



## Don't be a victim of 'Phishing' Attacks:

**DO NOT** reply, **DO NOT** click on a link, and **DO NOT** follow the instructions in any email (or Instant Messenger) message requesting personal or sensitive information, regardless of how authentic the message appears.

### NEVER

include private, sensitive, or financial information in an email or IM message.

**USE** a spam filtering program such to filter your messages.

**REPORT** phishing messages to the FTC ([spam@uce.gov](mailto:spam@uce.gov)), and to the targeted company's fraud unit

Want to learn more? Here are some excellent Web resources on spoofing and phishing:

<http://www.antiphishing.org>

<http://pages.ebay.com/education/spoof/tutorial/>

<http://www.citi.com/domain/spoof/learn.htm>

[http://www.usbank.com/cgi\\_w/cfm/promo/personal/fraud\\_email\\_info\\_and\\_help.cfm](http://www.usbank.com/cgi_w/cfm/promo/personal/fraud_email_info_and_help.cfm)



**NOTE:** This is intended as a basic guide to illustrate some effective practices and/or tools available to computer users.

*Sinclair Community College does not endorse, or offer technical support for, any of the software or vendors listed in this document.*

Current as of March, 2005  
Daniel V. O'Callaghan, Jr., CISSP  
Chief Information Security Officer  
<http://www.sinclair.edu/departments/infosec/index.cfm>  
Sinclair Community College  
444 West Third Street  
Dayton, Ohio 45402



## Scammers are 'Phishing'

### Don't Take Their Bait

**Phishing** is a high-tech scam that uses spam to deceive people into disclosing credit card numbers, bank account information, passwords, Social Security numbers, and other kinds of personal information.

**Email and Internet users are reporting a significant escalation in the number and sophistication of these scams**



## Scammers are 'Phishing' Don't Take Their Bait

Phishing messages, most often sent via email (but also via instant messenger, and cell phones), fake (spoof) the appearance of popular auction, financial, merchant, and other company Web sites in an attempt to commit identity theft.

**These spoofed messages/sites are very convincing and often look exactly like the legitimate sites.**

Currently, the most prolific appear to be sent from companies such as **US Bank, eBay, Citi, Amazon, and PayPal**. There are many other accounts/companies targeted as well.

If you receive an email message requesting you verify personal, financial, password, or other information, **DO NOT** reply, **DO NOT** click on a link, and **DO NOT** follow the instructions in the message, regardless of how authentic the message appears.

What you *should* do is forward the message to the Federal Trade Commission ([spam@uce.gov](mailto:spam@uce.gov)), and to the targeted company's fraud unit (see next column), then delete the message.

**Email is NOT a secure protocol**, so you should **NEVER** send private or sensitive information using email. You should also **NOT** respond to any request for personal or sensitive information (reputable companies will not even ask.) If you are in doubt as to the legitimacy of a message, **never click on an email link**; instead, go directly to the home page of the company supposedly requesting the information and validate the request.

For example, if you have an account with eBay and receive a message instructing you to update your account information via a web link or email form, **it is a scam!**

If eBay really needed you to update your information, they would send you a message instructing you to go directly to the legitimate home page by typing [www.ebay.com](http://www.ebay.com) in the address bar of your browser, and then login to your account from the home page.

They would **NOT** include a link or form in the message itself.



This is currently one of the fastest growing Internet threats, and there is little that can be done *technically* to prevent this. However there are a few technical tools that will at least help you identify potential Phishing messages.

Using a spam filtering program such as **SpamAssassin** to filter your messages (<http://spamassassin.apache.org>) can help you identify these spoofed messages. If SpamAssassin identifies the message as spam, it is likely not legitimate.

Other tools include:

**TrustWatch Toolbar.** Allows user to verify a site is legitimately registered.  
<http://www.trustwatch.com/>

**Phish Net.** Uses a 'vault' and blacklist to protect sensitive information. .  
<http://www.webroot.com/products/phishnet>

.Addresses to report fraud targeting some of the major companies are:

eBay: [spoop@ebay.com](mailto:spoop@ebay.com)

US Bank: [fraud\\_help@usbank.com](mailto:fraud_help@usbank.com)

Citi: [emailspoop@citigroup.com](mailto:emailspoop@citigroup.com)

PayPal: [spoop@paypal.com](mailto:spoop@paypal.com)

Amazon: [stop-spoofing@amazon.com](mailto:stop-spoofing@amazon.com)

Current as of March, 2005

Daniel V. O'Callaghan, Jr., CISSP  
Chief Information Security Officer

<http://www.sinclair.edu/departments/infosec/index.cfm>  
Sinclair Community College  
444 West Third Street  
Dayton, Ohio 45402