more person who's still forwarding the "good times" e-mail hoax or the "Bill Gates will pay you to forward this to everyone you know" e-mail or the latest chain letter.

It won't be hard to identify the gullible among us who need inoculation.

I think eBay and other frequently targeted Web sites should set up fake phishing services. Anyone could go to the site and type in the e-mail address of a suspected naive person.

The service would then send a fake phish to the target. If they click on the link, they could be directed to an educational site, where they could find a heartfelt message.

"Dear Granny, I love you very much and I was worried because the Internet can be a very dangerous place. Never, never, never click on this type of message."

More loutish offenders might require more direct language: "You dolt. Why did you click on that link? You just got phished, suckah."

Then, they could find tips on avoiding phishing scams, such as, "Never click on a link in an e-mail from a financial institution."

Another good tip is, "Never click on a link in an e-mail from a financial institution."

Then there's my favorite, "Never click on a link in an e-mail from a financial institution."

No doubt eBay will see the wisdom in my suggestion and launch such a service any day now. Until they do, it's up to everyone to identify the weak links among friends and family, and administer some tough love.

"Dear Granny: Remember the time you whacked me on the knuckles with a spatula when I tried to snatch a chocolate chip cookie? Don't ever click on the link in the e-mail from a financial institution. I know where you keep your spatulas. Get the picture?"

Copley News Service

Research on Phishing Uses Tricky Technique by Jonathan Sidener