What is a spear phishing scam?

Spear phishing describes any highly targeted phishing attack. Spear phishers send e-mail that appears genuine to all the employees or members within a certain company, government agency, organization [university] or group.

Spear phishers often customize e-mails with information they've found on Web sites, blogs, or social networking sites like Facebook or MySpace. They also might create fake social networking login pages to lure people into sites where they're used to entering personal information.

The message might look like it comes from your employer, or from a colleague who might plausibly send an e-mail message to everyone in the company, such as the head of human resources or the person who manages the computer systems, and could include requests for user names or passwords.

The truth is that the e-mail sender information has been faked or "spoofed." Where traditional phishing scams are designed to steal information from individuals, spear phishing scams work to gain access to a company's entire computer system.

If you respond with a user name or password, or if you click links or open attachments in a spear phishing e-mail, pop-up window, or Web site, you might become a victim of identity theft and you might also put your employer or group at risk.

Spear phishing also describes scams that target people who use a certain product or Web site. Essentially, scam artists will use any information they can to personalize a phishing scam to as specific a group as possible.

The good news is that you can help avoid spear phishing scams by using some of the same techniques you already use to help avoid standard phishing scams.

5 tips to help you avoid spear phishing scams

1. **Never** reveal personal or financial information in a response to an e-mail request, **no matter who appears to have sent it**.
2. If you receive an e-mail message that appears suspicious, **call the person or organization** listed in the **From** line before you respond or open any attached files.

3. **Never** click links in an e-mail message that requests personal or financial information. Enter the Web address into your browser window instead.

4. **Don't post any information** on your blog or social networking site that could be used by identity thieves to target you, your family or friends, or your company.

5. **Report any e-mail that you suspect might be a spear phishing campaign within your company.**