MYMETRO.NET
Something *news* every day!

Metro

Home | CEO Hotline | Viewpoint | Classified Ads | Archives

Metro.net (web)

Resources

- Safety
- Pressroom (web)
- Ask the CEO
- CEO Forum
- Employee Recognition
- Employee Activities
- Metro Projects
- Facts at a Glance (web)
- Archives
- Events Calendar
- Research Center/ Library
- Metro Classifieds
- Bazaar

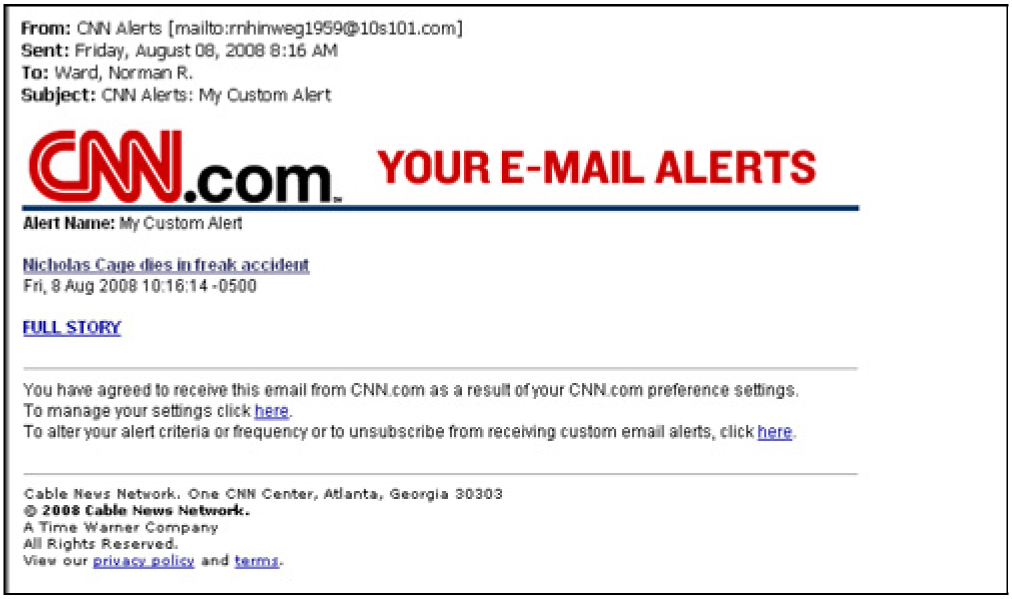
Metro Info

- 30/10 Initiative
- Policies
- Training
- Help Desk
- Intranet Policy

Need e-Help?

Call the Help Desk at 2-4357

Contact myMetro.net



From: CNN Alerts [mailto:rnhinweg1959@10s101.com]
Sent: Friday, August 08, 2008 8:16 AM
To: Ward, Norman R.
Subject: CNN Alerts: My Custom Alert

CNN.com YOUR E-MAIL ALERTS

Alert Name: My Custom Alert

Nicholas Cage dies in freak accident
Fri, 8 Aug 2008 10:16:14 -0500

FULL STORY

You have agreed to receive this email from CNN.com as a result of your CNN.com preference settings.
To manage your settings click here.
To alter your alert criteria or frequency or to unsubscribe from receiving custom email alerts, click here.

Cable News Network. One CNN Center, Atlanta, Georgia 30303
© 2008 Cable News Network.
A Time Warner Company
All Rights Reserved.
View our privacy policy and terms.

Besides the odd headline, the email address given for CNN does not look to be a CNN address.

Phishing Scams Target Your Assets and Confidential Information

By NED RACINE, Editor

- ". . . the most insidious Internet security problems today rely on human gullibility, not tricky software." --Walter S. Mossberg, Personal Technology, *The Wall Street Journal*

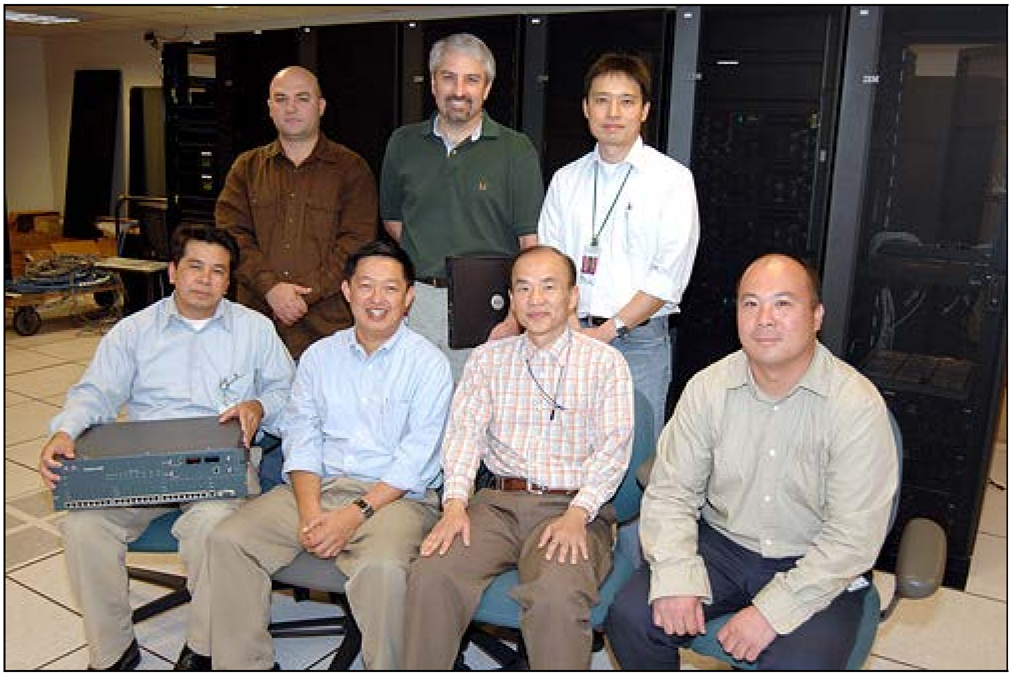
(Aug. 19, 2008) Every form of communication seems to be a double-edged sword: a greater ability to reach people comes with a loss of privacy; the ability to conduct transactions over the Internet comes with a new avenue for criminals to rob you.

"Phishing" (pronounced "fish-ing") is one such con game. Combining email and the Internet, phishing uses a variety of bogus identities to steal your assets, your confidential information or both. Phishing afflicts Windows and Mac users equally.

Phishing lures you into visiting an illegitimate website and pressures you to enter confidential information (passwords, Social Security numbers, etc.). That data makes its way to criminals around the world.

"People need to be more circumspect and less trusting," said Elizabeth Bennett, chief information officer. "If you've never given your email address to B of A, you have to question how they know how to send [an email] to you."

Even behind the defenses Information Technology Services (ITS) erects, some phishing emails break through—although much less frequently than with home email systems. In a continual game of cat-and-mouse, crooks develop new phishing emails and ITS software learns how to block them.

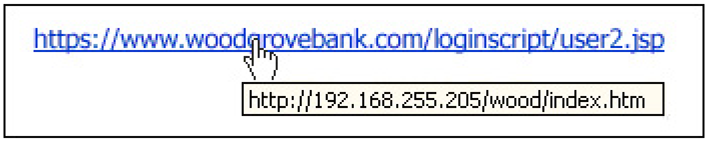


With network servers in the background, the phishing killers gather. They are, front row, from left, Vath Nquon, software engineer; Vincent Tee, director of System Architecture; Eddy Quach, system network administrator; Andy Liu, network administrator. Back row, from left, Ammar Jigani, network administrator; Richard Bezjian, manager of network administration; Ka Lok Liu, network administrator. *Photo by Ned Racine*

The number of bogus emails Metro receives is staggering. For a 14-day period from Aug. 2 to Aug. 15, ITS received an average of 5.8 million emails each day. The majority of these is filtered out, including over 2,000 containing a virus. After filtering the emails, 31,300 are distributed to Metro staff each day, meaning the great majority of emails are junk or dangerous.

“Of the total emails we get here at Metro, over 75 percent of it is filtered out and nobody sees it,” explained Bennett. “That’s how bad it is.”

Con artists rely on casting a wide net, hoping they will catch the naïve or gullible. They might send millions of bogus e-mail messages, apparently from trustworthy companies, counting on only a few email recipients to fall for their scam.



https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm

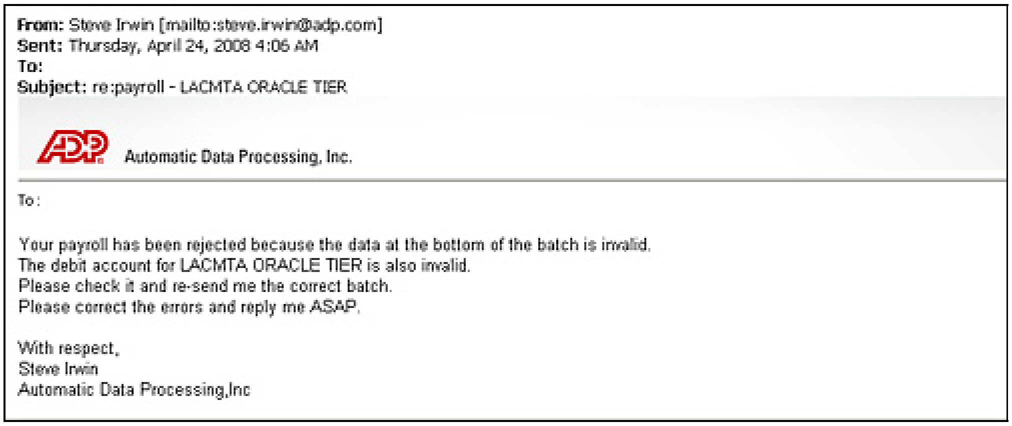
On its phishing website, Microsoft shows this example of discovering a web address’ real identity. By holding your mouse pointer over the link, a string of numbers appears, looking nothing like the supposed web address—a suspicious sign.

These fake websites are growing more sophisticated and may include the logos or other elements of a legitimate organization’s web site. A link sends the person to a seemingly legitimate web site. The goal is to reproduce the authority of a company people trust.

For emails from financial institutions, Bennett recommended Metro employees check the bottom of the email. Bogus emails provide little information there. “There is usually no person to call,” she said. “No bank representative name, title, anything.”

If you are unsure, check with your bank, Bennett advised. Many now post a warning when a new wave of phishing emails appear to inform their customers the bank did not send the emails.

How do these crooks acquire your email address in the first place? Bennett said that one way of collecting email addresses is through pop-up ads asking visitors to take a survey or advertisements of free offers. “If you don’t know where these online surveys come from, you’re taking a chance when you do it,” she said.



From: Steve Irwin [mailto:steve.irwin@adp.com]
Sent: Thursday, April 24, 2008 4:06 AM
To:
Subject: re:payroll - LACMTA ORACLE TIER

ADP Automatic Data Processing, Inc.

To :

Your payroll has been rejected because the data at the bottom of the batch is invalid.
The debit account for LACMTA ORACLE TIER is also invalid.
Please check it and re-send me the correct batch.
Please correct the errors and reply me ASAP.

With respect,
Steve Irwin
Automatic Data Processing,Inc

This phishing email was received by a few Metro employees in late April. Notice the poor grammar, often a tip-off that an email is phishing.

If you receive an email that seems suspicious, you can forward the email to the Help Desk mail box, Help Desk (ITS), call the Help Desk at 2-4357 or send the email to the Network Administration mail box at itsnetworkadministration. Bennett recommends that you then delete the email, so you do not accidentally click on it later.

She cautions Metro employees, both at work and at home, to beware of pop-up boxes that insist you need a new software to view a web site. “You could be introducing a virus,” Bennett emphasized. If you need an update at work, she asks Metro employees to call the Help Desk.

“These crooks play on your greed,” she said. “They prey on people’s vulnerabilities. That’s what they do. The real problem is when you get home, and there’s no one to protect you at home.”

Here are 8 tips to reduce your risk of falling victim to phishing:

- Remain skeptical. If that offer from the Nigerian lawyer appears too good to be true, it probably is.
- Don’t click on a link embedded in an email if it appears to come from a bank, stock market firm, PayPal or eBay. Even email addresses that look legitimate can be faked to hide a criminal’s real email address.
- If you visit a site that insists you need a new software to view something on the website, call the ITS Help Desk.
- Check the link to the apparently legitimate website. Instead of a link to *BankofAmerica.com*, the link might read *BanofAmerica.com*. You can do this by holding your mouse pointer (do not click) over the address.

- Ignore an email, even if it threatens dire consequences, if the email does not address you by name.
- Remember that institutions such as the Internal Revenue Service and courts only communicate through the mail, not email.
- Companies with which you have a relationship will not ask you for personal information (Social Security Number, passwords, login names) through email.
- Poor grammar or spelling in an email from a large company indicates a bogus email.

If you are interested in learning more defenses against phishing, Microsoft has a rich site at http://www.microsoft.com/protect/yourself/phishing/identify.mspx

| Home | Phone Directory | Forms Online | FIS Online