

How to Spot a Phishing Scam

A recent study recognized three reasons why people still fall prey to phishing scams: lack of knowledge, visual deceptions, and inattention to detail.

They say the devil is in the details, and I'll show you why that's true in this case.

Security Signs

There are a few ways to recognize a secure connection between servers. You probably miss them every time you visit a secure web site. Because these indicators are so subtle, most of us still can't easily spot them.

Follow along with me here, by going to the [Yahoo! Mail](#) login page. Notice a few very important things here:

1) The URL of the page is https://login.yahoo.com/config/login_verify2. Notice the "s" at the end of "https." This "s" means the connection is over SSL (Secure Socket Layer), which means the page has established a secure connection and will encrypt all the information you enter on this page. You must always look for "https" on any site you use to enter sensitive information. This includes login pages, online shopping sites and bank web sites.

2) Notice the closed padlock on the lower right corner of the browser window. If you move your mouse over it, it will say "Signed by Equifax." If you click on it, it will open a window that gives you more details regarding the certificate. Every company that asks you for sensitive information must have a digital certificate, preferably one from an established certificate authority. VeriSign, Thawte, GeoTrust, and Entrust.net are just a few of these companies. Also keep in mind that the padlock must always be on the browser bar; any padlock within the content of the page doesn't mean a thing.

3) Yahoo! users have added security when they activate Yahoo!'s new [phishing feature](#). If you notice on the mail [login page](#), users can now add an extra layer of security using personalized sign-in seals such as their own secret message or image on their login page. Every computer they use to login to their Yahoo! accounts will display this seal, making it easier for them to recognize if they're on the real Yahoo! site or a fake one. Phishers be warned!

URL Madness

You can't judge a book by its cover, and in this case, you won't be able to tell if a web site is a fake just by looking at the web design. These smart criminals can replicate any web site down to the last detail, and it wouldn't surprise me if they used the same web designer to do it. Consumers have lost \$630 million to email scams in the last two years, according to *Consumer Reports'* State of the Net. Phishing is a big business, so never think for a second that these criminals wouldn't spend thousands of dollars creating sites as credible as the real thing. Sometimes their designs feel so authentic; they even link to the real web site to boost your confidence. This is where it gets tricky, and you must watch out for illegitimate domain names.

Here's what you should look for:

- a) Misspelled domains are big deceivers. Phishers will purchase a domain name that resembles the real domain. They will replace letters with numbers or with other letters. Pay close attention to the spelling of a domain names, and learn to spot a fake like www.yohoo.com or www.paypol.com.
- b) Variations of domains should also be a red flag. Don't click on any email that contains URLs like <http://center.yahoo-security.net>. A legitimate URL should read <http://center.yahoo.com> if it actually belongs to Yahoo! Anyone could've purchased www.yahoo-security.net for a scam (I'm just using Yahoo! as an example here).
- c) An IP address looks something like 102.199.60.250. Bottom line, **never** trust emails that point you to URLs that only show an IP address.

Other Tips

- 1) Never test web sites to see if they're legitimate or not. This means entering passwords or personal information. These sites may install malicious software—known as keylogger software—that records everything you type, then sends that information to scammers.
- 2) Stay abreast of the latest scams: The [FBI's web site](#) has a list of all the latest scams reported, so check it periodically.
- 3) If you're being urged to "verify" sensitive account information, contact the company directly instead. Always type the web site's address in the address bar instead of clicking links on suspicious emails.
- 4) [PayPal](#) never uses generic greetings in their emails. Next time you get an email from PayPal, check the salutation, as PayPal will usually use your member name.
- 5) Emails from banks and credit card companies will usually include partial account numbers. Therefore, one should always be suspicious if the message does not contain specific personal information.