Five Ways to Identify a Phishing Email
By Wombat Security Technologies

Phishing and spear phishing attacks are becoming increasingly sophisticated in their appearance and their messaging. But if you are careful, you can avoid these types of attacks — and the ramifications that ill-advised clicks can bring.

Here are five ways to identify common phishing traps:

1. **Read**
   It may sound simplistic, but the act of reading an email can help you identify a phishing attempt. Don’t just skim and react.
   This exercise can be particularly helpful in identifying less sophisticated attacks. If a message seems nonsensical, contains spelling or grammatical errors, or just plain doesn’t feel right, do not interact with it, just delete it.

2. **Think**
   A favorite trick of social engineers is to motivate people to react without thinking, out of fear, anxiety, or excitement. These are common tactics to be wary of with phishing emails:
   - A message that creates fear or anxiety (e.g., a warning that an account has been frozen or hacked)
   - A prompt that urges you to act immediately (e.g., a “Hurry, don’t miss out!” message)
   - An offer that seems too good to pass up (e.g., a free tropical vacation for just a small processing fee)
   Before you click or respond to an “urgent request,” take a moment to think about what you could be compromising by acting in haste.

3. **Study**
   After you read an email, study the message, the sender, and even the address the email came from. Ask yourself these types of questions:
   - Would this company/person send this kind of message?
   - Do I interact with this company/person using this email account?
   - Would this company/person ask me to provide sensitive information via email?
   It’s critical that you take a moment to step back before interacting with an unsolicited message. And it’s important to remember that, though a legitimate company may alert you to an issue via email, they will likely never ask you to include information like account numbers or passwords in a reply.

4. **Hover**
   Attackers can make emails look legitimate by using recognizable logos, brand names, and web addresses. They can also use a technique known as spoofing to make the sending address appear to be something it’s not.
   Often, the simple act of hovering — i.e., moving your mouse’s pointer to a specific piece of text — can help you determine if a message is a phishing attack. For example, when you hover over text or a logo that has an embedded link, a pop-up bar (which generally appears in the lower left area of a computer screen) will show the destination URL of that link. If the link in that pop-up does not match what you think it should — e.g., the email appears to be from your bank, but the URL seems to point to a different site — this is a serious warning sign that the message is malicious.
   Similarly, you can hover over the sender’s name in the “From” field to see the identity behind the text that is visible on the surface. If there is a mismatch or if a well-known entity seems to be using a public email service like Gmail or Yahoo, you’ve got a phishing email on your hands.
   Hover functionality is not supported on mobile touchscreen devices, but you can often use a “long press” or “long click” technique to reveal a link’s identity. Press and hold your finger on a link until a pop-up box appears with the destination URL. But if that doesn’t work and you can’t verify a link, steer clear of the message.

5. **Confirm**
   If questions linger or you’re not sure what to do, it never hurts to go to the source. Before downloading an attachment you weren’t expecting, pick up the phone and verify that it’s legitimate. Instead of clicking through a link in an email, go to a trusted web page or call a known phone number to confirm that the offer, message, or request you received isn’t a ploy.

A few moments of caution can pay huge dividends when it comes to fending off phishing attacks. If you suspect a message you received in your business email account is malicious, alert your IT department as soon as possible. This can help prevent an attack from spreading.

© 2008-2015 Wombat Security Technologies, Inc. All rights reserved.