



USANEC-SC

Phishing Facts



8 May 2020



Overview

- **What is phishing?** Phishing is an online scam involving emails that appear to be from a trusted source. Recent examples try to convince recipients that they are exceeding their email quota and need to upgrade their account by clicking a link. Others have said that the recipient's account is going to be deleted unless they click the link to renew it. These are all scams!
- **What happens if I click the link?** By clicking a phishing scam link, you may compromise your computer account and/or your computer, you may even compromise your personal data.
- **What happens if I compromised my computer?** If the scam introduces malware to your computer, it is a lengthy process to clean the computer and restore it to pre-link clicking. That also may involve removal of your computer from the network, until it has been cleaned, as compromised computers may infect other computers on the network.



Phishing TIPS

Tip 1: Don't trust the display name

A favorite phishing tactic among cybercriminals is to spoof the display name of a legitimate company. Here's how it works: If a fraudster wanted to impersonate the brand "USAA," the email may contain a link that looks like this when you hover your cursor above the display name:



Note that the display name is 'WWW.USAA.COM' but the actual internet address that clicking on the link will take you to is 'WWW.USAAA.COM'. Email authentication defenses will not block this email on USAA'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 from header - if looks suspicious, flag the email. Do NOT click on the link.



Phishing TIPS

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.



Phishing TIPS

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 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.



Phishing TIPS

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!



Phishing TIPS

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.



How To Report Phishing Attempts

- What should I do if I receive a possible phishing scam email?
- **DO NOT** click it.
- Create a new email message.
- Enter the 'To' Email address.
- southcom.miami.scj6.mbx.omb-spambox-and-reported-incidents@mail.mil
- From your inbox, select the suspicious Email that you received (please select the Email, not the content) and drag then drop the selected item into the body of the new Email.
- Insert the subject line as: **SUSPICIOUS EMAIL**
- Provide us with a brief description.
- The new Email should include the suspicious Email as an attachment.
- Send the Email message.
- What if I can't tell if it is a scam? The way to be safe is to think before you act so you do not fall prey to the enemy. If ever in doubt, please contact the Help Desk at x1234



Questions?

Call the Help Desk at x1234