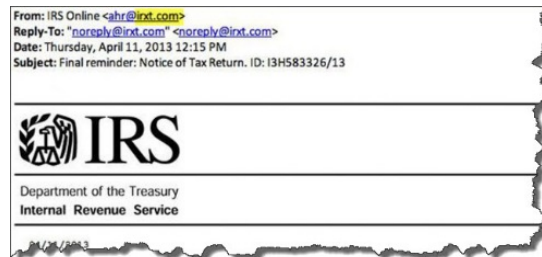


10 Best Practices to Avoid Infected Emails

#1 Don't Trust the Display Name

A favorite phishing tactic among cybercriminals is to spoof the display name of an email. Here's how it works: If a fraudster wanted to impersonate the IRS, the email may look something like:



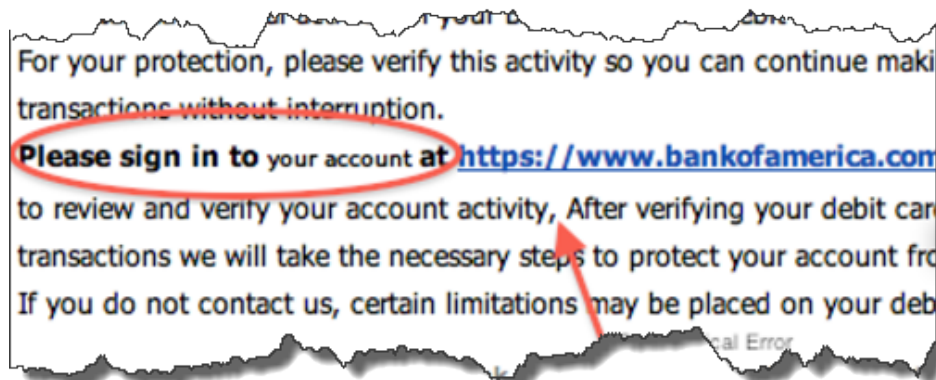
#2 Look But Don't Click

Cybercriminals love to embed malicious links into legitimate-sounding links. Hover your mouse over any links you find embedded in the body of your email. If the link address looks weird, don't click on it.



#3 Check for Spelling Mistakes

Brands are pretty serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious.



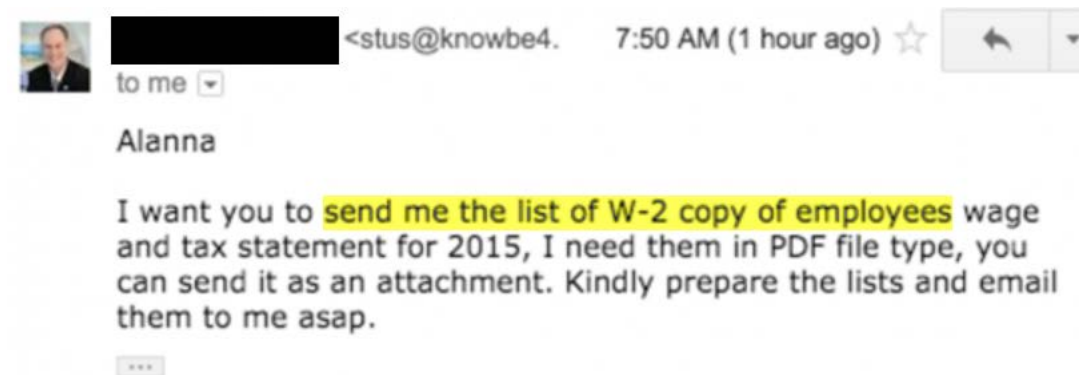
#4 Analyze the Salutation

Is the email addressed to a vague 'Valued Customer?' If so, watch out—legitimate businesses will often use a personal salutation with your first and last name.



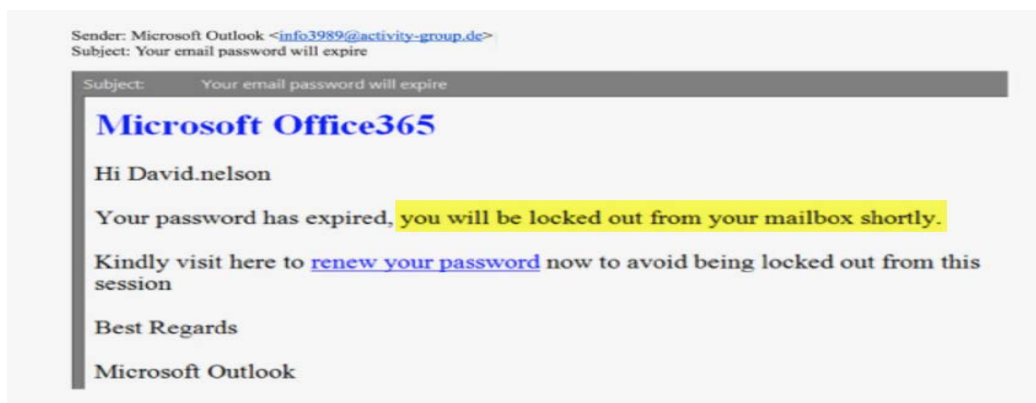
#5 Don't Give Out Personal or Company Confidential Information

Most companies will never ask for personal credentials via email.



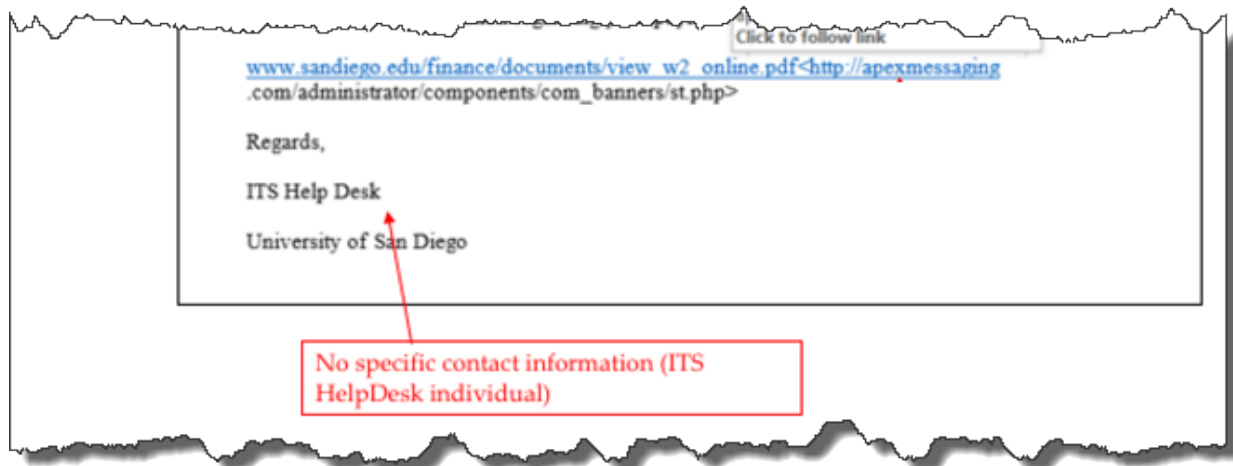
#6 Beware Of Urgent or Threatening Language in the Subject Line

Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your “account has been suspended” or ask you to take action on an “urgent request.”



#7 Review the Signature

Lack of details about the signer or missing contact information for a company strongly suggests a phish. Legitimate businesses always provide contact details. Check for them.



#8 Don't Click On Attachments

Including malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. **Don't open any email attachments you weren't expecting.**

#9 Don't Trust the Header From: Email Address

Keep in mind that just because the sender's email address in the header looks legitimate, it may not be. A familiar name in your inbox isn't always who you think it is.

#10 Don't Believe Everything You See

Phishers are extremely good at what they do. Many malicious emails include convincing brand logos, language, and a seemingly valid email address. **Be skeptical when it comes to your email messages — if it looks even remotely suspicious, do not open it.**