

# Protect Yourself from Identity Theft— Don't Get Hooked by 'Phishing' Scams

Sometimes the bait is the promise of money. Sometimes it's a threat to cancel your account. Most often it's a request to update your account information. But one thing is always the same: It's an innocent consumer – someone just like you – who gets hooked, reeled-in, and thumped with fraudulent charges.

The Internet is rife with thieves who aim to trick consumers into revealing personal financial information. They are committing an especially insidious type of Internet piracy –called “phishing.” Pronounced “fishing, ”the scams traditionally use e-mail to direct victims to phony Web sites. Once the victim enters personal information, their identity is stolen.

Recently, there's been a new twist in the phishing line. Scammers use deceitful e-mails to direct victims to call a customer support number where a voice response unit or individual awaits to gather your personal information. Typically, thieves are after passwords, Social Security numbers, credit and/or ATM card numbers and PINs and other confidential information. With this information they are able to take over accounts or even worse, assume their victim's identity.

Fortunately, there are some telltale signs of phishing. Most phishing emails warn of a serious problem that requires immediate attention. Look closely at phrases such as “Please contact us immediately” or “Immediate Attention Required.” Other techniques threaten account closure or suspension if recipients do not respond.

Look closely for those hallmarks if you suspect an email is a phishing expedition. Those same emails often encourage victims to click a link to a Web site or to contact a customer support number. In phishing scams, victims are usually redirected to phony Web sites that may look like the real thing. In some instances, victims are directed to the company's actual Web site – but watch out! Those are the cases in which a pop-up window quickly appears, enticing victims to enter their personal information.

## **PROTECT YOURSELF:**

- **Never provide your personal information** in response to an unsolicited request, whether over the phone or the Internet. If you did not initiate the communication, don't provide any information.
- **Never provide your password** over the phone or in response to an unsolicited Internet request. A financial institution would NEVER ask you to verify account information online.
- **Never click on the link** provided in an email you believe is fraudulent.

- **Do not be intimidated** by an email or caller who suggests dire consequences if you do not provide or verify financial information.
- **Go to the company's Web site** by typing in the site address directly. Or use a page you have previously bookmarked. Don't rely on links provided in a suspect email.
- **Before you call, research unfamiliar area codes** first using legitimate local phones companies to avoid long distance, international, or other toll charges.
- **Scrutinize your e-mail** for telltale signs of a phishing attempt;
  - Poor grammar
  - Typos
  - Strange Web site addresses (URLs)
  - Long Web site addresses (URLs)
  - Key Phrases such as: "verify your account", "Dear Valued Customer", "If you don't respond within 48 hours, your account will be closed", "Click on the link below to gain access to your account" and "Do not reply to this email".

If you are a victim of a Phishing attack, act immediately to protect your accounts and your identity. Alert your financial institution, place fraud alerts with the credit bureaus, and monitor your credit and bank account statements closely.

#### **Federal Trade Commission Identity Theft Resources**

Hotline: 877.IDTHEFT

Online: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

#### **Three Major Credit Bureaus**

Equifax: 800.5256285

Experian: 888.EXPERIAN

TransUnion: 800.680.7289