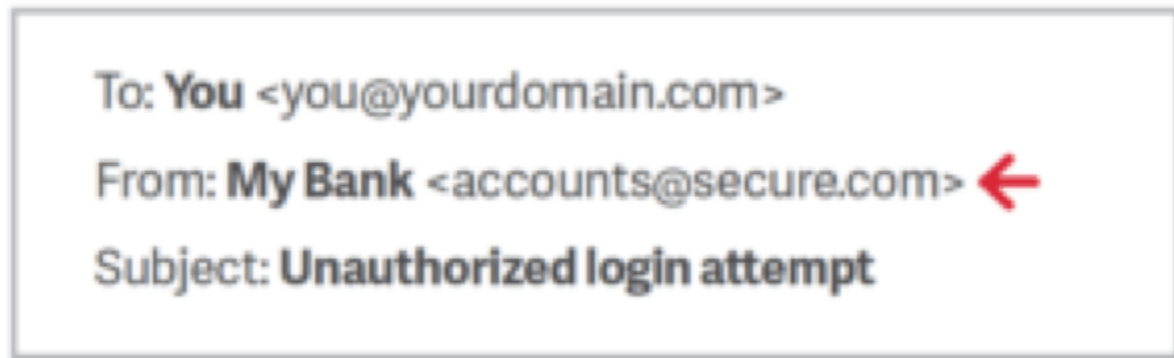**Tip 1: Don't trust the display name**

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 hypothetical brand "My Bank," the email may look something like:



Since My Bank doesn't own the domain "secure.com," email authentication defenses will not block this email on My Bank's behalf.

Once delivered, the email *appears* legitimate because most user inboxes and mobile phones will only present the display name. Always check the email address in the header from—if looks suspicious, flag the email.

**Tip 2: Look but don't click**

Cybercriminals love to embed malicious links in legitimate-sounding copy. 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. If you have any reservations about the link, send the email directly to your security team.

**Tip 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.

**Tip 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.

**Tip 5: Don't give up personal or company confidential information**

Most companies will *never* ask for personal credentials via email--especially banks. Likewise most companies will have policies in place preventing external communications of business IP. Stop yourself before revealing any confidential information over email.

**Tip 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 action an "urgent payment request."

**Tip 7: Review the signature**

Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details. Check for them!

**Tip 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.

**Tip 9: Don't trust the header from email address**

Fraudsters not only spoof brands in the display name, but also spoof brands in the header from email address, including the domain name. Keep in mind that just because the sender's email address looks legitimate (e.g sendername@yourcompany.com), it may not be. A familiar name in your inbox isn't always who you think it is!

**Tip 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.