

## Protecting yourself against Phishing

According to an August 17, 2005 Wall Street Journal Online article:

“In June 2004, more than 500 cadets at West Point received an email from Col. Robert Melville notifying them of a problem with their grade report and ordering them to click on a link to verify that the grades were correct. More than 80% of the students dutifully followed the instructions”.

The cadets were victims of Phishing, and West Point used the mock exercise to demonstrate its effectiveness in an effort to prevent future attacks on students. Training users in recognizing Phishing attempts is the best prevention against identity theft and fraud. Outlined below are the most common Phishing attacks, and ways to avoid falling victim to this widespread Internet deception.

### What is Phishing?

The best way to obtain another person’s password is by asking them. Though it sounds silly and obvious, it is the most widely used method to obtain sensitive information. Phishing has become the Internet’s equivalent of asking for a password, and computer users fall victims every year to phishing scams.

Phishing is defined in Wikipedia as the following:

“Phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication”

Phishing really means fishing for information: a bait is thrown out, and your username and password are the fish the thief is trying to catch.

### What does it look like?

Phishing will look like a legitimate email from a legitimate company such as PayPal, your bank, or the IRS. In the message, a scare technique might be used, such as “Your account will be terminated” but most often, the email will simply ask you to “verify” information by logging into your account. A link to log into your account will be provided in the email message. This link will go to a website that looks exactly like the legitimate site, and you probably won’t think twice about entering your username and password.

Phishing can also occur while you are logged into your account. The social network MySpace has been hit many times by this phishing method. In this technique, a pop-up window or a new screen appears, claiming that you have been logged out, and asking you to log back in to continue using your account.

### How to avoid Phishing?

#### 1. Don’t click that link!

If you receive an email from a financial institution, PayPal, e-Bay or the IRS claiming the need to verify your account, or using a scare technique such as “you owe back taxes”, take a deep breath, and **DO NOT** click on the link provided in the email message.

If you have legitimate concerns about your account, start a new browser window and type the company's website into the address bar of the browser to bypass the link provided by the email message. The IRS, PayPal or your bank will NEVER send emails with a link to your log-in account.

## **2. Don't log back in**

If it looks like you have been logged out of your account while working, **DO NOT** log back in immediately. Close your web browser completely, start a new web browser window, and go back to the site you were visiting by typing in the web address yourself in the address bar.

If you suspect Phishing activity, report the message to the company impersonated in the email.

To read more about Phishing on Wikipedia, go to:  
[http:// en.wikipedia.org](http://en.wikipedia.org) and search for "Phishing"