

How to avoid phishing scams and identity theft

Phishing scams represent a serious threat. This article describes tactics used by phishing scammers and strategies to avoid identity theft.

What is Phishing?

Phishing is an attempt to trick you into doing something you don't want to do. Phishing emails try to coerce you into giving away your most valuable information—bank account numbers, credit card numbers, passwords, social security number, even your mother's maiden name. The people behind phishing scams want all your personal info, and they're willing to go to great lengths to trick you into handing over your identity.

According to Webopedia.com, "phishing is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting."

Phishing Scams Lead to Identity Theft

Phishing scams often arrive as cleverly disguised emails. They may appear to be sent by trustworthy companies like eBay, PayPal, or your local bank or credit union.

Phishing emails may make threats like "Attention! Your PayPal account has been violated!" or "If you choose to ignore our request, we have no choice but to suspend your account." These matters seem urgent and unless you recognize the email as a phishing scam, you might fall victim to it.

Some phishing emails try to convince you that something good will come from your participation. A phishing email might say, "We are pleased to introduce our fully upgraded online banking. By clicking the link below, you will begin the process of updating your user details."

From Email to the Web

Clicking a link in a phishing email typically takes you to fake website. The phishing site is designed to look like a company's real website. The phishing site may even link to the official site and may use the same graphics, colors, and logos. This is all done to lull you into a false sense of security.

The phishing email and website are designed to get you to fill out their online web form. Once you've done that, the scam is complete.

An online web form used in a phishing scam asks for your personal info. They want anything you'll give them, including your bank account numbers, credit card numbers, social security number, passwords, etc. They might use your info to apply for new credit cards, run up bills on your existing cards, take out loans (never to be paid back), and anything else they can do.

How to Recognize Phishing Scams

How can you tell the difference between a phishing scam and a legitimate email or website? Unfortunately, phishing scams are becoming more and more sophisticated and increasingly difficult to identify. However, there are several strategies you can use to recognize phishing scams.

- **Be skeptical.** Since you *know* phishing scams are out there, be skeptical of emails you receive. Can your account really be violated? Do you really need to update your account information? Most companies don't wait until the last minute to spring emergencies like this on their customers. They send several notices, often times through the regular mail, or they call to warn you of potential security breaches. If you get emails like this, look for clues that they might be fakes.
- **Verify the web address and email address.** Checking the addresses is a good way of discovering a scam. If the *first part* of the web address consists of numbers, the site should probably not be trusted. For example, this is an untrustworthy address: <http://172.168.15.100/ebay/account/>. Even though "ebay" is part of the address, the first part contains numbers (called an IP address). This is a sign that something may not be right.
- **Look for signs of security.** Real corporate websites use secure, encrypted web pages any time their customers are asked to send personal and financial information. Look for "https://" in the web address. The "s" stands for "secure". Also look for a *locked* padlock icon in the lower part of your browser window. The locked padlock icon indicates the site is encrypted, which means your data is protected when you send it over the Internet. If you don't see these signs, then the site could be a fake.
- **Look for fishy details.** Most legitimate corporate emails and websites look professional. Phishing scams try to fool you, but like a photocopied dollar bill, they just don't look right. Look for bad grammar, bad spelling, and bad design. If your instincts tell you something's fishy, it probably is. Phishing scams are becoming more sophisticated each day, so this is not a sure-fire way of sniffing out a fake, but it's still a good place to start.
- **Make a few phone calls.** Before you click any links or fill out any forms, call the company—and don't use the phone number in the email. Get a real person on the phone to help you verify the legitimacy of the email you received.