JMARK
BUSINESS SOLUTIONS, INC.
Your Complete IT Services Partner

PHISHING AND SPEAR PHISHING SCAMS

DON'T GET CAUGHT IN THEIR NET

WWW.JMARK.COM

What is Phishing?

"Phishing" is tech-speak for an online scam which involves deceiving individuals into divulging their confidential information (such as credit card numbers, personal identification, usernames, and passwords). Phishing is nothing new. In fact, the first phishing scam occurred in 1996.

Phishing campaigns use social engineering techniques and some basic computer programming to lure email recipients and Internet users into believing that a fraudulent website is legitimate. Clicking on a phishing link takes the victim to a malicious site which either installs malware on their device or masquerades as a valid login page which harvests their login credentials. Once the hacker has hooked his victim, he then compromises his target, either stealing confidential information or executing any number of other malicious cyber activities.

What's the Difference Between Phishing and Spear Phishing?

General phishing emails usually involve a mass emailing campaign which targets a large set of users. They often impersonate a government agency, bank, social networking site, or an online service (like Amazon, Google, or Microsoft).

Spear phishing emails, on the other hand, target specific individuals. They are usually personalized with information pertinent to the victim which lures them in, and often appear to come from a company or person the victim knows.

A PHISHING OR SPEAR PHISHING EMAIL:

- Is usually unsolicited.
- May contain strange URLs and email addresses.
- Often uses improper grammar and contains spelling mistakes.
- Typically includes attachments that you don't recognize as legitimate.
- Asks you to take action by clicking on a link or downloading an attachment.
- May use language which is urgent or threatening.

PHISHING AND SPEAR PHISHING ARE EFFECTIVE BECAUSE THEY TARGET THE WEAKEST LINK IN ANY ORGANIZATION: ITS PEOPLE.

Sending out just 10 messages will result in:

- **90%** chance of at least one being opened.
- **8%** chance of a receiver clicking on an attachment.
- **8%** chance a user will fill out an illegitimate web form.
- **18%** chance a receiver will click a malicious link in an email.

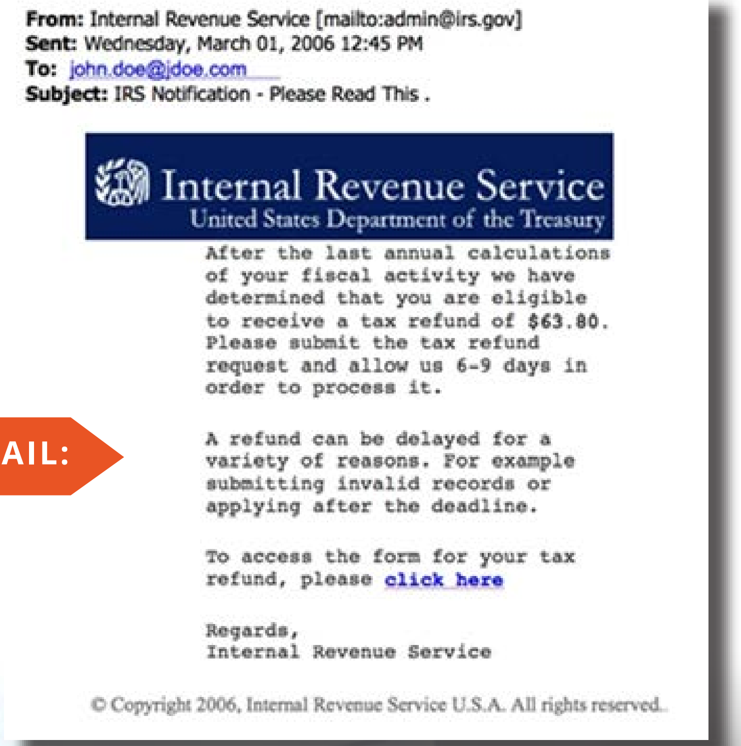
No one is immune. Even high-level executives have been deceived into divulging usernames and passwords.

THE AVERAGE COST OF A PHISHING SCAM IS $1.6 MILLION.

PHISHING IS A MAJOR SECURITY CONCERN FOR ANY BUSINESS:

- ✓ 1 in 3 companies are affected.
- ✓ 30% of phishing emails get opened.
- ✓ Phishing is now the #1 vehicle for ransomware and other forms of malware.

SAMPLE OF A PHISHING EMAIL:



From: Internal Revenue Service [mailto:admin@irs.gov]
Sent: Wednesday, March 01, 2006 12:45 PM
To: john.doe@jdoe.com
Subject: IRS Notification - Please Read This .

Internal Revenue Service
United States Department of the Treasury

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $63.80. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here

Regards,
Internal Revenue Service

© Copyright 2006, Internal Revenue Service U.S.A. All rights reserved.

HOW TO PREVENT YOURSELF FROM BECOMING A VICTIM OF PHISHING OR SPEAR PHISHING.

Follow these 8 essential rules:

1. **Stay informed about phishing techniques.**
Hackers develop creative phishing scams daily. Ongoing security awareness training should be a top priority for your organization.

2. **Think before you click a link.**
Don't click on links from random emails or text messages. Hover your mouse arrow over a link to see where the link leads. Most phishing emails begin with a generic greeting such as "Dear Customer," so keep an eye out for those. Verify the website's phone number before placing any calls. Remember, websites that start with "https" are more secure—although you should still watch for other warning signs

3. **Never divulge personal information requested by email, such as your name or credit card number.** Typically, phishing emails direct you to a webpage asking you to enter your financial or personal information. When in doubt, visit the primary website of the company mentioned in the email, and give them a call. Remember: never send sensitive information in an email to anyone.

4. **Consider installing an anti-phishing toolbar and other security tools.** Some Internet browsers offer free, anti-phishing toolbars that can run quick checks on the sites you visit. If a malicious site shows up, the toolbar will alert you. Be sure to stay informed about updated computer security tools, such as anti-virus software, spyware blockers, and firewalls. These solutions drastically reduce the chances of hackers and phishers infiltrating your computer or network.

5. **Never download files from suspicious emails or websites.** Double check the website URL for legitimacy by typing the actual address into your Web browser. Check the site's security certificate. Beware of any pop-ups, as they may be phishing attempts. Your browser settings give you the ability to block these or allow them on a case-by-case basis. If one gets through, don't click on the "cancel" button, as this could be a ploy. Click the small "x" in the upper corner of the window instead.

6. **Get into the habit of changing your passwords often.** You can also use a password manager like Dashlane or Last Pass which will automatically insert new, hard-to-crack passwords for you.

7. **Regularly check your online bank and credit card accounts.** Remain vigilant. Check your bank and credit card statements regularly to prevent bank and credit card phishing scams. Obtain monthly reports on all your financial accounts and check every entry carefully to ensure no fraudulent transactions have taken place without your knowledge.
8. **Update your browsers to the latest version.** Software vendors regularly release security patches in response to vulnerabilities that phishers and hackers have exploited. Don't ignore messages to update your browsers. Download and install these updates as soon as they're available.

Protect your confidential information and your business.

JMARK makes training your staff to recognize and block phishing and scams an important part of our cybersecurity services. Contact us at 844-44-JMARK or email JMARK@JMARK.com to learn more.