

TIPS TIPS

DON'T BE FOOLED IF:

■ **You recognize the sender's email address or if the address seems trustworthy.**

An email address is NOT a good sign of whether the message is legitimate or not.

■ **The sender's email address includes numbers or a "domain" that looks like a personal email account.**

Often, if an official contacts you from your bank or other real company, the sender's email address will look something like "official@nameofbank.com." An official communication about your account will never be sent from a Hotmail, Yahoo, Gmail or other free, web-based email account. Again, real companies will never ask you to confirm your personal identification information directly through an email!

■ **You're addressed in the message correctly, either by name or as an account holder.**

The greeting may be intentionally general so you won't suspect a scam. For example, "Dear eBay Account Holder;" "Dear Chase Bank Account Holder;" "Dear Amazon Customer;" "Dear Western Union Member;" or "Dear Customer." Remember, an official email about your account will probably be sent to your direct attention, and will typically not include a generic greeting like these examples. But also, remember that just because a sender addresses you by your real name does NOT mean that they know you or that they are legitimate.

■ **A phone number is provided in the email message.**

Always be suspicious of a phone number in an email. For example, if the message appears from "BANK X," always check the Web site for "BANK X" for a phone number or look it up in the phone book. Don't rely on the number in the email because it could be fake.

■ **The sender urges you to click on a link and to enter personal information on the Web site the link takes you to.**

It could be a spoof Web site. Always verify the Web address, open a new Web browser and type the URL rather than clicking on a link.

LawHelp.org/NY

City Bar Justice Center
42 West 44th Street
New York, NY 10036



Internet Fraud: Crimes & Prevention

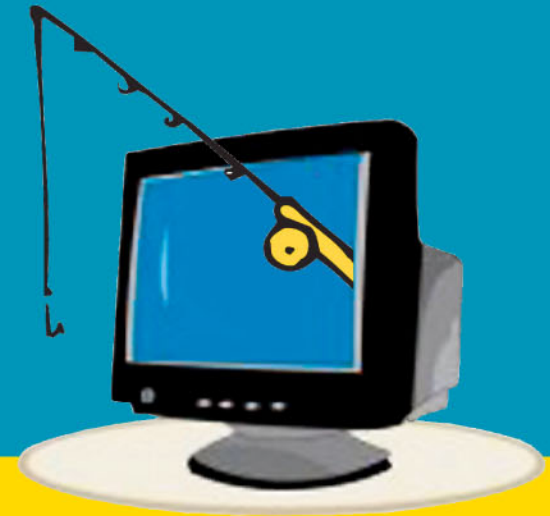
LawHelp.org/NY features:

- A mirror site in Spanish
- Instructional videos
- Resources in over 30 languages
- Over 500 legal service organizations and projects

www.LawHelp.org/NY
info@LawHelp.org

To develop the Internet Fraud: Crimes & Prevention topic area, LawHelp/NY received a Consumer Cyber-Awareness Grant of funds from a court-approved settlement of antitrust claims brought by the Office of the New York State Attorney General and the Federal Trade Commission. The views and statements expressed herein do not necessarily reflect the views and opinions of the Attorney General or the Federal Trade Commission.

Don't Get Caught! **BE AWARE OF PHISHING EMAILS**



Phishing (pronounced "fishing") happens when a criminal sends you an email that LOOKS like it comes from a real company or bank, with the company logo, colors, etc., and asks for your personal information.

THIS IS REALLY AN ATTEMPT TO LURE YOU into giving your personal information, which will be used to steal your identity and/or your money.

Phishing is an increasingly common problem. Each day, scammers create fake emails and "spoof" Web sites that look like the real thing.

LawHelp.org/NY

Helping low income New Yorkers solve legal problems

It could be a **PHISHING EMAIL** if it includes:

- **Extreme statements, or punctuation marks in the subject line or message.**
- **A threat describing something bad that may occur if you don't respond right away**, such as: "Important information is needed so we can deposit a check into your account," or "Your account is being deactivated unless you verify your account number and user name within the next 72 hours," or "Log in immediately using the link provided in this email or using the screen box below and take action or your account will be suspended."
- **A familiar logo from a bank** and says, "There was a third party breach on your account," or "Your account has been compromised. Please click on the link in this email and verify your account information on the next screen."
- **A claim that you're a customer of a bank** where you know you don't have an account.
- **A claim that the attachment in the email doesn't include a virus** (to fool you into opening it).

When you receive an unsolicited email request for personal information:

- **NEVER CLICK "REPLY"**
- **NEVER PROVIDE PERSONAL INFORMATION BY CLICKING ON A LINK WITHIN THE EMAIL**
- **NEVER ENTER PERSONAL INFORMATION IN FIELDS WITHIN THE EMAIL**
- **NEVER CLICK ON ATTACHMENTS WITHIN THE EMAIL**

Real banks and other real companies will never ask you to provide your full name, user name, password, account number, credit card number, driver's license number, Social Security number, PIN number or other personal identification information in an email! Many phishing emails include a clickable link to a "spoof" Web site that looks like an official Web site, but is actually a fake Web site criminals use to steal personal information, so don't click on the link. If you want to bank online or update your account information online, always open a new browser window and log onto the real company Web site to contact them directly.

Beware, attachments to phishing emails often contain spyware or viruses that can harm, or sometimes destroy, your computer's hard drive. Always find out exactly what a file is and whom it's from before you open or install it.

To report the phishing email and protect your computer:

STEP 1: Warn the company or bank named in the email about the scam being sent in their name.

Many banks and online merchants have departments that teach consumers about Internet fraud and inspect phishing emails. If you receive a "phishing" email, **DO NOT** make any changes to the email and **DO NOT** reply to an email address or phone number provided. From your inbox, click the "forward" button and send the email to the online security center at the bank or institution. After you alert the company or bank, you may receive a confirmation of receipt, and, almost 100% of the time, you will be told that the email you forwarded is fake.

STEP 2: Learn how to forward the phishing email with its header.

An email's header includes information that can be extremely helpful to track the origin of the email and may help authorities catch the criminal who sent the fake email. For directions on how to include the header data, visit this link from GetNetWise:

<http://spam.getnetwise.org/action/header>

STEP 3: Forward the phishing email to the Federal Trade Commission (FTC) at spam@uce.gov AND to your email provider. If possible, include the email header data as described above.

STEP 4: DELETE the email from your inbox.



**Internet Fraud:
Crimes & Prevention**