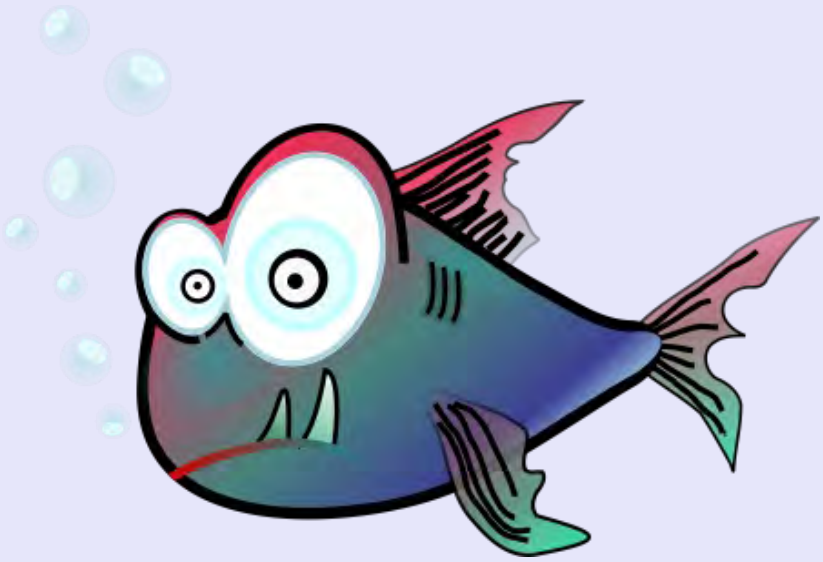
PC410: A Division of Science Translations
Managed IT Services, PC Service and Sales in Central Maryland

Security & PC News, April 2015

Do You Smell Something Phishy?

by Jerry Stern

Email is treacherous. What looks like a nice easy offer to help a Nigerian Prince to distribute an inheritance just about always turns out to be a scheme to launder stolen checks. Or worse. You just have to be suspicious of any email that's unsolicited and promises something that's too good to be true. But that's not all that's going on--these emails are teeming with phish. And they bite.



So what's a phish? A phish is a bulk email that looks like it's from a real company, one that you might already be doing business with, that's completely fake, and dangerous. There are several kinds, and you need to know what to look for. But first: The easiest way to avoid being tricked by a phish is to not click on any link in the email. If you need to visit your bank's site, type in the address, or click your bookmark for the site. Just don't click the email links.

An email arrives that looks like it comes from Bank of America. It looks real--every

logo is correct, but when you look at the links, they go to http://www.bankofamerica.com.*something-else.ru*. That's not Bank of America; it's mostly likely an attempt to send you to a look-a-like site that will ask you to log in, thus capturing your password, and then send you to an error page.

The end result--a phish can empty your bank account.

So how does the sender know you have an account of Bank of America? They don't--it's bulk, and they're sending similar messages to everyone, looking like any or all of the top 50 banks, on the assumption that someone will think it's really from their own bank.

A Verizon phish has been arriving recently, asking for readers to click the link and sign up for a new online account portal for a Verizon email account. There are multiple links, and all but one of them go to Verizon, but that last one goes somewhere completely different, and again, it's a password capture page with all the right logos, because it's a copy of the real thing.

The end result--the phish can send email in your name. In bulk, by the tens of thousands. And you will receive all the bouncing error messages.

A phish arrives, apparently with a court summons attached. Or it's an important pickup-receipt for a package. Or the IRS has sent a document. These are all 100% fake, and the attachments are dangerous--delete them. Courts, delivery companies, and the IRS never send attachments.

Spear Phish

While a phish is a generic bulk message to millions of people, looking like something genuine and important, a spear phish is a targeted email, sent in a personalized attempt to have a reader click into the links on the email, usually in order to capture a login for a specific government or corporate network. Ask your IT department if they're seeing spear phish showing up; they might have captured some specimens.

Finally: Your visits to banks and other sites should always be by typing in the address or visiting through your bookmarks and shortcuts, and never by clicking in an email or clicking a search result. Float the mouse over any link you're not sure of, and if it's not short and clearly going to the right site, don't click that link.

Could you be an Updates Mystic?

Yes, you too, can impress your friends by glancing at their screen and instantly telling them that they need to install updates. The secret is all in the system tray icons--that's the small icons near the clock. Read how:

How to be a Computer Mystic

Contact US

PC410.com is the local computer services division of Science Translations, serving central Maryland, including Baltimore and Westminster.
Call us at 410-871-2877, or from Baltimore, at 410-205-9250.
Was this email forwarded to you? Subscribe here!