Science Translations
Established 1990
PC410.COM™

Managed Services,
PC Consulting, Sales, & Service in Central Maryland

Phish Evolution

Back to Basics: a phish is an email that's 'fishing' for you to click a link or take an action that hooks you into a scam, either to take your cash or control your online accounts, or convert your computer into an online employee ('bot') of the phish-sender (the 'botnet herder').

And a 'spear phish' is a targeted phish, customized to just one recipient, frequently with scary amounts of inside knowledge, like the names of coworkers, where you bank, and so on. In-between, there's just a rough attempt to make the message look personal, usually by taking the domain from your email (yourbusiness.com) and using it throughout the email. It's rarely a true one-recipient spear phish, unless you are a public officer of a large corporation, or a 'target of value.' Some of the Democrats hacked during the last election were attacked using spear phish emails. For most of us, we'll just see phish with some mail-merge insertions of our email addresses in a few spots.

So, do you believe that the email shown below is real? Did I win the lottery?

facebook

Facebook INTERNATIONAL ANNUAL PROMOTIONAL DRAW 2012.

1543 Eglinton Avenue East, Suite 8444
Toronto, Ontario FM4P 1B5 Canada

Your email has won **USD 1,200,000.00 UNITE STATE DOLLARS**, from Facebook INTERNATIONAL EMAIL PROMOTION DRAW 2012, Ref: FB 7866MW, Batch No.Lotto 7/38.

Your e-mail address is one of 34 lucky addresses who have won in the monthly promotion, be aware that your prize will be paid from our paying bank in South Africa branch

Contact your claim agent in South African branch, Dr. Patrick Felix with following information.

1. Full Names:
2. Address:
3. Age:
4. Sex
5. E-Mail Address:
6. Telephone No:..., Batch No...., Ref No....
7. Country:
8. Occupation:
9. A copy of your valid identification or driver's license:

DR PATRICK FELIX
Payment Department, Ext 006.
Executive Vice President and Chief Information Officer & Claims Agent
TEL/FAX:+27 86 664 0668
EMAIL IS: patrickfelix2012@yahoo.co.jp

APPROVED

Yours Sincerely,
Mr. Arnold Charles (Sec.Zonal Co-coordinator).CONGRATULATIONS!!
GOOD NEWS

I hope there were only ‘no!’ answers for that. The "UNITE STATE" company mentioned, Facebook, is made to appear to have a Canadian address, a South African bank, and a FREE email address from Yahoo of Japan, and a phone number with a South Africa country code of 27. And they’re asking for enough information, with that driver’s license, to run a credit check or apply for a loan. So, clearly I did not win a lottery that I never entered in the first place.

So, if no one believes that phish, why is this one so convincing? It’s a new version, just showing up this month in very large numbers, somewhat shortened because the original

content is far too crude to include here:

Hello there,

Hope u do not mind my english sentence structure, because i'm from Germany. I contaminated your machine with a malware and im in possession of all of your personal data from your operating-system... (vague threats of web site history recordings here)

After some time additionally, it pulled out every one of your social contacts. If you ever would like me to remove your everything i currently have - transmit me 790 us in btc it's a cryptocurrency. Its my account transfer address - 141...

At this moment you will have 26 hours. to make up your mind Once i will receive the transaction i'll eliminate this video and every little thing thoroughly. Or else, please remember this evidence would be sent to your contacts.

Some of these show up with your own email address as the 'from' or 'reply-to' address. It's faked. Scammers who have your real email login information use it to send bulk mail, not ask for Bitcoin.

There have been a lot of these for the last two months, blackmail letters with Bitcoin payment demands and claims about webcams. Bitcoin is difficult to trace and impossible to call back. Delete these hoaxes. Some of them include real passwords-mine included a password for a video website I visited 6 years back, so I know that "learntoprogram.tv" was hacked and lost their user list.

I know that site was hacked because I gave it a unique password. No passwords used online should be used in more than one location, because once a site owner realizes that they've been hacked, they don't tell you. They just set the database for everybody to "lock out user until they request a 'forgot my password' reset link." But if they were hacked, that means that some hacker has your email address and a password that you have used, somewhere, at least once. So they'll start bulk attempts to use their new million-address database of stolen email and password pairs to log in at the top 50 banks, Amazon, the Apple Store, even some online games where you've built up a powerful character to take over. They'll attempt to log into anything with digital resale value or a cash equivalent. If they succeed, they can take over that account, and whatever it contains.

Again, don't re-use passwords. When they're hacked on one site, they're tested elsewhere and everywhere.

Phish Test

Now, you can take a test to see if you recognize a phish. Follow the link below for an 8-question phishing quiz, with explanations of each answer. It was created by Google's Project Jigsaw, formerly 'Google Ideas'; they describe themselves like this: "The team's mission is to use technology to tackle the toughest geopolitical challenges, from countering violent extremism to thwarting online censorship to mitigating the threats associated with digital attacks."

https://phishingquiz.withgoogle.com/

A hint: Security hoaxes usually have False Authority Syndrome. You MUST do this, it's from someone claimed to be an EXPERT, it's SCARY, and you need to take action NOW. It's also called the FUD factor, for spreading Fear, Uncertainty, and Doubt.

Contact

Address all editorial and unsubscr be requests to:
Jerry Stern, Editor, Science Translations, P.O. Box 1735, Westminster MD 21158