4 Tips to Avoid Phishing Trips

The criminal art of “phishing,” e-mail spoofing that aims to get the recipient to click on a bad link or attachment, has been around for years. Recently, more phishing attempts are direct, targeted efforts aimed at specific individuals within an organization. This variation goes by the clever name “spear phishing.” Criminals now realize a message with specialized content that is directed to one person, or a small group of people, can be quite successful. After all, it typically only takes one machine to compromise an entire network.

Security awareness consultancy PhishMe has designed spear-phishing-awareness training that focuses on changing user behavior. Jim Hansen, vice president of sales for the company, gave us five tips his team offers clients to help them avoid getting hooked by a phony message.

1. **Be skeptical of all e-mails.**
   Ask yourself: Who is this message from? If the sender is someone you do not recognize, chances are this e-mail is either some form of unsolicited spam or it is a phishing e-mail, says Hansen.

2. **Ignore commands and requests for action.**
   If the e-mail is urging you to do something, stop and think. If it is too good to be true or seems too far-fetched, it probably is.
   
   "There are two motivations a criminal will try to appeal to: reward or authority," says Hansen.
   
   In an authority-based scam, the e-mail may say you need to take some action and the message purports to come from someone in a high position at your company. These messages may also say you have a package that was “undeliverable” or your bank account has been breached.
   
   The reward scenarios usually involve some kind of prize for entering a raffle or filling out a survey. Ignore them all, says Hansen.

3. **Be wary of attachments.**
   If you do open the e-mail and you are prompted to download images or attachments, don’t! They could contain malicious content.

4. **Use the phone.**
   Remember the phone? If you’re unsure, try to call the sender. To confirm that the e-mail was legitimately sent from that person or company, look up his phone number in your company directory or call the organization he claims to represent.