



Storyboard

OVERVIEW

Course Title:	Phishing Cybersecurity Training
Department:	
Instructional Designer:	Nereida Rondon
Learning Objectives:	Identify the different types of phishing attacks and methods used by cyber criminals
	Recognize the warning signs of a potential phishing attempt
	Recall preventative measures that can be used to avoid Phishing scams
	Determine if an email is safe or a phishing attempt

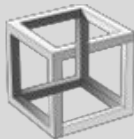
STYLE GUIDE

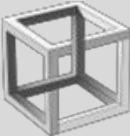
Logos:		
Cover Photo:		
Custom/Brand Colors:		
Color Palette:	<div><div></div> #26DEF2</div> <div><div></div> #ffffff</div> <div><div></div> #05737E</div> <div><div></div> #0A83EB</div>	
Font 1:	Roboto Slab	
Font 2:		
Additional Notes:		

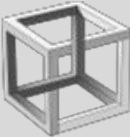
MODULES

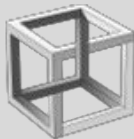
#	Title	Content
1	Intro	Objectives and Definition
2	Types of Phishing	Vishing, Smishing, Common Sign of Email Phishing
3	Identifying Phishing Emails	Phishing video,
4	Signs of Phishing	Urgency, Unknown senders, too good to be true, attachments and hyperlinks
5	Preventative Measures	Ways to prevent being scammed
6	Go Phish Quiz	Determine if the form of communication is a scam or legitimate

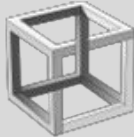


SLIDE	1.1 Title		Image:	
Voice Over (VO):				
Animation Notes:	Title flies in from left			
Programming Notes:				
On-Screen Text (OST):	Phishing Cybersecurity Training			

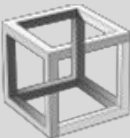
SLIDE	1.2 Objectives		Image:	
Voice Over (VO):			 ABC Global Inc.	
Animation Notes:				
Programming Notes:				
On-Screen Text (OST):	<p>Objectives</p> <ul style="list-style-type: none">● Identify the different types of phishing attacks and methods used by cyber criminals● Recognize the warning signs of a potential phishing attempt and recall how to respond appropriately● Determine if a communication is legitimate or a phishing attempt			

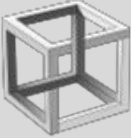

SLIDE	1.3 Definition	Image:	
Voice Over (VO):		 ABC Global Inc.	
Animation Notes:			
Programming Notes:			
On-Screen Text (OST):	<p>Definition</p> <ul style="list-style-type: none">• Phishing is a cyber crime where individuals are targeted via email, text messages or phone calls in order to retrieve private information.• Information acquired can be passwords, documents pertaining to identification, or credit cards and banking information.		

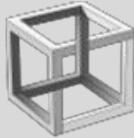
SLIDE	1.4 Phone Calls	Image:	
Voice Over (VO):		 ABC Global Inc.	
Animation Notes:			
Programming Notes:			
On-Screen Text (OST):	<p>Phone Calls</p> <ul style="list-style-type: none">• "Vishing" (Voice Phishing) is the criminal practice of using social engineering over the telephone system to gain access to personal and financial information from the public for the purpose of financial reward.• This method of Phishing aims to verbally coerce a user into revealing sensitive		

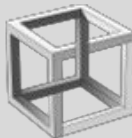

SLIDE	1.5 Text Messages		Image:	
Voice Over (VO):			 ABC Global Inc.	
Animation Notes:				
Programming Notes:				
On-Screen Text (OST):	<p>Text Messages</p> <ul style="list-style-type: none">• Text Message Phishing is also known as "Smishing" (SMS Phishing).• When a "phish" occurs, cybercriminals send deceptive messages that attempt to persuade individuals into clicking harmful links or opening malicious attachments.			


SLIDE	1.6 Examples of "Smishing"		Image:	
Voice Over (VO):			 ABC Global Inc.	
Animation Notes:				
Programming Notes:	Image state scales up on hover			
On-Screen Text (OST):	Examples of "Smishing" Do any of these texts seem suspicious?			

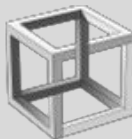

SLIDE	1.7 Email	Image:	
Voice Over (VO):		 ABC Global Inc.	
Animation Notes:	Top layer Swivels on exit at 3.5 seconds to reveal Base layer Shape fly in entrance after 1 second intervals from left, then right, then left, then finally right		
Programming Notes:			
On-Screen Text (OST):	Top layer: What are common signs that an email is a Phishing scam? Base Layer: Email Common signs of a Phishing email are: Shape 1: Unidentified senders. Shape 2: When the email seems too good to be true. Shape 3: There is a sense of urgency for the target to respond. Shape 4: Contains suspicious looking links or attachments.		

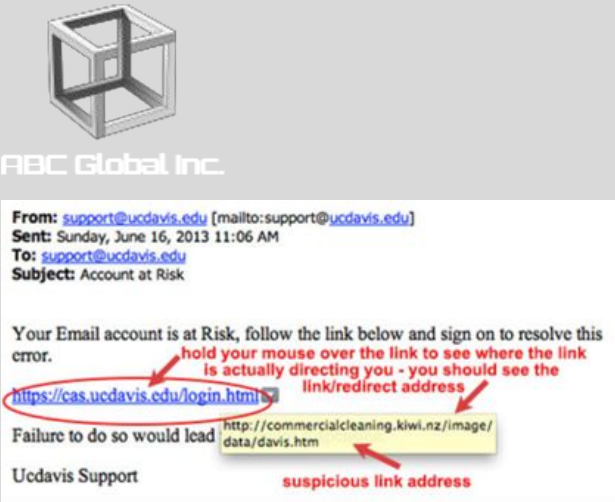
SLIDE	1.8 Identifying Phishing Emails	Image:	
Voice Over (VO):		 ABC Global Inc. 	
Animation Notes:			
Programming Notes:			
On-Screen Text (OST):	Identifying Phishing Emails		

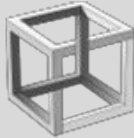

SLIDE	1.9 Identifying Phishing Emails Video		Image:	
Voice Over (VO):			 ABC Global Inc.	
Animation Notes:				
Programming Notes:	Video about Phishing plays on screen			
On-Screen Text (OST):	Identifying Phishing Emails			


SLIDE	1.10 Urgency	Image:	
Voice Over (VO):		 <p>ABC Global Inc.</p> 	
Animation Notes:			
Programming Notes:	Image state scales up on hover		
On-Screen Text (OST):	<p>Urgency</p> <ul style="list-style-type: none">Some email content may pressure you to respond fast or claim that an account or subscription you hold will be suspended.It is beneficial to be mindful of the urgency within an email, this is a primary sign of a Phishing scam.		

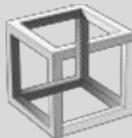
SLIDE	1.11 Unknown Senders	Image:	
Voice Over (VO):		 The screenshot shows an email interface. At the top left is a logo for 'ABC Global Inc.' consisting of a 3D wireframe cube. Below it, the email header reads: 'From: "Virginia Commonwealth University" <ceter.Loeffelmeier@t-online.de>', 'To:', 'Date: 02/26/2012 05:35 PM', and 'Subject: New Secure Message Regarding Your Virginia Commonwealth University Webmail'. A red rectangular box highlights the sender's email address. A red arrow points from this box down to a black-bordered note box that contains the text: 'NOTE that the domain is not a VCU domain but a domain outside of the US'. Below the note box, the email body text reads: 'Dear valued customer,', 'You have 1 new Security Message Alert!', 'Log In into your account to update your profile.', and a blue link 'Click here to Log In'. At the bottom, it says 'Virginia Commonwealth University.'	
Animation Notes:			
Programming Notes:	Image state scales up on hover		
On-Screen Text (OST):	Unknown Senders <ul style="list-style-type: none">• When receiving emails be on alert for unfamiliar senders.• Even if the email is from a known contact, be aware if the content of the email seems out of the ordinary or unexpected, it could be a scheme.		



SLIDE	1.12 Too Good to be True	Image:	
Voice Over (VO):		 ABC Global Inc. 	
Animation Notes:			
Programming Notes:	Image state scales up on hover		
On-Screen Text (OST):	Too Good to be True <ul style="list-style-type: none">Phishing emails can contain promising rewards for the designated target.Suspicious attention-grabbing emails often guarantee the recipients that they will receive items or cash prizes.		

SLIDE	1.13 Attachments & Hyperlinks	Image:	
Voice Over (VO):		 <p>The screenshot shows a phishing email interface. At the top is a 3D wireframe cube logo and the text 'ABC Global Inc.'. Below is an email header: 'From: support@ucdavis.edu [mailto:support@ucdavis.edu]', 'Sent: Sunday, June 16, 2013 11:06 AM', 'To: support@ucdavis.edu', and 'Subject: Account at Risk'. The main body text reads: 'Your Email account is at Risk, follow the link below and sign on to resolve this error.' Below this is a link 'https://cas.ucdavis.edu/login.html' circled in red. A red arrow points to this link with the text 'hold your mouse over the link to see where the link is actually directing you - you should see the link/redirect address'. Below the link is the text 'Failure to do so would lead' followed by a yellow highlighted area containing the URL 'http://commercialcleaning.kiwi.nz/image/data/davis.htm'. A red arrow points to this URL with the text 'suspicious link address'. At the bottom left is the text 'Ucdavis Support'.</p>	
Animation Notes:			
Programming Notes:	Image state scales up on hover		
On-Screen Text (OST):	<p>Attachments & Hyperlinks</p> <ul style="list-style-type: none">• In Phishing emails it is common to see attachments or links requesting your attention.• Be cautious of suspicious looking links or attachments.• Hover over link to see actual URL.		


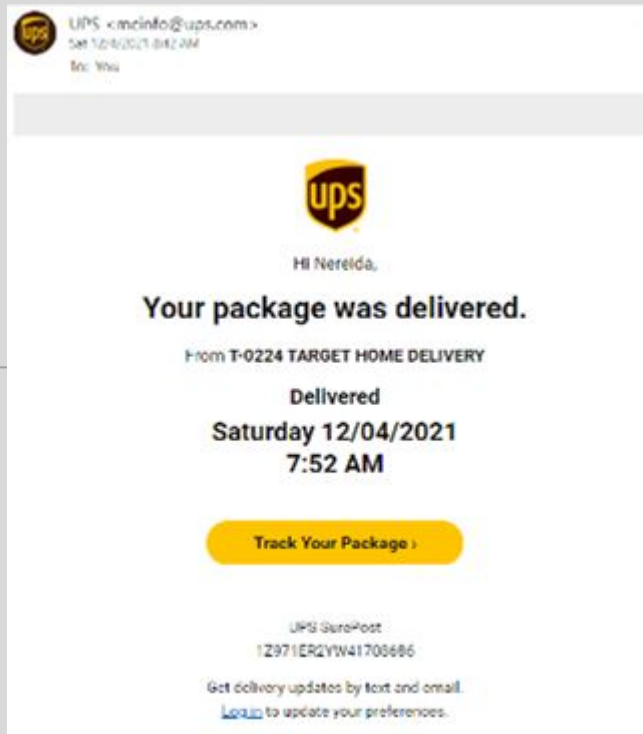
SLIDE	1.14 Preventative Measures		Image:	
Voice Over:			 ABC Global Inc.	
Animation Notes:				
Programming Notes:	Shapes on hover displays info in box Image disappears when shapes are on hover, to display info associated with each shape in box			
On-Screen Text (OST):	Preventative Measures Hover each button for more information Delete Emails Change Passwords Avoid Downloads Configure Browser Settings Spam Filters Avoid Public Networks Check URLs Awareness			


SLIDE	1.15 Go Phish	Image:	
Voice Over (VO):			
Animation Notes:			
Programming Notes:	<p>Start Button, on click displays an image</p> <p>Phish Button, learner selects if scam</p> <p>Safe Button, learner selects if safe</p> <p>Image state scales up on hover</p> <p>Score % shape</p>		
On-Screen Text (OST):	<p>Go Phish</p> <p>Catch as many fish as you can. Determine whether the communication is a phishing scam or if it's legitimate. Click the correct answer. Don't run out of time.</p>		

SLIDE	1.16 Results		Image:	
Voice Over (VO):			 ABC Global Inc.	
Animation Notes:				
Programming Notes:	Submit button , completes course and restarts course Correct answer: Correct! Fish appears on fish line Incorrect answer: Sorry, you didn't catch that fish!			
On-Screen Text (OST):	Results: Your Score: % Passing Score: % Result: Success Layer: Congratulations, you passed. Failure Layer: You did not pass.			

ASSESSMENT		
#	ANSWER	QUESTION
1	Phish	 
2	Phish	

ASSESSMENT		
#	ANSWER	QUESTION
3	Safe	<div data-bbox="415 218 981 757" data-label="Image"> <p>Amazon.com <auto-confirm@amazon.com> Reply-To: no-reply@amazon.com To: Nery0524@gmail.com</p> <p>amazon Order Confirmation</p> <p>Hello Nereida,</p> <p>Thank you for shopping with us. We'll send a confirmation when your item ships.</p> <p>Details</p> <p>Order #111-2308333-5070660</p> <p>Arriving tomorrow, February 13</p> <p>Ship to: Jose LEHIGH ACRES, FL</p> <p>View or manage order</p> <p>Order Total: \$14.90</p> </div>
4	Phish	<div data-bbox="1068 477 1796 1042" data-label="Image"> <p>Wells Fargo Online.</p> <p>WV Wells Verification <wfbank.connect.auth@t-online.de> no-reply.message@wellsfargo.com Tuesday, April 9, 2019 at 9:52 AM Show Details</p> <p>To protect your privacy, some pictures in this message were not downloaded.</p> <p>Wells Fargo wellsfargo.com</p> <p>Verify Your Account</p> <p>Dear Customer</p> <p>During our safety inspection we noticed that your account has not been completely verified and protected, so we require you to verify some of your information in order to automatically secure and encrypt your account with the latest update.</p> <p>Verify your account now by signing in to wellsfargo.com/update.</p> <p>Failure to verify your account immediately might lead to the temporary suspension/restriction of your account.</p> <p>Thank you. We appreciate Your Compliance.</p> <p>Wells Fargo Online Customer Service</p> <p>wellsfargo.com Fraud Information Center</p> <p>ec3ac241-6f58-432f-a86c-83cb93be0c60</p> </div>

ASSESSMENT		
#	ANSWER	QUESTION
5	Phish	 <p>The screenshot shows a text message conversation on a mobile phone. The contact is named 'Apple'. The message is a 'Text Message' received 'Today 14:40'. The content of the message is a 'Final Notification' stating: 'Your Apple ID is due to expire today. Prevent this by confirming your Apple ID at http://update-apple.uk'. The message is signed 'Apple Inc'.</p>
6	Safe	 <p>The screenshot shows an email from UPS. The header includes the UPS logo, the email address 'UPS <mcinfo@ups.com>', and the date 'Sat 12/4/2021 8:42 AM'. The body of the email says 'Hi Nereida,' followed by 'Your package was delivered.' Below this, it specifies 'From T-0224 TARGET HOME DELIVERY', 'Delivered Saturday 12/04/2021 7:52 AM', and a yellow button that says 'Track Your Package >'. At the bottom, it mentions 'UPS SurePost 1Z971ER2YW41703686' and provides a link to 'Get delivery updates by text and email. Login to update your preferences.'</p>

ASSESSMENT		
#	ANSWER	QUESTION
7	Phish	 <p>donation of Euro 2,000,000.00</p> <p>charles jackson Sat 2/12/2022 2:45 AM To: Recipients Hello</p> <p>I am Charles W. Jackson jr the mega winner of a \$344M Powerball jackpot in the USA, I'm donating to 5 random individuals if you get this email then your email was selected. I have spread most of my wealth over a number of charities and organisations. I have voluntarily decided to donate the sum of €2 Million to you as one of the selected 5.</p> <p>Hope to make you and your family happy.</p> <p>Regards Charles W. Jackson jr.</p>
8	Phish	

ASSESSMENT

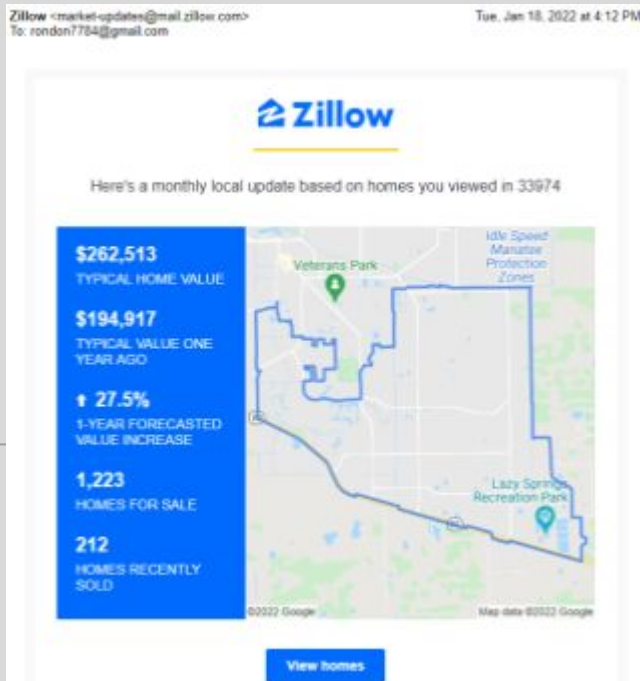
#

ANSWER

QUESTION

9

Safe



10

Phish

You have been selected!

Your chance! <sdhxnab@ogame-private-server-list.info>

Mon 2/7/2022 12:37 PM

To: sh3xm9sv <sdhxnab@ogame-private-server-list.info>

Thank you
for shopping with us

Dear customer,

Congratulations! We would like to offer you a unique opportunity to receive a brand new **Dyson V11i**! To claim, simply take this short survey about your experience with us.

Your opinion is very valuable. Click **OK** to begin

OK

[unsubscribe here](#)

The advertiser does not manage your subscription.
If you prefer not to receive further communication please unsubscribe [here](#)
Or write to: 6181 Long Prairie Rd Ste 744 #511, Flower Mound, TX, 75028