

Identifying Phishing Scams

A CyberAngels Quick Tutorial



Adapted from the US Computer Emergency Readiness Team

Phishing Scams

After completing this tutorial, you will be able to:

- Identify the main ways in which a phishing attack can affect you.
- Describe ways to tell a phishing attack from a legitimate website.
- Identify ways to avoid becoming the victim of a phishing attack.
- Explain what to do if you are the victim of a phishing attack.

What is Phishing?

Phishing is a type of online fraud in which a scam artist uses an e-mail or website to illicitly obtain confidential information.

Phishing scams frequently involve a copycat website designed to mimic that of a reputable company, often a bank or other financial institution, asking users to transmit sensitive data.

What is Phishing?

Phishing scams are often intricate, and scam artists are skilled in deceiving users.

However, there are a few simple steps that will ensure that your data is kept private and safe. This tutorial will show you how to minimize the risks of a phishing attack.

Phishing – What Scam Artists Want

A phishing attack is designed to obtain sensitive information. This can include financial data, social security numbers, home addresses, telephone numbers, medical information, and other private data you would not ordinarily share.

Information stolen by a phishing attack can be used as part of an identity fraud.

How Can You Identify a Phishing Attack?

If you received an e-mail reporting a problem with your account, first check the address from which the e-mail was sent, and the address of any link in the e-mail. If the address does not match the company's website, it is fraudulent.

Many phishing scams will employ a different domain – e.g. www.ebay.net (note the .net domain) or www.eebay.com (note the double E) instead of www.ebay.com, the real website.

How Can You Identify a Phishing Attack?

Legitimate companies do not ask for more information than they need, so be wary of any website asking you to reveal your Social Security number, bank account number, or other private information you do not ordinarily share.

If you receive an e-mail from a financial institution other than your own, it is likely a phishing attack, especially if it asks you for private information.

How Can You Identify a Phishing Attack?

If you are still unsure, try to contact the company directly by returning to the main page. Do not use the contact information from the e-mail or the website linked in the e-mail, as these may be spurious. Do not send private or financial information by e-mail.

What Can You Do?

Never send personal information via e-mail. A legitimate website will have a secure, encrypted form. An easy way to tell whether a website is secure is to look at the HTTP in the address bar. Secured sites will read https instead of http. For instance, the sign in page for eBay is <https://signin.ebay.com>, which tells you that your data is protected.

What Else Can You Do?

Most current anti-virus and firewall programs will help keep you safe from some attacks, but these should not be relied on as a primary measure.

Additionally, some browsers will warn you if you are being redirected to a potentially malicious website.

The Anti-Phishing Working Group maintains a list of known phishing attacks. Their website can be found at

http://www.antiphishing.org/phishing_archive.html.

Take the Phishing Attack Quiz

Phishing Quiz Question 1

What information can be stolen by a phishing attack?

- A) Financial data
- B) Addresses
- C) Passwords
- D) Social Security information
- E) All of the above

**The correct answer to Question 1 is
E) All of the above.**

Phishing Quiz Question 2

Which of the following is a common type of phishing attack?

- A) Logging in to your eBay account.
- B) An e-mail designed to mimic your bank's website.
- C) You check your bank balance on a secured website.
- D) You shop for clothes online.
- E) All of the above

**The correct answer for question 2 is
B) An e-mail designed to mimic your
bank's website.**

Phishing Quiz Question 3

If you suspect a phishing attack, you should:

- A) Send all of the personal information the e-mail asks for.
- B) Forward the e-mail to your friends.
- C) Report the e-mail to the appropriate organization.
- D) All of the above.

**The correct answer to Question 3 is
C) Report the e-mail to the
appropriate organization.**

Phishing Quiz Question 4

What should you do if you think your financial information may have been compromised?

- A) Contact your bank, credit company, or other financial institution.
- B) Closely watch any accounts that may be compromised for unusual activity.
- C) Report the attack to the police, FTC, or other organization.
- D) All of the above.

The correct answer to Question 4 is

D) All of the above.