

Anti-Phishing Tips for *All* Computer Users

Phishing emails are designed to look like real email messages so they can fool you into clicking a link, opening an attachment, or sending information that you shouldn't send. Don't let yourself be fooled! Even if your work computer filters out most junk email, don't assume that whatever lands in your Inbox is safe to open.

- **Don't click on a link, open an attachment, or reply to any questionable email message.**
- Before you open any email message, look closely at the sender and the subject and think whether it could be a hoax, especially if it has an attachment.
- Suspect a hoax or scam if ...
 1. the message is from a sender you know but don't have reason to email with right now,
 2. the message is from you,
 3. the subject is empty or vague (such as "Check this out") or misspelled,
 4. the subject implies a recent business activity (an order, tracking number, or scan), says you've won something, or urges you to act quickly, or
 5. anything doesn't seem quite right.
- In Microsoft Outlook, the Junk Mail folder disables and unmarks internet links (URLs), so you can put a suspicious email into your Junk folder and open it there to read the message and inspect the actual URLs to determine if it is legitimate. For instance, something that claims to be from a certain company but has a URL that doesn't include the company's name is probably a ploy, hoax, scam, or risk.
- The most convincing scams look like they are coming from someone you know. In a recent ploy, an email was sent using the email address of a top-level manager telling employees to reply immediately and provide certain financial information. Any actual reply would send that sensitive information to the scammer.
- Don't let yourself be rushed into a bad decision: take a few minutes to check with the apparent sender, or even a co-worker, to figure out whether an email is legitimate.

Your brain is your best defense. Hackers and crooks are coming up with new scams every day, so no list published today can protect you against tomorrow's threats. Always keep your eyes and ears open for the latest hoaxes and scams.