TRAINING QUIZ: MALWARE, VIRUSES AND PHISHING

Part I: Background and Context – Malware, Phishing etc.

1. What do phishing, spear phishing, vishing, scareware, watering hole attacks and their ilk have in common?

☐ A. They are all "social engineering" attacks that commonly disguise themselves as coming from trusted individuals in order to manipulate you (their target) into letting down your guard and falling for cyber attacks. A social engineering attack leverages the human factor to obtain sensitive information. A cyber attacker will exploit the human nature of trusting, the desire to be helpful and the lack of awareness of social engineering attacks such as phishing, vishing and smishing to obtain personal information.

☐ B. They are all funny-sounding terms that have no harmful significance other than their ability to wreck your computer, steal or corrupt your personal and other confidential information, ruin your day (and possibly more than just that one day), and bring ill repute to yourself or to your company or organization.

☐ C. They are today's common examples of a much larger and constantly evolving set of methods used by bad guys to exploit human behavior in order to wrongfully access computers and their contents.

☐ D. All of the above are correct.

* * *

2. Who are the targets of modern day hackers?

☐ A. Banks and finance companies who process a lot of payments.
☐ B. Any organization or individual is liable to be the victim of hackers.
☐ C. Companies which hold a lot of proprietary information.
☐ D. Companies which hold credit card numbers of customers.

* * *

3. True or False: To protect personal information and other sensitive data, you need only worry about outsider threats such as hackers, phishing scams and ransomware.

☐ A. True
☑ B. False

* * *

4. True or False: If you install software from the internet there is a possibility that viruses or malware could infect your computer and access PII or sensitive data.

☑ A. True
☑ B. False

* * *

5. An email claiming that you won the lottery and requesting that you fill out the corresponding information, is an example of what type of cyber-attack?

☐ A. Baiting
☐ B. Phishing
☐ C. Scareware
☐ D. Vishing

* * *

6. Which of the following is/are example(s) of a phishing attack?

☐ A. Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows.
☐ B. Creating a fake website that looks nearly identical to a real website in order to trick users into entering their login information.
☐ C. Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest.
☐ D. All of the above are correct.

* * *

7. True or false: Scareware is malicious software that tricks computer users into visiting malware-infested websites by displaying a fake pop-up warning on the screen.

☐ A. True
☐ B. False

* * *

8. In a "watering hole" attack, the attacker compromises a site likely to be visited by a particular target group, rather than attacking the target group directly. True or False?

☐ A. True
☐ B. False

* * *

9. "Vishing" is a cybercrime that uses the phone to steal personal confidential information from victims. True or False?

☐ A. True
☐ B. False

* * *

10. True or false: You can trust that an email from your client really comes from that client if it uses the client's logo and contains at least one fact about the client that you know to be true.

☐ A. True
☐ B. False

* * *

11. Cyber security protection of an organization is the responsibility of:

☐ A. Everyone in the organization.
☐ B. The CIO or CISO executive.
☐ C. A specialized cybersecurity defense team.
☐ D. The board of directors.

* * *

Part 2: Cyber-Attacks in Action (with Examples)

1. What are some of the ways to distinguish a legitimate email from a phishing email?

☐ A. Bad spelling, poor syntax and grammar are common signs of a fake email. On the other hand, an email with good spelling, syntax and grammar is probably ok.
☐ B. Look at the email headers to see where it really came from.
☐ C. Poorly replicated logos.
☐ D. Contact the sender on some other medium besides email to verify whether they sent you the email.

* * *

2. A new window pops up on your screen telling you that a virus has been found on your computer. You are presented with a message intending to deceive you into thinking your computer is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or downloading the actual malware, or redirect you to malware-infested websites. For example:

"Scareware" is a false alarm or fictitious threat. How can you tell this is Scareware?

☐ A. Hovering over any of the links will direct you out to third party websites for action, not to Microsoft domains.
☐ B. Windows Firewall will not direct you out to third party websites for action.
☐ C. Seeks to make you click on buttons for "Enable Protection" and "Click here to pick recommended software to resolve the issue".
☐ D. The entire pop-up window may be hyperlinked, directing you to third party websites for action.
☐ E. All of the above are correct.

The window then presents you a button for you to click offering to resolve the issue. Your best course of action is to:

☐ A. Click on the button to remove the virus.
☐ B. Place your cursor over the button and check the link's website address (URL). If the address looks legitimate, click on it. If it looks like a scam link, close the window.
☐ C. Close both the original browser window and the new "pop-up" window. Do not return to that site.
☐ D. Hit the back button and see if it goes away.

* * *

3. Unexpectedly, you get an email from a colleague who asks you to urgently click on an email link which they've sent you. Q: What's going on here? A: Who knows, but it has common signs of phishing: An urgent request for action. An unsolicited link sent to you. Q: What should you do?

☐ A. The link is from a known person therefore it's safe to open.
☐ B. If the link was malicious the organization's firewall would have flagged or blocked it, therefore it's safe to open.
☐ C. Reply to the sender to double-check if the link is safe to open as they might have sent it accidentally.
☐ D. Do not click the link. Telephone or email or text the sender for verification: Any method other than replying to the email.

* * *

4. A colleague calls you telling you she has an urgent deadline to meet. Unfortunately, your colleague forgot her password to [whatever system] and asks you to provide her your password. What should you do to help?

- ☐ A. Go to a computer terminal and log the user in so they can meet their deadline.
- ☐ B. Suggest to your colleague that they call your IT helpdesk for a password reset link.
- ☐ C. Give them your login credentials temporarily so your colleague can meet their deadline.
- ☐ D. Put your login credentials on an encrypted USB memory stick and hand it to them.

* * *

5. You receive an email from your bank warning you that suspicious activity has been detected and to login immediately using a link provided. Which of these actions should you <u>not</u> do?

- ☐ A. Login immediately and change your password to a more complex one.
- ☐ B. Login to your bank account immediately and check your balance.
- ☐ C. Check the headers in the email and then login.
- ☐ D. Contact your bank by telephone or email using the contact information provided in the email notice you received.
- ☐ E. You should not do any of these things.

* * *

6. You get a call from your support helpdesk saying they are performing an urgent server upgrade. They ask you for your password. What should you do?

- ☐ A. Get the caller's name and give him your login and password.
- ☐ B. Get the caller's email address and email him your login and password.
- ☐ C. Give the support representative your password, but not your login.
- ☐ D. Refuse and contact your manager or technology director.

* * *

7. True or false: If you're working on a project with a colleague or a vendor, you can click on any links as long as you have a spam blocker and anti-virus protection.

- ☐ A. True
- ☐ B. False

* * *

8. You get an email from your Operations Director asking you to provide personal information right away. True or false: You should check it out first to verify who they say are and the validity of the request, and then it's ok to send.

☐ A. True, but ….
☐ B. False

* * *

9. You receive an email from your boss or manager or the company CFO: She asks for the name, addresses, and credit card information of the company's top clients. The email says it's urgent and to please reply right away. You should reply right away. True or False?

☐ A. True
☐ B. False

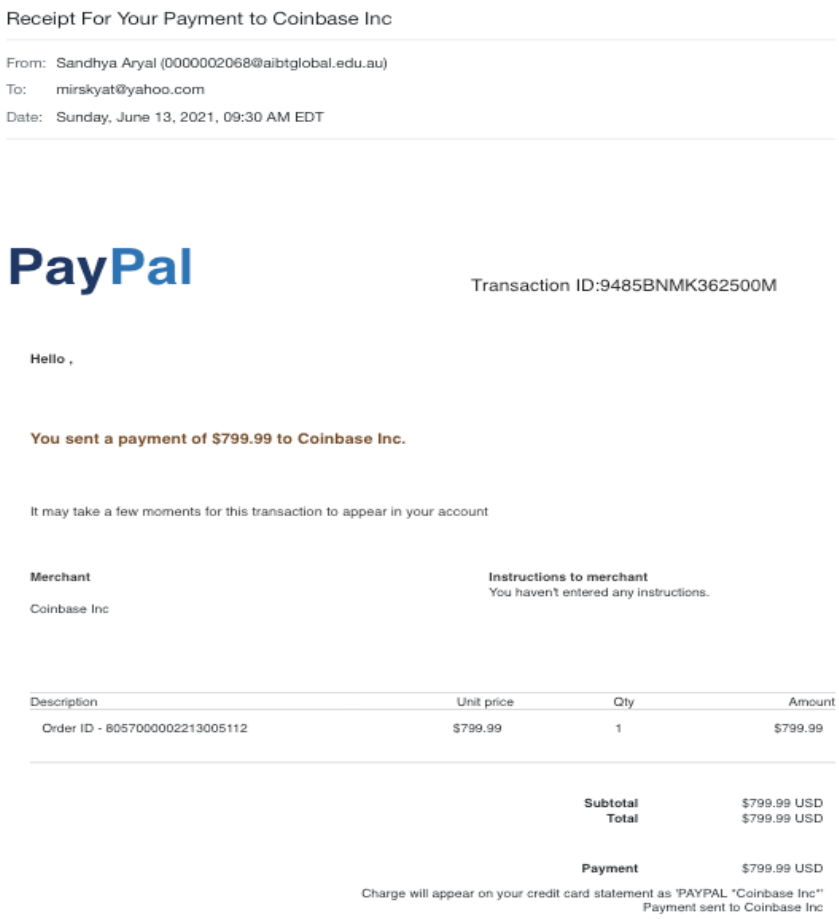
Or … you get this email:

How can you check whether the request is valid?

☐ A. Check the sender's email address for discrepancies, by hovering over the address with your mouse (or by pressing – and holding, not clicking – if on a phone).
☐ B. Follow normal procedures for payments and wires, which may include double sign-offs on certain threshold amounts.
☐ C. Pay attention to unusual circumstances in the request, such as statements of urgency.
☐ D. All of the above are correct.

* * *

10. You receive this "Receipt for your Payment to Coinbase" email from PayPal:



Receipt For Your Payment to Coinbase Inc

From: Sandhya Aryal (0000002068@aibtglobal.edu.au)
To: mirskyat@yahoo.com
Date: Sunday, June 13, 2021, 09:30 AM EDT

PayPal

Transaction ID:9485BNMK362500M

Hello ,

You sent a payment of $799.99 to Coinbase Inc.

It may take a few moments for this transaction to appear in your account

Merchant
Coinbase Inc

Instructions to merchant
You haven't entered any instructions.

Description	Unit price	Qty	Amount
Order ID - 805700002213005112	$799.99	1	$799.99

Subtotal $799.99 USD
Total $799.99 USD

Payment $799.99 USD

Charge will appear on your credit card statement as 'PAYPAL *Coinbase Inc*'
Payment sent to Coinbase Inc

You know you didn't authorize a payment, so this probably gets your attention regardless. But how else can you tell that this is a fraudulent email?

☐ A. The sender's email is "0000002068@aibtglobal.edu.au" (rather than from a PayPal sender).
☐ B. The phone number is not the actual PayPal number.
☐ C. The whole email is hyperlinked (not just embedded links), so that if you click on any part of it, it will take you too a malicious website. Or …by clicking on any part of it, it may then immediately download malware onto your device.
☐ D. The PayPal logo is not accurate.
☐ E. All of the above are correct.

What actions(s) is the sender trying to get you to do?

☐ A. Click on (and dial) the (fake) phone number, and then provide personal information when solicited by the sender.
☐ B. Click on the hyperlinked email and thereby cause you to download malware, or be redirected to a malware-infested website.
☐ C. Nothing. While the email is a fake message pretending to be from PayPal, the sender is not trying to cause you to do anything other than simply annoy you.

☐ D. Both A and B are correct.

* * *

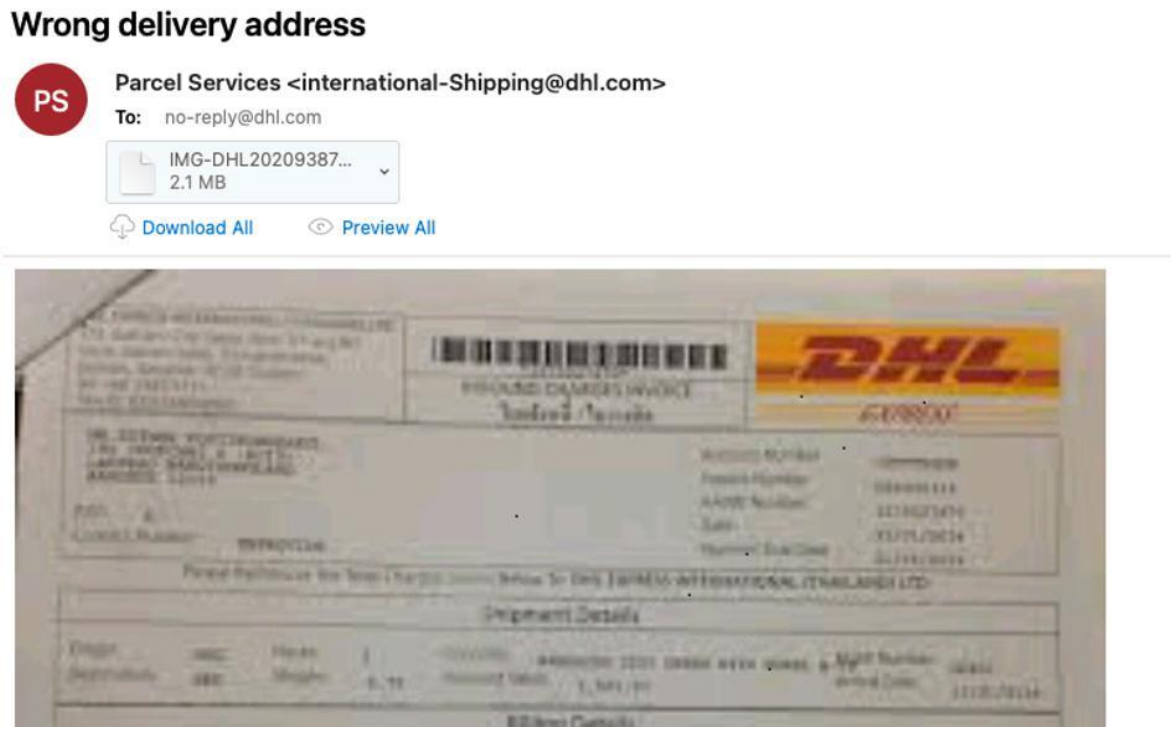
11. You get a text from a vendor asking you to click on a link to renew your password so that you can log in to its website. You should:

☐ A. Reply to the text to confirm that you really need to renew your password.
☐ B. Pick up the phone and call the vendor, using a phone number you know to be correct, to confirm that the request is real.
☐ C. Click on the link. If it takes you to the vendor's website, then you'll know it's not a scam.

You receive this email from that same vendor or perhaps from an unknown person:

Source of image:
https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

Or you receive this email, presumably from a package delivery service:



Source of image: https://www.forbes.com/sites/barrycollins/2021/01/16/dont-click-on-these-5-dangerous-email-attachments/?sh=253b0e577847

In both examples, the senders are trying to get you to click on the attachments. In one case, it's a pdf ("Invoice.pdf") that looks like a perfectly legitimate (or harmless) invoice file, and in the second it looks like a fuzzy screen shot of an actual DHL invoice. In both cases, the files will cause malware to download onto your computer.

Which of these may indicate that these emails are trouble?

☐ A. The email is unsolicited or from an unknown source.
☐ B. The email address uses a strange "to" field, perhaps a long, alphabetical list of recipients, or the "to" field is blank.
☐ C. A vague or ambiguous subject line.
☐ D. No salutation addressing you.
☐ E. Poor grammar/spelling
☐ F. A sense of urgency in the requested response
☐ G. All of the above are correct.

The file type of an attachment is also a tip-off, but that can be more challenging to perceive, for several reasons. ".exe" files are executable files, which launch programs when you click on them and which can install malware on your computer. It's unusual to share ".exe" files by email, since there's typically no reason to do so. On the other hand, some attachments can show the icon for a Microsoft Office document (Word, PowerPoint, etc.) or PDF, but still have the .exe extension.

The problem gets trickier with other file types, including Word and other commonly used Microsoft Office files and Adobe files such as PDF. These files are of course shared routinely countless times

every day, and mostly quite safely. However, these files can be embedded with macros which can cause malware to download onto your computer.

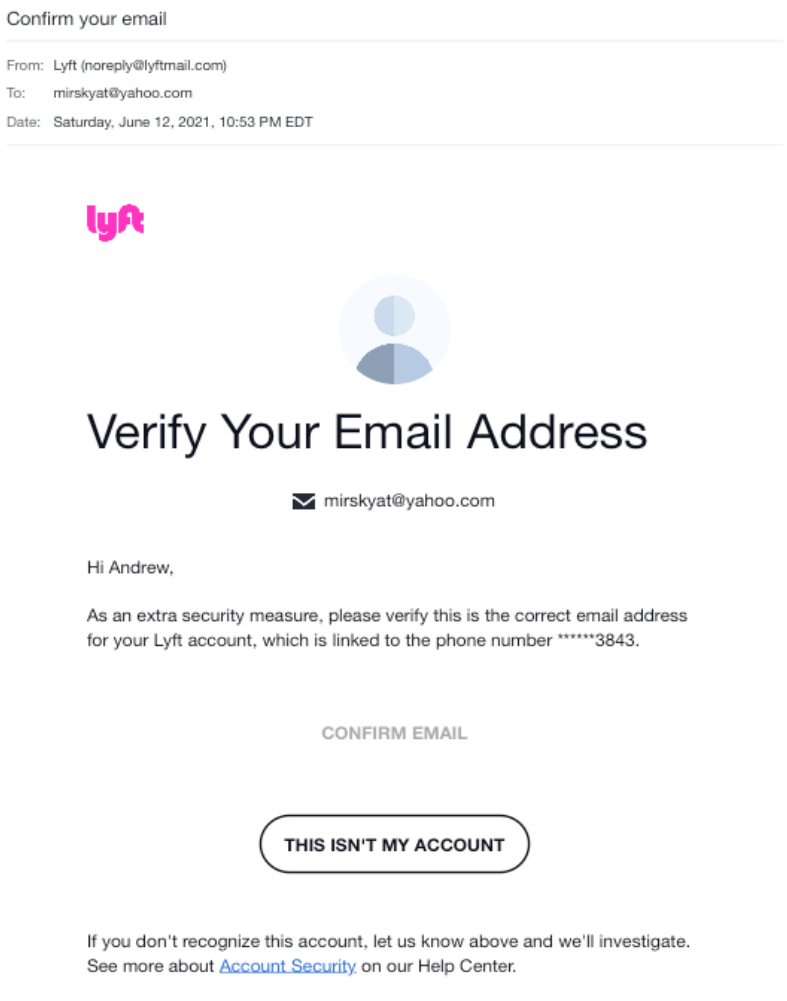
What is one to do to protect oneself against these sorts of attacks via malicious attachments?

☐ A. Don't click on attachments. Period.
☐ B. If the email has passed the "tests" above, but you're still unsure whether the attachment is safe to open, call or email or text the sender by a method other than by replying to the email.

Not clicking on any attachments is certainly a safe way to prevent phishing or malware attacks via malicious attachments, but perhaps not the most practical way to live in the modern technologically interactive world. Especially when there are safe and practical alternatives.

* * *

12. This email from Lyft asks you to confirm your email address. How can you tell that this email from Lyft is <u>not</u> suspicious?


Confirm your email

From: Lyft (noreply@lyftmail.com)
To: mirskyat@yahoo.com
Date: Saturday, June 12, 2021, 10:53 PM EDT

lyft

Verify Your Email Address

mirskyat@yahoo.com

Hi Andrew,

As an extra security measure, please verify this is the correct email address for your Lyft account, which is linked to the phone number ******3843.

CONFIRM EMAIL

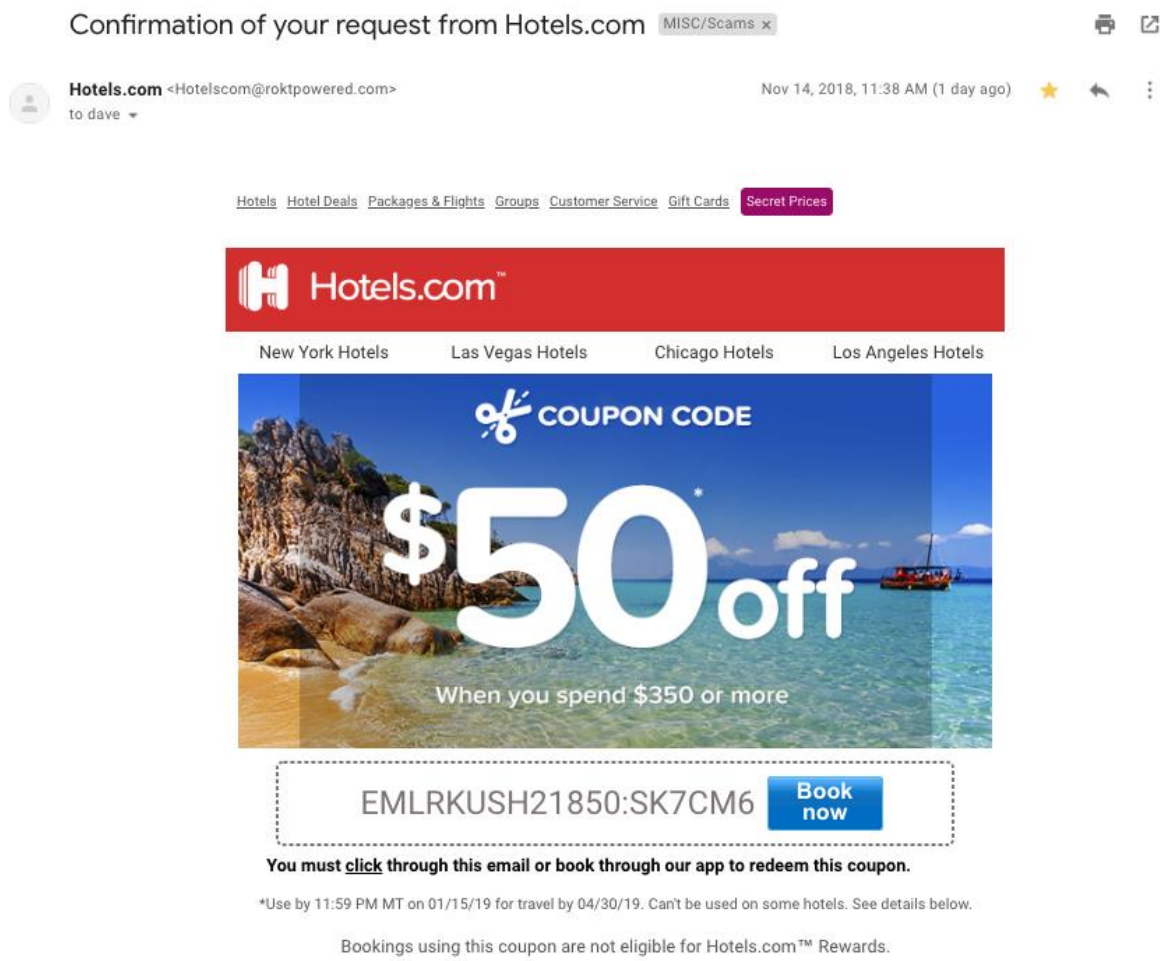
THIS ISN'T MY ACCOUNT

If you don't recognize this account, let us know above and we'll investigate.
See more about Account Security on our Help Center.

☐ A. The sender's email looks like it's from a valid Lyft email domain: "noreply@lyftmail.com".
☐ B. If you roll your mouse over the links (without clicking), the links direct you to Lyft domains (subpages on https://account.lyft.com or https://help.lyft.com), all of which also have the "https://" security indication.
☐ C. You were using the Lyft app only minutes before receiving this email, and it made sense that you ☐ should receive this email based on that context.
☐ D. All of the above are correct.

* * *

13. You get this email from Hotels.com:



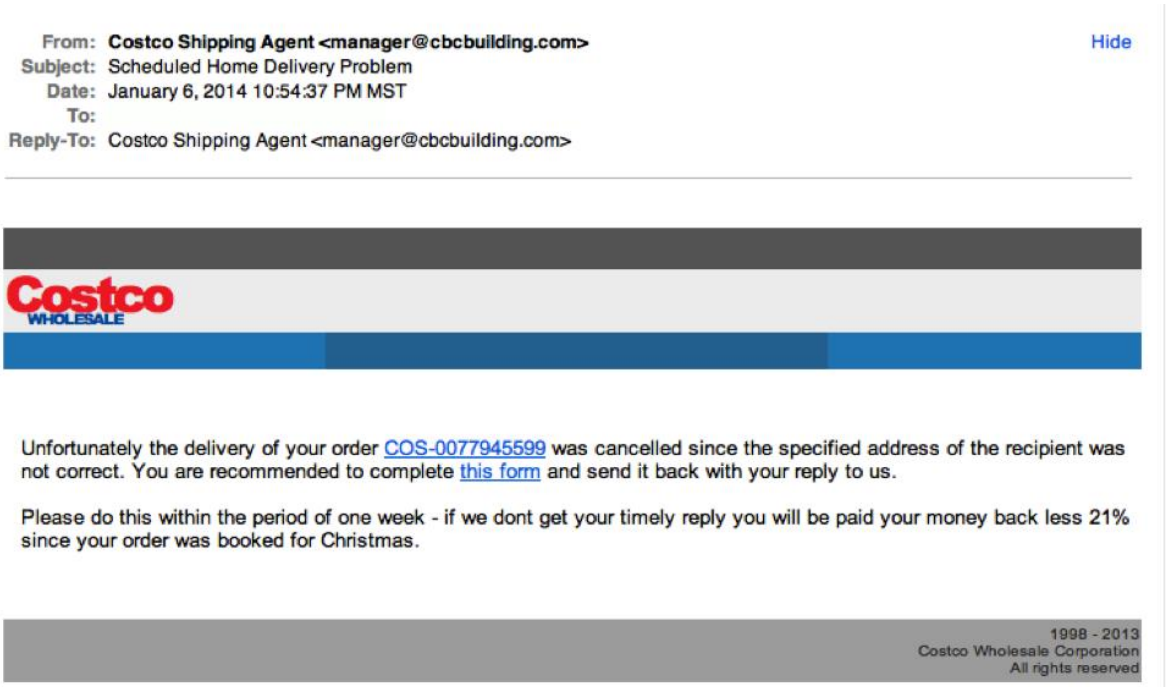
How do you know this one is <u>not</u> legitimate?

☐ A. Hotels.com would never send an ad like this.
☐ B. The sender's email is "Hotelscom@roktpowered.com" (rather than from a Hotels.com domain).
☐ C. The urgency that "you must **<u>click</u>** through this email or book through our app to redeem this coupon."
☐ D. Answers B and C are the strongest reasons for questioning the validity of this ad.

Source of this image: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

* * *

13. You receive this email from Costco about a problem with delivery of your order:



From: **Costco Shipping Agent <manager@cbcbuilding.com>** Hide
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>

Costco WHOLESALE

Unfortunately the delivery of your order COS-0077945599 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

1998 - 2013
Costco Wholesale Corporation
All rights reserved

What actions(s) is the sender trying to get you to do?

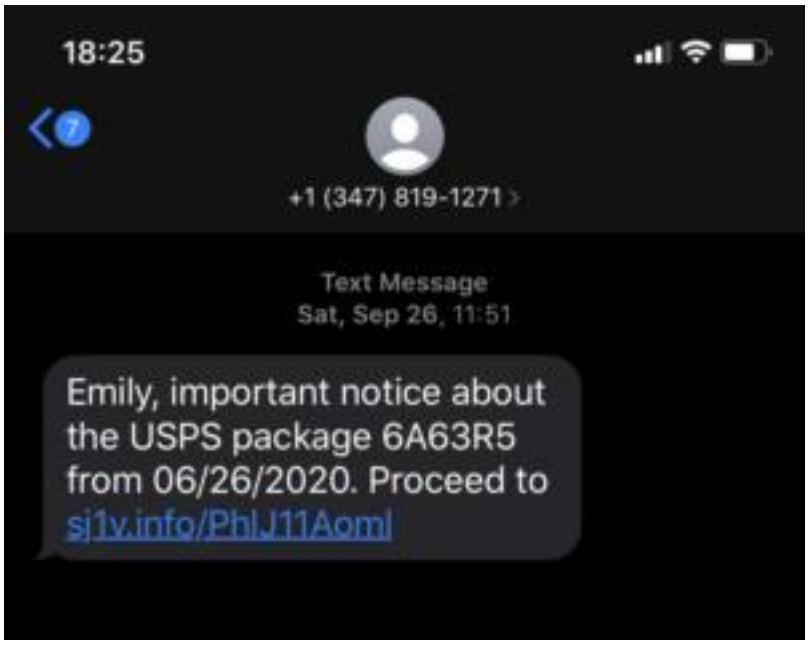
☐ A. Click on the link in the email to "complete this form" and thereby cause you to download malware, or be redirected to a malware-infested website or provide personal information when solicited by the sender.
☐ B. Nothing. While the email is a fake message pretending to be from Costco, the sender is not trying to cause you to do anything other than simply annoy you.

What should you do now that you believe these are phishing emails?

☐ A. Delete and ignore them.
☐ B. Contact PayPal using the phone number listed in the email.
☐ C. Login to your PayPal (or Costco) account and check your account status and look for fraudulent transactions in the transaction history.
☐ D. Email or phone PayPal (or Costco) using the contact methods listed on PayPal's website.
☐ E. Both C and D are correct.

* * *

14. How would you recognize whether this is (or is not) a genuine text message from a the US Postal Service:



[Source of image: https://havocshield.com/post/smishing-example]

☐ A. You aren't actually expecting anything from USPS.
☐ B. Your name isn't Emily.
☐ C. You never signed up for text alerts from USPS.
☐ D. The URL link looks suspicious, for (among other reasons) it isn't a USPS domain.
☐ E. All of the above are correct.

* * *

Part 3: Preventing Successful Cyber-Attacks (and Mitigating Damage if/when it Happens)

1. Which of the following are signs that you may have a virus?

☐ A. Mass emails sent to your contact list without your authority
☐ B. Slow performance
☐ C. Unusual pop-ups prompting you to download antivirus and other programs
☐ D. Password changes without your authority
☐ E. Hard drive making continual noise
☐ F. Files missing
☐ G. A change to your website homepage
☐ H. Error messages
☐ I. Computer freezes or crashes
☐ J. Unfamiliar programs start up when you start your computer
☐ K. All of the above are correct.

Recognizing the signs of a virus can – if detected early enough – allow you to take remedial action without major loss of data or other adverse consequences. (Source: https://www.safetydetectives.com/amp/blog/what-is-a-computer-virus-and-how-to-avoid-infection-in/)

* * *

2. Which of these are things you should <u>not</u> do if you detect a virus?

☐ A. Quit any application or software that seems to be affected.
☐ B. Stop shopping, banking, and doing other things online that involve usernames, passwords, or other sensitive information – until you get your device cleared of any virus or malware.
☐ C. Continue using the same passwords as previously.
☐ D. Check to see if you have security software on your device – if not, download and install it.
☐ E. For Windows-based devices, run a virus scan with your security software. (For Macs, go to 'Activity monitor' and search for known Mac viruses such as 'MacDefender', 'MacProtector', or 'MacSecurity'.) Delete any viruses or malware identified.
☐ F. Make sure your software is up to date. Check that all software — the operating system, security software, apps, and more — is up to date. Consider turning on automatic updates so your software always stays up to date.

* * *

3. Turning on your firewall is sufficient to prevent malware attacks, true or false?

☐ A. True
☐ B. False

* * *

4. "Private browsing" is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser.

Does private browsing prevent malware attacks?

☐ A. Yes
☐ B. No

Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?

☐ A. Yes
☐ B. No

* * *

5. If a Scareware window pops up on your computer – for example, a new window pops up stating "Your iPhone has been infected by viruses and malware", telling you to click a green button to "Repair iPhone Now" – and you recognize it (which is good!), is it ok to simply click the "X," "cancel," or "close" button on the pop-up window?

☐ A. No
☐ B. Yes

* * *

6. If you fall for a phishing scam, what should you do to limit the damage?

☐ A. Delete the phishing email.
☐ B. Unplug the computer. This will get rid of any malware.
☐ C. Change any compromised passwords.

* * *

7. What are steps you can take to minimize the risk of a malware or phishing or ransomware attack (and minimize the impact of a successful attack)?

☐ A. Ensure that anti-virus tools are running and up to date
☐ B. All of these answers are correct.
☐ C. Keep your computer software up to date
☐ D. Ensure that you are backing up your critical files

* * *

8. You've inadvertently opened a link or download or open a file contained in a suspicious email and now your computer is behaving strangely. What course of action should you take next?

☐ A. The purpose of a firewall and security software is to block malicious code getting into your computer in the first place, so no further action is needed.
☐ B. Update and run your anti-virus software.
☐ C. Contact your IT help desk or Information Security team.
☐ D. Keep an eye on the performance of your computer.

* * *

9. What does the "https://" at the beginning of a URL denote, as opposed to "http://" (no "s")? And what is its significance to your accessing websites?

☐ A. The site has special high definition.
☐ B. Information that you exchange with that website travels via a secure connection.
☐ C. The site is not accessible to certain computers.
☐ D. None of the above

* * *

10. If a public Wi-Fi network (such as in an airport or coffee shop) requires a password to access (as opposed to being open-access without password to all users), is it generally safe to use that network for sensitive activities such as online banking?

☐ A. Yes, it is safe.
☐ B. No, it is not safe.

* * *

11. How can you identify an unsecure Wi-Fi network?

☐ A. The Wi-Fi is available for free in public places.
☐ B. Does not require a username and password to connect.
☐ C. Not sure.

* * *

12. What actions can you take <u>today</u> to secure your devices, your password-enabled accounts and your personal information and files from snoopers, thieves and other unwanted intruders?

A: Self-Assessment Checklist (of Information Security and Data Privacy Actions)

This is Checklist of basic device and account security measures that you can take to prevent or mitigate the most common data security and privacy vulnerabilities, sort of the "low-hanging fruit" of data security and privacy protection. The Checklist can be accessed here:

https://mstreetlegal.com/privacydatasecurityresources#datasecuritytraining