

Recognizing phishing e-mails

What is phishing?

Phishing is an attempt, usually via e-mail, to trick people into revealing sensitive information like usernames, passwords, and credit card data by pretending to be a bank or some other legitimate entity. The e-mails typically include a link to a Web site that appears to be legitimate and which prompts users to provide information. Sometimes, the phishing e-mail will include a form in an attachment to fill out. One common tactic phishers use is to pretend to be from the fraud department of a financial institution or online retailer like PayPal and ask for information to be provided to prevent identity fraud. In one case, a phishing e-mail reporting to be from a state lottery commission, asked recipients for their banking information so their "winnings" could be deposited into their accounts.

What should I look for in an e-mail?

Check the sender information to see if it looks legitimate. Criminals will choose addresses that are similar to the one they are faking. For instance, phishers have used "Alerts@Paypal.co.uk." However, legitimate PayPal messages in the U.S. come from Service@paypal.com" and include a key icon. Most phishing e-mails come from outside the U.S. so an address ending in ".uk" or something other than ".com" could indicate it's a phishing attempt.

The e-mail address may also be obscured. Hitting "reply all" may reveal the true e-mail address. You can also set your e-mail preferences to show "full header" to see the full e-mail address and other information. If you are at all unsure whether the e-mail is legitimate, go to the company's Web site to see the address listed. Legitimate companies tend to use customer names or user names in the e-mail, and banks often will include part of an account number. Phishing emails typically offer generic greetings, like "Dear PayPal customer."

Inspect the hyperlinks inside the body of the e-mail. Phishers typically will use sub domains, letters, or numbers before the company name and sometimes the words in the links are misspelled. Often, it's difficult to tell if the link is legitimate just by looking at it. By mousing over the link you can see the real address on the bottom of most Web browsers. In addition, PayPal, Amazon, banks, and many other businesses use the SSL (Secure Sockets Layer) protocol which is designed to ensure that customers are visiting the real site. That means https:// will be seen in the URL address bar instead of just http:// and usually there will be some other change in the address bar. For instance, PayPal displays a "P" and its name is highlighted in green at the front of the URL. The major browsers have antiphishing measures designed to detect malicious sites. Some phishers also try to hide the real Web address they are sending victims to by using URL shortening services. If the e-mail has an attachment, be wary of .exe files or text files. Scammers like to hide viruses and other malware there so it executes when opened.

Do not be fooled by the look of the Web site that you may be directed to. The Web site may look just like a real bank or PayPal page, including the use of the real logos and branding. It could be a good fake page or it could be a legitimate page with a phishing pop-up window on top.

```
-----Original Message-----
From: Facebook [mailto:notificationzj4oo4ta4c9@newparamejnetco.com]
Sent: Friday, November 06, 2009 2:52 PM
To: undisclosed-recipients
Subject: Caroline sent you a message on Facebook...

Caroline sent you a message.

(no subject)

Hello, have we met ever before??

Thanks,
The Facebook Team

To reply to this message, follow the link below:
http://facebook.montadalitihad.com/html-h1.htm
```

Figure 1: Above is an example of a possible phishing e-mail.