



Security Advisory

Security Advisory – Advice on how to avoid phishing scams

We're all comfortable using email to conduct personal and professional transactions. Spam is an irritating reality. But now there are sophisticated confidence schemes using email. And if you don't pay attention you could be ensnared. Probably the most devious of all email scams are "phishing" exploits.

What is Phishing?

Creators of phishing attacks start by creating fly-by-night websites aimed at luring you into divulging sensitive data. The goal is to capture usernames, passwords, credit card numbers and social security numbers and more. Once these web sites are up and running the scammers entice you to visit these sites by sending email messages. Phishing messages are pretty convincing-- if you go by appearance alone. They incorporate appropriate corporate logos, slogans and design schemes. So they look like the real thing. (And in most of these messages, the sender's address has been spoofed to appear as if it has been sent by a legitimate organization.)

Somewhere in each phishing message you are encouraged to click on a link. If a URL is visible for that link it appears to be a legitimate web site. To lure you there, the scammer dangles bait. These messages create a sense of urgency -- the email claims you have an account problem that will result in cancellation or warns that you're a victim of a fraud threat. There may even be an implied deadline.

Be Suspicious! Forward any suspicious emails to:

support@payrollcompany.biz

- ❖ If you received a suspicious email that appears to be from the Payroll Company, please forward this email to: **support@payrollcompany.biz**
- ❖ If you receive a suspicious email requesting sensitive corporate information, please forward this email to: **support@payrollcompany.biz**.

Anti-Phishing Work Group-Consumer Advice (www.antiphishing.org)

The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While online banking and e-commerce is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. The Anti-Phishing Working Group has compiled a list of recommendations below that you can use to avoid becoming a victim of these scams.

- Be suspicious of any email with urgent requests for personal financial information
 - unless the email is digitally signed, you can't be sure it wasn't forged or 'spoofed'
 - phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
 - they typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.
 - phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are
- Don't use the links in an email to get to any web page, if you suspect the message might not be authentic
 - instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser
- Avoid filling out forms in email messages that ask for personal financial information
 - you should only communicate information such as credit card numbers or account information via a secure website or the telephone
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
 - to make sure you're on a secure Web server, check the beginning of the Web address in your browser's address bar - it should be "https://" rather than just "http://"
- Regularly log into your online accounts
 - don't leave it for as long as a month before you check each account
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate
 - if anything is suspicious, contact your bank and all card issuers
- Ensure that your browser is up to date and security patches applied
 - in particular, people who use the Microsoft Internet Explorer browser should immediately go to the Microsoft Security home page -- <http://www.microsoft.com/security/> -- to download a special patch relating to certain phishing schemes
- Always report "phishing" or "spoofed" e-mails to the following groups:
 - forward the email to reportphishing@antiphishing.com
 - forward the email to the Federal Trade Commission at spam@uce.gov

- forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
- when forwarding spoofed messages, always include the entire original email with its original header information intact
- notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/

For more information, check some of the following sources:

For more information about how to protect yourself, see our Fact Sheet 17a Identity Theft: What to do if It Happens to You at <http://www.privacyrights.org/fs/fs17a.htm>. Read the information and tips put out by the Federal Trade Commission about phishing at <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>. Read the Department of Justice's recent whitepaper "Special Report on Phishing" at http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf

Typical Components of a Phishing Message:

- ❖ The "From" address in the email header appears to be coming from a reputable source.
- ❖ The message includes an official-looking logo.
- ❖ The link appears to have a URL in a legitimate domain.

❖ The message contains material taken from the legitimate website



Other Tip Offs

Check the URL when a message asks you to click on a link.

- ❖ Many fishing messages use an IP address rather than a domain as the destination. Legitimate organizations don't use an IP address as a public URL.
- ❖ Some scammers register misleading domain names. They use tricks like character replacement (using the number "0" for the letter "o" for example).

The legitimate URL www.cool-widgets.com could be replaced with:

www.c00l-widgets.com or www.cool-widgets.com.

Don't take the bait. Don't click reflexively on email links. Visit the legitimate web site by launching the web browser yourself. Type addresses directly into your browser. Or use your personal bookmarks.

- ❖ Scrutinize all email. What you see in the email body may seem familiar because it has been stolen from legitimate sources. The sender's address or return address can be spoofed. The email header can also be manipulated to disguise its true origin.
- ❖ Confirm domains and match up URLs. Check the web address in your browser to verify that the Web address in your browser is the same as the address shown in the email. Confirm that the address in your browser is associated with a legitimate company. Don't type your user name and password into a web page linked from an email message.
- ❖ Check the SSL certificate for sites requesting personal information. Double click the closed lock icon near the bottom right corner of your browser window to access the site's proof-of-identify security certificate.
 - Microsoft Internet Explorer: Check the name following "Issued to:" in the General tab of the pop-up window.
 - Netscape or Firefox: Click the "View" button that appears in the pop-up window's Security tab to see the security certificate, which will pop up in another window. In the General tab, check the "Common Name (CN)" and "Organization (O)" under "Issued To."
 - The name you check in the certificate window should match the site as depicted by the email message. If the name differs, you have reason to be suspicious.
- ❖ Don't enter sensitive information into pop-up windows. One common phishing technique is to launch a fake pop-up window when you click on a link. The popup may even be displayed over a window you trust.

No matter how official this window may appear to be, avoid entering sensitive information-- there is no way to check the security certificate. Close pop-up windows by clicking on the X in the window's corner. Don't rely on any buttons placed in the window by scammers.