

Review the email below. Identify if it is a phishing email or if it is legitimate.



From: Msonlineservices <noreply@ms-notifications.com>  
Subject: Security Alert: Password has expired!  
Monday, April 17, 2023 at 5:19:18 PM

Hello Microsoft User,

Your Microsoft Account has expired!

Don't be alarmed as this happens often, you just need to update it immediately.

Click on the link to update your password now. View attachment to see our password security guidelines.

[Update Password Now](#)



It is a phishing attempt



It is a legitimate email

Submit

You receive an unexpected email that appears to be from a co-worker, but you don't recognize the email address. The email is asking you to complete a wire transfer because your co-worker is out of the office, and the request was urgent from your CEO. Which of the following actions will help keep you and your organization secure?

- ☐ Complete the transfer, then confirm if the request was legitimate.
- ☐ Complete the transfer; it's from someone you trust.
- ☒ Call your co-worker using a phone number you know is correct, and ask if they sent this message.
- ☐ Ignore the message; let someone else report it.

**Vivian just received a voicemail asking for her username and password in order for the IT department to add new software to her computer. What should she do?**

- ☐ Call the number back and ask for more information about the software.
- ☒ Call your known IT department number and verify the request.
- ☐ Ask her co-worker if they also received the call.
- ☐ Call the number back and give the information they asked for.

Submit

**You accidentally click on an unknown link in an email, and your system seems to be running very slowly. Which of the following actions will help keep you and your organization secure?**

- ☒ Report it immediately to your IT department.
- ☐ Delete your web browser history.
- ☐ Restart your computer.
- ☐ Delete the message, and monitor your computer for other problems.

**You receive the following email from a co-worker you've never met. What should you do?**

**Date:** September 2

**Time:** 4:00 pm

Hi Felipe,

Nice to virtually meet you! I am emailing you today regarding account 674927. Fatima has reached out and would like for us to collaborate on that account. Can you forward me all account details, and share the folder by 4:30 today? I am hoping to get a headstart on it before the quarterly updates meeting on Wednesday. Thanks for your help!

- ☐ Reply to the message asking for more information.
- ☐ Delete the message since you do not know the sender.
- ☒ Verify the request is legitimate by contacting your co-worker via another method.
- ☐ Send all account information to the sender. Since they mentioned Fatima, it was probably approved.

**You receive an email from someone that you don't recognize but is listed as an executive at your organization. The message contains a link to a shared file. Which of the following actions will help keep you and your organization secure?**

- ☒ Review the link carefully before taking any other action, and notify IT/Security if it seems suspicious.
- ☐ Click on the link; it's ok because the message came from someone you work with.
- ☐ Ignore the request; they most likely accidentally typed the wrong email address.
- ☐ Reply to the email, and ask if they intended to send it to you before you open it.

**You get an email from HR discussing some new return to office policies. It looks like someone mistakenly attached a spreadsheet entitled "Payroll" to the message. What should you do?**

- ☐ Open the attachment as long as an anti-virus scan says it's clean.
- ☒ Don't open it; report the message as suspicious.
- ☐ Respond directly to the message and let them know about the mistake.
- ☐ Check the "From:" address and if it's legit, sneak a peek at the attachment.

**You notice your computer is running slowly, constantly taking you to websites that you didn't choose to go to, and frequently shutting down without warning. What are these signs of?**

- ☐ Your computer getting old
- ☐ One of your co-workers pulling a prank on you
- ☐ Your computer needing an update
- ☒ Your computer being infected with malware

**As a cloud administrator, you are responsible for asking many questions. Which of the following questions should you be asking if you have concerns about availability?**

- ☐ Which resources are shared between the different clients?
- ☐ What permissions should be allocated to different types of users?
- ☐ How does my cloud provider maintain data privacy?
- ☒ Is it possible to do a complete system restore to a secondary location?

What traits generally make a cloud a cloud? Select the three options that apply?

- ☒ Usually offered as a web site or service
- ☒ Usually have more than one customer
- ☐ Always on the Internet and publicly accessible to anyone
- ☒ Usually run on virtual machine platforms

What is the most common reason for cloud compromise?

- ☒ Social engineering
- ☐ Shared tenancy
- ☐ Rogue APIs
- ☐ Cloud-based malware

**Which of the following steps can you take to reduce the risk from overly permissive permissions?**

---

- ☒ Make sure that only the people who need to view content can see it.
  - ☐ Broaden permissions to ensure that users can get to everything.
  - ☒ Minimize the number of permanent members of any elevated group.
  - ☒ Regularly audit all security settings and permissions.
- 

**What is the name of the independent organization dedicated to cloud security?**

---

- ☐ Amazon AWS
  - ☒ Cloud Security Alliance
  - ☐ Microsoft Azure
  - ☐ Google
- 

**Which of the following steps can you take to reduce the risk from overly permissive permissions?**

---

- ☒ Make sure that only the people who need to view content can see it.
  - ☒ Broaden permissions to ensure that users can get to everything.
  - ☐ Regularly audit all security settings and permissions.
  - ☐ Minimize the number of permanent members of any elevated group.
-