

9.12 Lab: Respond to Social Engineering Exploits

Candidate: COMPTIA COMPTIA ()

Time Spent: 00:45

Score: 0%

Task Summary

Required Actions

- ✗ Delete the Microsoft Windows Update Center phishing email
- ✗ Delete the Jim Haws malicious attachment email
- ✗ Delete the Executive Recruiting whaling email
- ✗ Delete the Riverdale Estates HOA Online Banking phishing email
- ✗ Delete the Grandma White forwarded email hoax
- ✗ Delete the Daisy Knudsen spear phishing email
- ✗ Delete the Rachelle Hancock malicious attachment email
- ✗ Delete the Grandma White forwarded email hoax

Explanation

Complete this lab as follows:

1. Read each email and determine whether the email is legitimate.
2. Delete any emails that are attempts at social engineering.
3. Keep all emails that are safe.
4. The following table lists a summary of the results:

Email	Diagnosis	Action	Description
Microsoft Windows Update Center New Service Pack	Phishing	Delete	Notice the various spelling errors and that the link does not direct you to a Microsoft website.
Jim Haws Re: Lunch Today?	Malicious Attachment	Delete	This email appears to be from a colleague. However, why would he fail to respond to your lunch question and send you a random attachment in return?

Executive Recruiting Executive Jobs	Whaling	Delete	Whaling uses tailored information to attack executives. Clicking the link could install malware that would capture sensitive company information.
Human Resources Ethics Video	Safe	Keep	While this email has an embedded link, it is digitally signed, so you know it actually comes from your Human Resources department. In addition, if you hover over the link, you see that it is a secure link to the corporate web server.
Riverdale Estates HOA Payment Pending	Phishing	Delete	This is a carefully crafted attempt to get your bank account information. Hover over the link and notice that it does not direct you to your credit union website but to an unknown IP address instead.
Grandma White FW: FW: FW: Virus Attack Warning	Hoax	Delete	Any email that asks you to forward it to everyone you know is probably a hoax.
Daisy Knudsen Web Site Update	Spear Phishing	Delete	While this email appears to come from a colleague, notice that the link points to an executable file from a Russian domain name. This probably is not a message a real colleague would send. This file will likely infect the computer with malware.
Rachelle Hancock Wow!!	Malicious Attachment	Delete	Emails with attachments from random people who address you as "Dear Friend" are probably not safe.
Grandma White Free Airline Tickets	Hoax	Delete	Any email that asks you to forward it to everyone you know is probably a hoax, even if the contents promise you a prize. In addition, there is no way to know how many people the email has been forwarded to.
Human Resources IMPORTANT NOTICE-Action Required	Safe	Keep	While this email appears very urgent, it doesn't ask you to click on anything or run any attachments. It does inform you that you need to go a website that you should already know and make sure your courses are complete.
Activities Committee Pumpkin Contest	Safe	Keep	This email doesn't ask you to click on anything or run any attachments.
Bob Avez Presentation	Safe	Keep	This email doesn't ask you to click on anything or run any attachments.