

Anti-Phishing Guide

Can you tell a legitimate e-mail from a phishing e-mail?

Take the **SonicWall Phishing IQ Test** at <http://www.sonicwall.com/phishing> to find out. If you don't score 100% finish reading this page and try again.

Phishing is an attempt by criminals, typically done by e-mail, to steal your personal information. Learning to recognize a phishing e-mail is the best way to protect yourself and your identity.

Phishing emails nearly always appear to come from a well-known organization. In addition, they ask for your personal information like a credit card number, social security number, account number or password or user name. Very often these attempts come from websites or companies where you don't even have an account.

For these criminals to be successful, they must get you to click a link. Phishing emails nearly always ask you to click a link that takes you to a website where you can enter your personal information. Legitimate organizations **do not** ask for this information by email.

What to look for in a phishing email

- 1) Generic greeting.** Criminals send out large numbers of phishing emails at a time. They usually use a generic greeting like "First Generic Bank Customer" since they don't actually know if you have an account at First Generic Bank. If the e-mail doesn't contain **your name**, be suspicious.
- 2) Forged link.** Even if the e-mail contains the name of a bank, company or organization you recognize, it probably doesn't contain a link to the real organization. Roll your mouse over the link they want you to click on to see if it matches the email. If there is a discrepancy, don't click on the link.
- 3) Non-secure website.** Any website where it's safe to enter your personal information should begin with "https" — the "s" means the server is secure. Don't go any further if you don't see "https."
- 4) Requests for personal information.** **ANY** e-mail requesting personal information is probably a phishing email. The bad guys make a living by tricking people into providing their personal information. If you receive an email request for any personal information, assume it's a phishing attempt.
- 5) Sense of urgency.** The bad guys want your personal information **NOW**. Part of the trick is to make you believe that you must act fast. The faster they can get you to respond, the faster they can move on to another victim.

What you should, and shouldn't do...

1) Never follow any link in an e-mail you're uncertain about. Rather than clicking the link in the e-mail, type the address of the page in your browser manually and log in through the official site.

2) Never send any personal information through e-mail. If the e-mail says your account is invalid or suspended, visit the website as directed above and log into the account normally.

3) Contact the company directly if you're still not sure about the e-mail. Use an e-mail address or phone number provided on the official website. Never trust the information in the e-mail.

For even more good information, visit the website of the **Anti-Phishing Working Group** at <http://www.antiphishing.org/>