SOPHOS

Security made simple.

Ten Telltale Signs of Phishing

Phishing emails come in all shapes and sizes, but fortunately there are some "tells" you can look for to help suss out potential scams.

1. **It just doesn't look right.** Is there something a little off with the emails? Too good to be true? Trust your instincts if they tell you to be suspicious.

2. **Generic salutations.** Instead of directly addressing you, phishing emails often use generic names like "Dear Customer." Using impersonal salutations saves the cybercriminals time so they can maximize their number of potential victims.

3. **Links to official-looking sites asking you to enter sensitive data.** These spoofed sites are often very convincing, so before revealing personal information or confidential data examine the site to make sure it's real.

4. **Unexpected emails that use specific information about you.** Information like job title, previous employment, or personal interests can be gleaned from social networking sites like LinkedIn and then used to make a phishing email more convincing.

5. **Unnerving phrases.** Thieves often use phrases meant to scare you (such as saying your account has been breached) to trick you into acting without thinking, and in doing so revealing information you ordinarily would not.

6. **Poor grammar or spelling.** This is often a dead giveaway. Unusual syntax is also a sign that something is wrong.

7. **Sense of urgency.** For example: "If you don't respond within 48 hours, your account will be closed." By convincing you the clock is ticking, thieves hope you'll make a mistake.

8. **"You've won the grand prize!"** These phishing emails are common, but easy to spot. A similar, trickier variation is asking you to complete a survey (thus giving up your personal information) in return for a prize.

9. **"Verify your account."** These messages spoof real emails asking you to verify your account with a site or organization. Always question why you're being asked to verify – there's a good chance it's a scam.

10. **Cybersquatting.** Often, cybercriminals will purchase and "squat" on website names that are similar to an official website in the hopes that users go to the wrong site, such as www.google.com vs. www.g00gle.com. Always take a moment to check out the URL before entering your personal information.

For more information and tools to help you avoid the phisherman's net, visit www.sophos.com/prevent-phishing.