What is a phishing email?

Q: What is a phishing email?

On this page:

Answer
Examples of "phishy" MIT emails
Other phishing examples
If you've fallen for a Phishing scam, follow these steps

Answer

Almost everyone has gotten an email message disguised with the subject or message, "Your account has been suspended." or "We need to verify your password." These subject lines coupled with a spoofed (simulated) return address of e.g., Administrator@mit.edu, Admin@ebay.com, or AccountsDept@(your bank).com can confuse the untrained "fish." Further, the messages themselves often contain logos, and trademarks that add to the deception.

When trying to determine if email is authentic or not, remember one very important detail: no legitimate company will ever send you email requesting your username, password, or any other personally identifying information.

Things to look for to verify if the email is a phishing email:

- Spelling errors and bad grammar
- Odd formatting (e.g., incorrect use of capital letters or punctuation)
- No real person's name included either in the greeting or the signature
- A return or reply-to email address that is spoofed. You can view "full headers" to see what is listed as the actual return address.
- If a password is being requested, you know the email is not legitimate. No legitimate business will ever request your password. Look at what else is being requested as well (e.g., requesting your sex and country or territory is not a legitimate customer service request)
- No mention of a phone number to call or person to contact
- Deleting an account due to lack of response: a legitimate business doesn't follow that kind of practice
- Includes a hyperlink that has an odd looking URL (for instance with a foreign country as the domain, or trying to match a legitimate web address but spelled differently)

Examples of "phishy" MIT emails

Emails coming from such spoofed addresses as "support@mit.edu," or "webmail@mit.edu" are asking MIT community members to confirm their email accounts by supplying their username and password.

These messages are not coming from MIT
Although these messages may appear to be coming from MIT, they are in fact from an address that has either been hacked or simulated. MIT will never ask you to confirm or supply your passwords. These messages are an attempt to steal your username and password, or to install malware on your computer. Don't open attachments you aren't expecting, or click on any links in a "phishy" message - Report phishing messages to the IS&T Security Team

To see examples of some of the email messages that are attempting to steal your passwords or other personal information see:

- Examples of phishing emails that appear to come from MIT.

Other phishing examples

These examples show that the "reply-to" address in the email does not match the name or organization that appears in the "from" field or it is different from what you would expect. For example, an email from the IRS would come from an address that contains irs.gov, the official IRS online address. In the second example, the "from" field shows a different name from the one listed in the return address. This information can also be verified by looking at the email's full headers.
04/11/2013
Reference: 13H583326/13

Claim Your Tax Refund Online

Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to $319.05.

In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

From: MT Exchange (Monique Yeaton)  
To: PETER ROY  
Cc:  
Bcc:  
Subject: Re: where are you??

On 4/28/13 2:20 PM, "PETER ROY" <peterroy@arcor.de> wrote:

Hey, Monique. How are you doing? You must see this
http://edl.velente.si/bringdressedadmacdonald/

Best regards,
Peter Roy
If you've fallen for a Phishing scam, follow these steps

Change your email password immediately. Hackers have been known to hijack an email account within 30 minutes of receiving a username and password, and using that account to send out thousands of spam messages.