

IGNORE THE BAIT

DON'T GET HOOKED BY PHISHING SCAMS

Smart Computing, February 2005

RULE #1: Pay Attention to URLs

URLs (uniform resource locators) are the characters you enter in a browser's address bar to visit a particular site, and a favorite trick among phishing scammers is to make users think they are going to one URL when they really are visiting another URL.

RULE #2: Watch the Padlock

All popular browsers display padlock icons when users visit secure sites; these icons are generally in the lower-right corner of the browser window. When users visit secure sites, or secure portions of sites after they've logged in, the padlock icon appears and the URL in the address bar begins with "https:" instead of the usual "http:" we see. Knowing this, if you ever see "https:" in the address bar but don't see a padlock icon displayed, the page isn't secure and it's likely you're visiting a phishing site, so don't fill anything out or click any links.

RULE # 3: Type, Don't Click

The Internet has conditioned us to click hyperlinks to open new pages, but don't let that habit get the best of you when a seemingly urgent email arrives. One of the main techniques phishing scammers use to lull users into a false sense of security is to put links in an email that look like they point to a legit company site when they actually point to a phishing site. This is called link masking, and it's easy to spot and avoid if you know what to look for.

RULE #4: Notice Login Inconsistencies

Some scammers cover their tracks by sending victims to the legitimate company sites after collecting personal information. Common examples of this are phishing sites that ask users to enter user-names and passwords they would use to log in at legitimate sites, and then automatically connect users to those sites after collecting their valuable login information.

If you ever attempt to log in to a legitimate account after following a hyperlink in an email, and the Web site rejects your login information even though you typed it correctly, it's likely you've just been scammed. Contact the legitimate company that the phishing scammer pretended to represent to let it know what happened and change your login password immediately.

RULE #5: Protect Bank Account Data at All Costs

It's bad when scammers gain access to your credit card accounts, but at least these accounts are protected to the point where victims are liable for only a maximum of \$50. Debit card and bank accounts often don't have this level of protection, so never divulge bank account information in response to an email.

RULE #6: Keep Personal Info Personal

If you take nothing else away from this article, remember this: Legitimate companies never should ask for personal info via email (and if they do, they're not worth doing business with anyway). Never fill out a form via an email, and never blindly follow links embedded in emails—no matter how official they appear to be. Scammers rely on input from you to do their work, so by trusting your instincts and never responding to emails that ask for personal information, you can force these jerks to find real jobs and earn their own money.