HORIZON FOUNDATION ANALYSIS RESULTS

Connie Malamed

[Company name]

[Date]

HORIZON FOUNDATION ANALYSIS RESULTS

Contents

NEEDS ANALYSIS

Introduction

This needs analysis summarises the findings completed for the Horizon Foundation regarding last year's phishing event which resulted in a data breach of 45 000 donors' personal information. It explores the requirements to prevent vulnerability to future phishing attacks.

The Problem

Phishing scams over the past few years have become more sophisticated and harder to detect. Last year's data breach at Horizon resulted in loss of income, donor trust and donor subscriptions.

With a diverse and distributed workforce, Horizon is vulnerable to email data breaches. There are 2 primary causes of the data breach:

1. Employee awareness of:
- Role in email security issues – understanding potential financial and reputation impacts of phishing attacks and taking an active role in defending again attacks.
- Protocol for managing suspicious emails.
- Repercussions of following link and opening attachments in phishing emails.

2. Horizon's email security systems. Horizon has undertaken steps to strengthened firewalls, internet security and email filtering. Testing and verification of the efficacy of these measures is required.

The Goals

Horizon Foundation are committed to

- preventing future data breaches
- securing donors' personal information
- reducing security risks
- rebuilding donor trust that personal data is safe
- increasing donations to levels prior to the data breach
- improving employee vigilance against phishing emails and commitment to data security

Horizon Foundation expect to achieve these goals in 2 ways.

1. Through educating employees in email security, including:
- understanding the risk and impact of phishing emails
- recognising phishing emails
- eliminating clicking on links or attachments in phishing emails
- reporting procedures for suspicious emails
2. Strengthening firewalls, internet security and email filtering. Install AI software to detect suspicious emails.

The Performance Gap

Performance gaps were identified through employee surveys and interviews. The following performance gaps were identified.

Skills and Knowledge	Expected Performance	Actual Performance
Identify risks associated with phishing emails	Describes what phishing is and names common risks	• Minimal knowledge of phishing or its risks • Do not identify risks associated with phishing emails because staff are not aware of the repercussions of the data breach at Horizon – they have no personalised context
Value role in email security and actively monitor email for scams	Reads email with commitment to data security. Takes time to identify and manage suspicious emails.	• Rush through emails with little attention to scams or suspicious email clues • Staff may be busy, lack motivation or may not recognise their role in defending Horizon's data security
Identify suspicious email	Recognise key attributes of suspicious emails	• Open all emails. Cannot recognise suspicious emails • Can identify some phishing emails, but not more sophisticated ones. Over the past few years, cyber criminals have become more sophisticated in designing effective phishing emails. This not only puts Horizon at risk, but also staff themselves. Identity theft is a serious risk
Follow Horizon's email security policy and procedure by reporting suspicious emails	Follow key steps in email security policy and procedure. Reports suspicious emails. Does not open suspicious links or attachments	• Little recognition of Horizon's email security P&P • Open links and attachments in email • Do not follow through on reporting suspicious emails as required by Horizon's email security policy and procedure because they are unaware of it. Training happened a long time ago, and many staff are unsure of how to check the P&P, so they simply delete suspicious emails and hope the problem goes away

Training as a Solution

Although we will need to conduct further analysis to determine the type of training and delivery solution that will be most effective, we agree that training will help the Horizon Foundation meet its performance and business goals.

While IT solutions to increase email security is an essential first step, the strongest defence is additional and repeated employee training in email protocols in recognising and avoiding phishing emails. Training should be followed up with in-house phishing emails to measure effectiveness of training.

Initial analysis indicates the following training is required:

- Timely follow-up training after onboarding on email security
- Review of Horizon's email security policy and procedure
- Building personal commitment to guarding data security
- Phishing risk awareness
- Concrete steps for successfully avoiding phishing emails
- Practice identifying phishing emails

AUDIENCE ANALYSIS

Introduction

This audience analysis summarises the staff interview and survey results collected from clinical staff at the Horizon Foundation. The analysis aims to draw conclusions about the audience which will help us design an effective training solution for Horizon's email security issues.

Overview of Our Approach

The IT team reported that previous email breaches resulted primarily from clinical staff using mobile phones. The training design team undertook 2 data collection methods to gather information on clinical employees' training needs.

1. **Staff surveys**
   We distributed the online survey to all clinical staff at Horizon and collected 7 500 responses which represents 30% of clinical staff. Responses represented all field locations and was a representative distribution of clinical positions and tenure.
2. **Staff interviews**
   We interviewed a representative group of 60 clinical staff via Zoom. The goal of the interviews was to better understand work environment, awareness of email security and attitude regarding training on this subject.
3. **2 key staff profiles**
   In the following section, we identify 2 key staff profiles which represent the respondents' responsiveness to training. These profiles will be used to guide the training design content and approach.

Data Trends

After analysing the data, we identified emerging trends and their training implications.

Data Trend (of clinical staff)	Training Requirement
75% access email on mobile phones	• Largest focus on phishing risks on phones. As 75% of staff use phones for email, training should focus on the actual device used • Review onboarding training to confirm it focuses on mobile phone use
61% do not remember undertaking internet security training during onboarding	• All staff should undergo email security training / retraining • A series of 'booster' training sessions after initial retraining will aid staff in retaining key info • Review onboarding email security training for efficiency – determine what, if any, parts can

	be reused. Determine efficacy of timing – e.g. better week after onboarding?
31% were unaware of Horizon's data breach	● While this is outside the scope of this training, it is recommended Horizon review their staff communication strategy to ensure a range of communication tools and mediums reach all staff
59% do not know Horizon's procedures for open emails	● Review email protocols in training
Highly varied demographic base comprised largely of native English speakers with higher ed qualifications from variety of religious backgrounds	● Sensitivity to cultural and religious difference. Use respectful, unbiased language – recommend trialling and feedback from staff before launch ● Use neutral pronouns ● Avoid technical / technology jargon ● Communication pitched at higher ed-level readers
Motivated to help others and making a positive contribution	● Focus on the human experience. Relate internet security training to staff values in helping others – e.g. the negative repercussions of phishing emails ● Use narratives and examples staff can relate to. Staff are motivated by how their work helps protect Horizon from attack and their role in preserving donor trust
Many staff are stressed by low bandwidth	● Provide release time to undertake training ● Consider some face-to-face training to ensure all staff have time to complete it - This would have the side benefit of a team building opportunity ● Follow up training with short, concise, contextualised knowledge checks or "Phishing Challenges"
75% believe they can recognise phishing emails. Therefore, attitude toward email security training is neutral to negative.	● Focus on how phishing emails have become sophisticated and hard to detect ● Open with examples of really successful phishing emails or show how they've changed over time– this may help to focus staff on how phishing has changed ● Follow up with IT sending 'in-house phishing emails". Provide personalised feedback to staff you click on these emails. Identify staff for further training.

Horizon was negatively impacted by a data breach resulting in loss of income, donor confidence and support. Therefore, a multi-pronged approach to staff training is recommended including:

1. Reviewing Horizon's email policies and procedures
2. Reviewing Horizon's communication strategy to ensure all staff are informed about new phishing attacks
3. Global staff training to practice recognising the risks and attributes of phishing emails
4. Post-training IT solution: Testing staff's ability to recognise phishing emails with in-house phishing simulations

CLINICIAN PERSONA 1

Name: Technophile

Descriptor: New recruit Nurse. Highly adaptable and flexible. Ambitious.

Quote: Phishing emails are so obvious. I'm not sure how this could be a problem.

Who is it?	Clinical Field Nurse at various centres around South Africa. First nursing position. 2 years in the role. Highly skilled in technology with avid interest in online gaming
Goals	To move into management at Horizon or other NGO. Wants to make a difference in worldwide healthcare access.
Challenges	Not enough time for patient care as still learning the ropes and traveling between clinics takes a lot of time.
Values	Strongly committed to improving access to healthcare, and improving the lives of families.
Attitude toward Training	I'm okay with it if we can keep getting donations! But it doesn't feel personally relevant.

CLINICIAN PERSONA 2

Name: Technophobe

Descriptor: Highly skilled and experienced nurse. Great team-player. Often behind in paperwork and responding to emails.

Quote: This is an IT problem. Can't they fix it?

Who is it?	Clinical Nurse at clinic in Chang Mai, Thailand. 20 years experience, last 7 years with Horizon.
Goals	To be a highly skilled nurse and develop clinical skills.
Challenges	Highly focused on clinical skills. Due to time constraints and interest level, is not
Values	Helping patients. Knowing that I make a difference. Wants to follow Horizon's procedures, though not always aware of them.
Attitude toward Training	Is fearful of technology and looking 'behind the times'. Is concerned that they will fail the training or look stupid in front of colleagues. Is concerned about when they could complete the training as the days are already so full and works a lot of overtime.

Instructional Analysis

Goals

- Data breaches from email will decrease to less than 1% within 3 months of training as all clinical staff follow Horizon's email policies and procedures.
- Reporting suspicious emails to IT will increase by 85% within 3 months of training.
- Staff will be confident and motivated to identify and defend Horizon against phishing emails. This will be measured through training feedback surveys by achieving an 80% satisfaction score.

Expected behaviours (i.e. What do people need to do?)

1. Identify risks associated with phishing emails.
2. Staff value their role in email security and actively monitor email for scams.
3. Identify suspicious emails.
4. Follow Horizon's email security policy and procedure by reporting suspicious emails to IT.

Solutions (i.e. What changes will help them)

Tool	Solution	Responsibility	Timeframe
Job Aid	Create infographic on identifying common features of phishing emails. Revise the email security policy and procedure – ensure it focuses on mobile phone use as 75% of staff actually use phones for email. Ensure info is concise and up-to-date. Provide this as a job aid.	IT & HR	1 month
Communication Strategy	Review the Horizon communication strategy – are they reaching all staff? What are employees' preferred form of communication and updates – newsletter, staff portal, email? How frequently does Horizon communicate with staff? How frequently do staff want to be communicated with?	HR	3-6 months
Training 1	**Phishing Risks** Create practice activity to identify phishing risks to companies and individuals. Use real-world examples of the repercussions of phishing scams – including Horizon's recent data breach. Build on personal role in ensuring data security.	ID Team, HR and IT as SMEs	3-4 months

Training 2	**Phishing Examples** Create practice exercises in which staff need to recognise salient features of phishing emails – make the practice move from easier to harder. This approach will build staff confidence and gamify the experience to make it more enjoyable and engaging.	ID Team, HR and IT as SMEs	5-6 months
Training 3	**Phishing Responses** Create practice activity to test knowledge of what to do when staff receive a phishing email. The activity could provide a variety of scenarios with actions staff commonly take – participants are provided with feedback as they make decisions.	ID Team, HR and IT as SMEs	7-8 months
Post-Training in-house phishing emails	**In-house phishing emails** IT staff send in-house phishing emails to identify percentage of staff who recognise and report suspicious emails vs staff who require further training	IT & HR	9-12 months

Instructional Map – Skills and Knowledge

Data breaches from email will decrease to less than 1% within the next 3 months as all clinical staff follow Horizon's email policies and procedures.

Identify risks associated with phishing emails & role in preserving data security

Identify features of suspicious emails

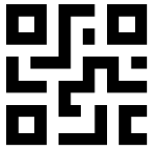
Follow Horizon's email policies and procedures when they encounter suspicious emails

practice activity identifying phishing risks to companies and individuals with real-world e.g. of repercussions of phishing scams – e.g. Horizon's recent data breach

practice activity recognising features of phishing emails – moves from easier to harder e.g. to build staff confidence and gamify the experience to make it more enjoyable and

practice activity reporting phishing emails. Scenarios with decision to / not to report with feedback on results as they make decisions

Staff email / release on recent data breach at Horizon
CTA to follow Horizon's updates



CTA to follow Horizon's updates

Horizon's email security P&P

Horizon Phishing Training Design Plan

Brief Introduction

Horizon is committed to keeping donor's personal information safe and secure. To achieve this goal, Horizon will provide staff with the following training:

1. Identify phishing email risks and their role in keeping data secure.
2. Identifying suspicious emails and their common attributes.
3. Follow Horizon's email policies and procedures for reporting suspicious emails.

Evaluation Plan

- Successful completion (80%) on Quizzes 1 & 3 and Assessment 2, parts 1 & 2.
- Participant feedback survey with 80% satisfaction with training.
- Follow up in-house phishing emails will have an 85% reporting rate and 1% click rate.

Training Design Matrix

Performance Goal: Staff will identify and report phishing emails.

PERFORMANCE OBJECTIVES	SUPPORTING CONTENT	INSTRUCTIONAL STRATEGY/TREATMENT
1.0 Staff will identify phishing email risks and their role in keeping data secure.		This lesson will provide participants with real examples of companies that experienced loss – financial, legal, reputational – from data breaches due to phishing emails. Staff will see their role by observing the consequences.
1.1 Identify potential negative consequences of opening phishing emails.	• Real-world examples of consequences of data breaches due to phishing emails • Testimonial from Horizon donors on the effect the data breach and their willingness to continue donating	Presentation • 6 real-world examples of personal and corporate harm from phishing attacks. • Brief overview of real world scams and features of how they worked. Quiz 1 • Participants have to select the real-world consequences e.g. How much money did company X lose in the phishing attach? A) $10M B) $30M C) $50M – participants guess and then see results.
1.2 Identify how phishing emails work to collect personal data • Sharing passwords for access to server	• Examples of common phishing features and their goals/outcomes in parts of emails	Quiz 1 cont. • Participants will be presented with phishing emails and participants select the outcome e.g. An email warns you to

PERFORMANCE OBJECTIVES	SUPPORTING CONTENT	INSTRUCTIONAL STRATEGY/TREATMENT
• Sharing personal information for identity fraud • Transferring money • Downloading ransomware or malware		change your password. What is this email trying to accomplish? A) access your company's files B) collect your password C) Keep you safe
2.0 Staff will identify features of suspicious emails and report to Horizon IT centre within 2 days of receiving them. Please refer to storyboard and protype link below.		In this lesson, participants will examine phishing emails and identify the specific feature that is suspicious. They then decide whether to report a series of 6 emails.
2.1 Identify features of suspicious emails, including • Incorrect email address • Incorrect urls • Urgency calls to action • Spelling errors • Odd grammar and phrasing	• Examples of phishing emails • Explanations of suspicious parts	Phishing Infographic: 6 common signs of phishing (see storyboard below) • Present top 6 features of phishing emails Assessment: Phishing Game & Report (see storyboard below) • 6 examples of whole emails with phishing attributes – odd URL addresses, links, urgency, etc. All game emails are phishing. Users identify and explain the parts of the email that makes them suspicious. Players get a point for each part they correctly identify. • Participants monitor their email for phishing emails. They analyse, research and report on a phishing email they receive. They identify the appropriate action they took to manage the email.

PERFORMANCE OBJECTIVES	SUPPORTING CONTENT	INSTRUCTIONAL STRATEGY/TREATMENT
2.2 Follow Horizon procedures for reporting suspicious emails	• Mix of phishing and non-phishing emails • Horizon email security P&P	Quiz 2 • 6 examples of phishing and non-phishing emails. Participants decide if they should report the email and why.

Storyboards for 2.1 Identify features of suspicious emails

Phishing Infographic: 6 common signs of phishing

This Infographic is designed to be easily understood by people with a range of technical skills. Often the people most vulnerable to phishing attacks are people with limited experience or confidence using email, particularly online advertising, payments and banking info. This infographic is designed to be accessible to all to help improve awareness of and vigilance against scams.

This infographic was designed with accessibility and equality in mind, including:

- Language is plain English. Despite the technical nature of the content, every attempt was made to explain topics in simple, easy to understand terms.
- Glossary of terms provided for common phishing terms
- Icons help readers identify key information
- Essential information is presented for quick understanding. Users can tap interactive elements to learn more.
- Navigation is free-form to allow users to focus on most important information for them.
- Accessible – formatted for mobile and laptop
- Accessible – images have alt tags
- Gender and identity – All explanations use gender-neutral pronouns
- Avoids use of blue and green for colour blind viewers
- Uses responsive images for mobile viewing

You can view the prototype at
Version 1 - https://view.genial.ly/607f855a3cd945101f1890c6/interactive-content-6-common-signs-of-phishing
Version 2 - https://view.genial.ly/6080b5cbd6512b1026c59797/interactive-content-6-signs-of-phishing

Slide Title: Infographic, Page 1

6 Common Signs of Phishing

We all get unsolicited emails every day. Most are harmless advertising. Some are dangerous phishing scams. Phishing scammers pose as a company or person you trust. They try to trick you to:

1. Share personal information such as passwords, credit card details, banking information.
2. Download software to your computer such as malware, spyware or ransomware.

Outsmart scammers when you spot the 6 common signs of phishing.

(plus icon) Use this icon to Learn More (star icon) Use this icon for Tips

1. **Generic email: Legitimate companies use company domains**

   (plus icon)

   What to watch for:

   - Sender's email address doesn't match the person or company – e.g. companies don't use gmail
   - Sender's email address is misspelled
   - Sender's company is unknown – e.g. you do not use their services
   - Email sent at an unusual time outside of business hours
   - Company logo is incorrect or missing

   (Image)

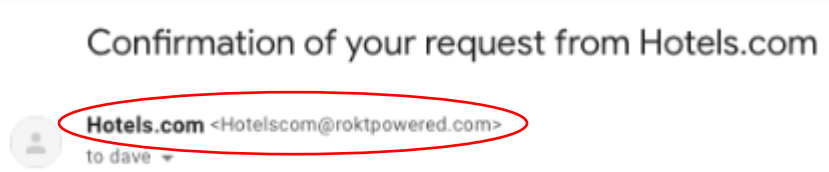


Figure 1 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

(star icon)

TIP: Hover your mouse over the from address and check that the domain is correct with no spelling errors, alterations or numbers

TIP: Common phishing scams pose as banks, law enforcement, postal and delivery services, government agencies, billing companies. Do an internet search to confirm correct URLs.

Programming / Interactions

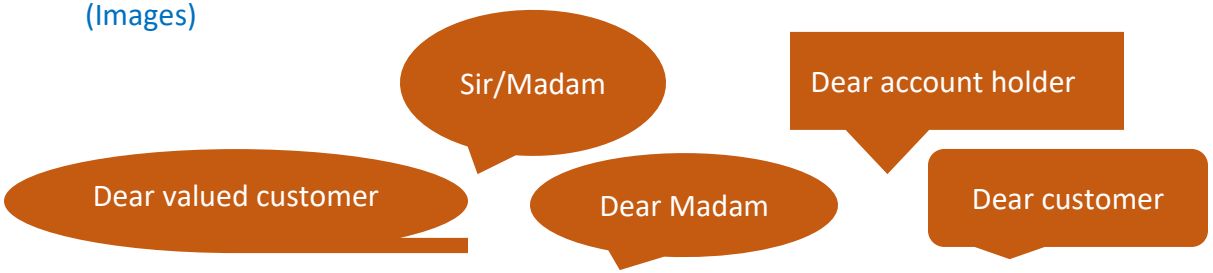
- (plus icon) On click opens lightbox with "What to watch for" explanations of attribute
- (star icon) On hovers displays tips on how to avoid phishing
- (Book icon) On click opens Phishing Vocabulary
- (star icon) On click opens Page 2

Reviewer Comments

- many words would be unknown to some people, especially vulnerable people, like my mother
- Darken text to improve contrast and visibility

2. **Generic Greetings: Legitimate companies know your name**
   (plus icon)
   What to watch for:
   - Generic greeting
   - No greeting or salutation

   (Images)



3. **Alarming, Urgent or Too Good to Be True: Message baits you to take immediate action**
   (plus icon)
   What to watch for:
   - Subject line is unusual, urgent or doesn't match the message
   - Message is too good to be true - Offers prizes or unbelievable promotions – e.g. *New payment on your account*
   - Message is alarming – requires you to click a link or download attachment to avoid negative action – e.g. *suspicious activity on your account*
   - Message is urgent - requires you to take action now or within a short time e.g. *your account has been hacked*
   - Email is unexpected - email is a reply to a message you didn't send or request

   (image)

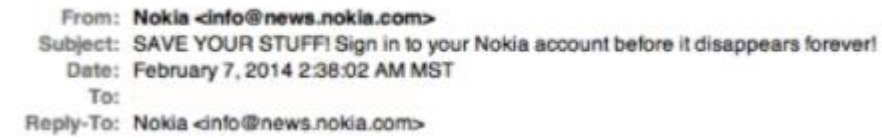

From: **Nokia <info@news.nokia.com>**
Subject: SAVE YOUR STUFF! Sign in to your Nokia account before it disappears forever!
Date: February 7, 2014 2:38:02 AM MST
To:
Reply-To: Nokia <info@news.nokia.com>

Figure 2 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

4. **Oddly worded with errors: Legitimate companies know how to write clearly and correctly.**

(plus icon)

What to watch for:

- Spelling, punctuation and grammar errors
- Out of character for the sender – e.g. your CEO asks you to send money

(Image)

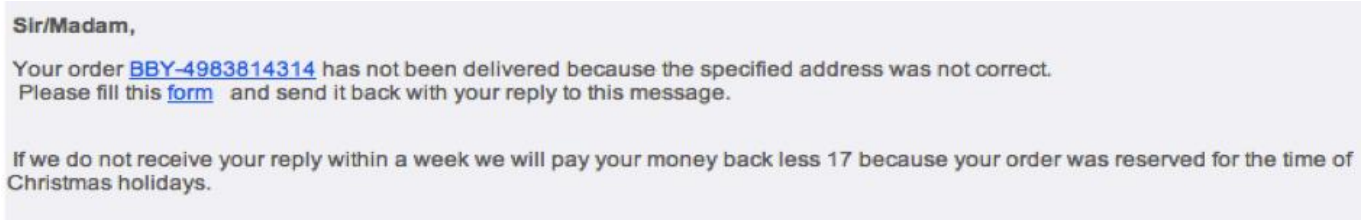


Figure 3 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

(star icon)

TIP: Trust your hunches. Does this sound like a message the sender would write?

5. **Fraudulent Links: Incorrect links try to force you to an unknown website**

(plus icon)

What to watch for:

- Links don't match company URL
- Links are misspelled
- The entire email is a link
- No alternate form of contact info provided

(Image)

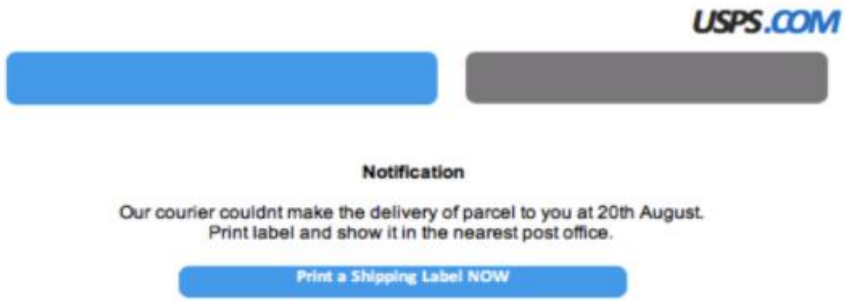


Figure 4 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

(star icon)
TIP: Hover over links to see if the URL is different from the link text or the company's domain
TIP: Secure links start with https:// NOT http://
TIP: If in doubt, ignore the link. Login to the official company website directly and check your account.

6. **Unexpected Attachments**

(plus icon)
What to watch for:

- Unexpected or unsolicited attachments
- Unusual attachment that doesn't match the message
- Attachment claims it is a picture of you or people you know

(Image)
To continue using our services plese download the file attached and update your login information.

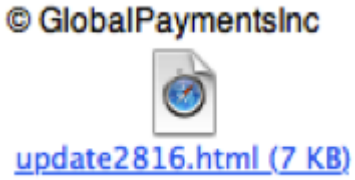


Figure 5 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

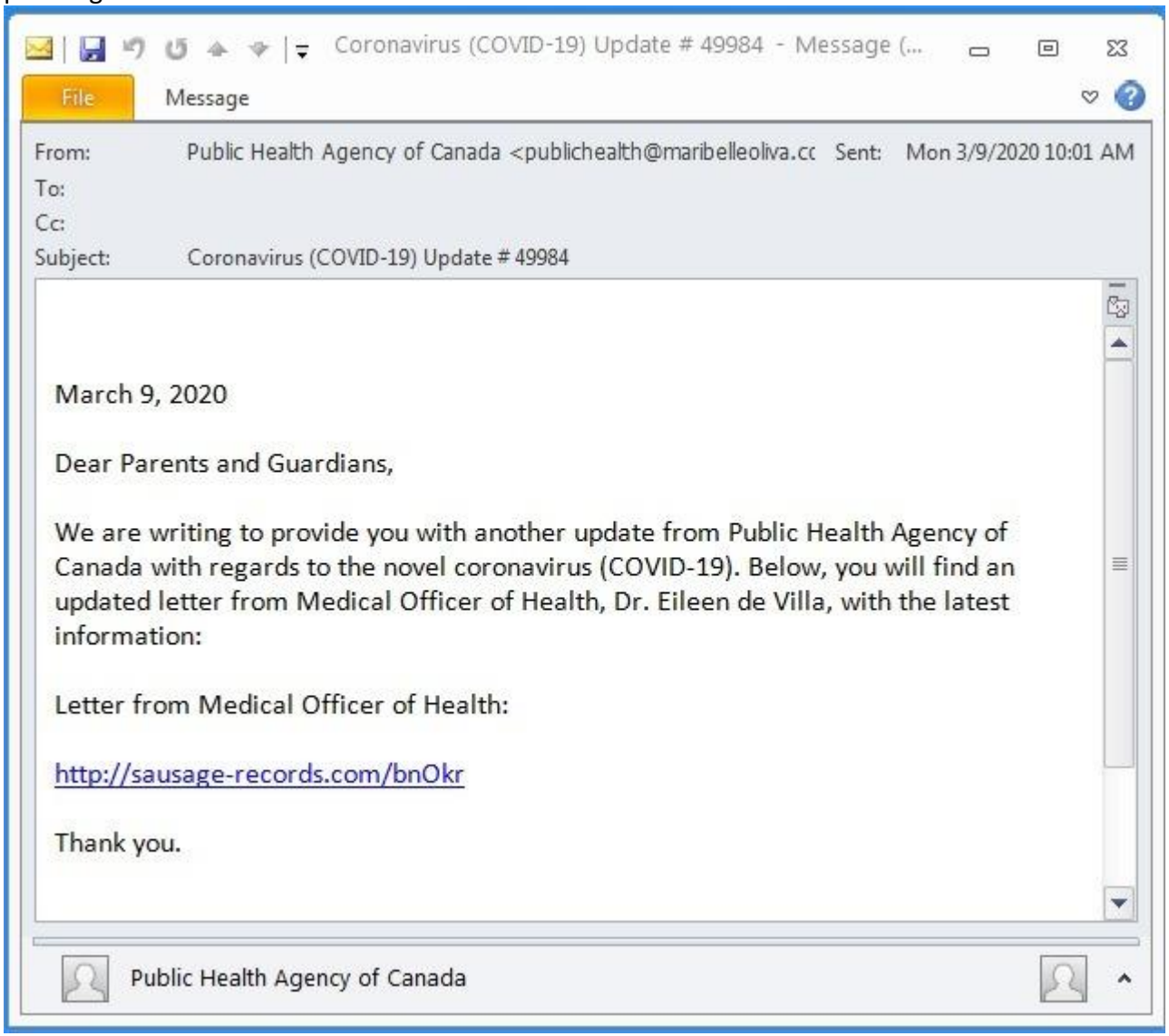
(star icon)
TIP: If in doubt, contact the company directly from their website, not the email
TIP: The only safe attachment is a .txt file

(Book icon) Phishing Vocabulary (star icon) See example

Report phishing scams to the ACCC Scam Watch at https://www.scamwatch.gov.au/report-a-scam

Phishing Vocabulary

- Domains – A group of online websites, pages or resources that belong to a specific group, company or individual.
- Legitimate – Follows laws or rules
- Malware - software that damages or disables computers and computer systems.
- Ransomware - software that blocks access to computer files until a sum of money is paid.
- Salutations – greeting
- Scammer – Dishonest person
- Scams – Dishonest plan or fraud
- Spyware – software that allows a user to access private information on another person's computer.
- Unsolicited – not asked for or requested
- URL - An address on a World Wide Web page

Slide Title: Infographic, Page 2	**Programming / Interactions**
Phishing scams increase during crises because people are already vulnerable and anxious. Here is a COVID-19 phishing scam.  *Figure 6 from https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html* (explanations) email address is not from the Canadian government Generic greeting	- (explanations) to be placed above and below image of example email in textboxes

No Canadian government logo Message contains no contact info or helpline numbers. No grammatical errors BUT, the phrasing does not match a government agency http link. Secure links are https Odd link name No sign off – Who wrote the email?	

Assessment: Phishing Game & Report

The Assessment: Phishing Game and Report are designed as Train-the-trainer activities.

Part 1: The Phishing Game is designed to be played with staff responsible for phishing training at each Horizon clinic globally. It can be reused as a training activity with Horizon staff in distributed clinics. As an interactive PowerPoint, the Phishing Game is designed to be played in person, or in a live, online meetings.

Part 2: The Phishing Report encourages trainers to be more critical when reading emails. It requires staff to independently identify, research and report phishing emails.

The Phishing Game and Report can be assigned in the same training session. However, the time to complete Part 2 will vary as staff actively monitor their emails, vigilantly looking for phishing scams. They may report phishing emails they find in either their work or personal email. The goal is to monitor, analyse and report phishing emails.

You can view the prototype in the attached Phishing Game PowerPoint.

Trainers' Guide

Visuals and Text

Part 1: Phishing Game

Participants: 2 players

Time: 1 hour

Trainer Instructions:

The Phishing Game is designed for face-to-face training in a corporate, college or school setting. Players are placed in teams of 2 players. Pairs analyse phishing emails together to identify and explain all attributes of the phishing email. Teams receive one point for each attribute they correctly identify.

1. Print 1 game board and 1 set of cards for each pair.
2. Ask learners to read through game instructions and commence playing.
3. Give teams 1 hour to analyse all 6 phishing emails and describe the phishing attributes.
4. Monitor learners and resolve any questions or challenges that arise. You may award additional points if a team adequately demonstrates knowledge of phishing attributes.
5. At the end of the hour, collect the team scores to complete the Rubric, Part 1.

Part 2: Research, analyse and report on a phishing email

500 words

In this activity, learners will identify and analyse a phishing email they received. They must present a screenshot of the suspected email. They must analyse the parts of the email that are suspicious. They will explain why each of the parts identified is suspicious. They will then conduct research to determine if the email is a phishing email. They must provide evidence of their research. Lastly, they must explain what action they took on the email.

Criteria

- Recognise phishing emails.
- Identify attributes of phishing emails.
- Analyse and explain the specific attributes of phishing emails.
- Conduct research to confirm if it is a phishing email.
- Take appropriate action on phishing emails.

Rubric

Concerns	Criteria	Competency
	Assessment Part 1 Identified 80% or 19/24 attributes of phishing emails in the Phishing Game.	
	Assessment Part 2 Correctly explained the attributes of the phishing emails.	
	Assessment Part 2 Undertook research to confirmed of refuted if the email was phishing.	
	Assessment Part 2 Described appropriate action to take with email.	

Phishing Game: Assessment Instructions

Visuals and Text

Part 1: Phishing Game

Participants: 2-3 players

Time: 1 hour

Player Instructions:

In this game, there are 6 phishing emails. To win the game, you must identify all of the suspicious parts and explain why they are suspicious. You will get a point for each part you describe correctly.

1. Place your marker on the "Start" square. Make your game marker with a paper-ball, eraser or other small object.
2. Place the phishing cards Question-side up in the centre of the board. Answer-side has the fish image.
3. Take a phishing card from the centre of the board. *Do not turn the card over until you have finished answering the questions.
4. Read the phishing email.
5. Underline of highlight the suspicious parts.
6. Describe why it is suspicious in the spaces provided.
7. Turn over the card and read the answers.
8. For each correct answer, move your marker one spot forward. e.g. 4 correct answers, move forward 4 spaces.
9. When you are finished all phishing cards, report your score to the trainer.

If you identify any answers not provided on the answers card, your trainer will make the final decision on points.

Part 2: Research, analyse and report on a phishing email

500 words

In this activity, you will identify and analyse a phishing email you received.

1. Monitor your emails for phishing scams. Be careful not to click any links or download any attachments!
2. Take a screenshot of the phishing email.
3. Analyse the parts of the email that are suspicious.
4. Explain why each of the parts you identified is suspicious.
5. Conduct research to determine if the email is a phishing email. Provide evidence of your research such as a URL.
6. Explain and justify what action you took on the email.

Phishing Game: Game Board

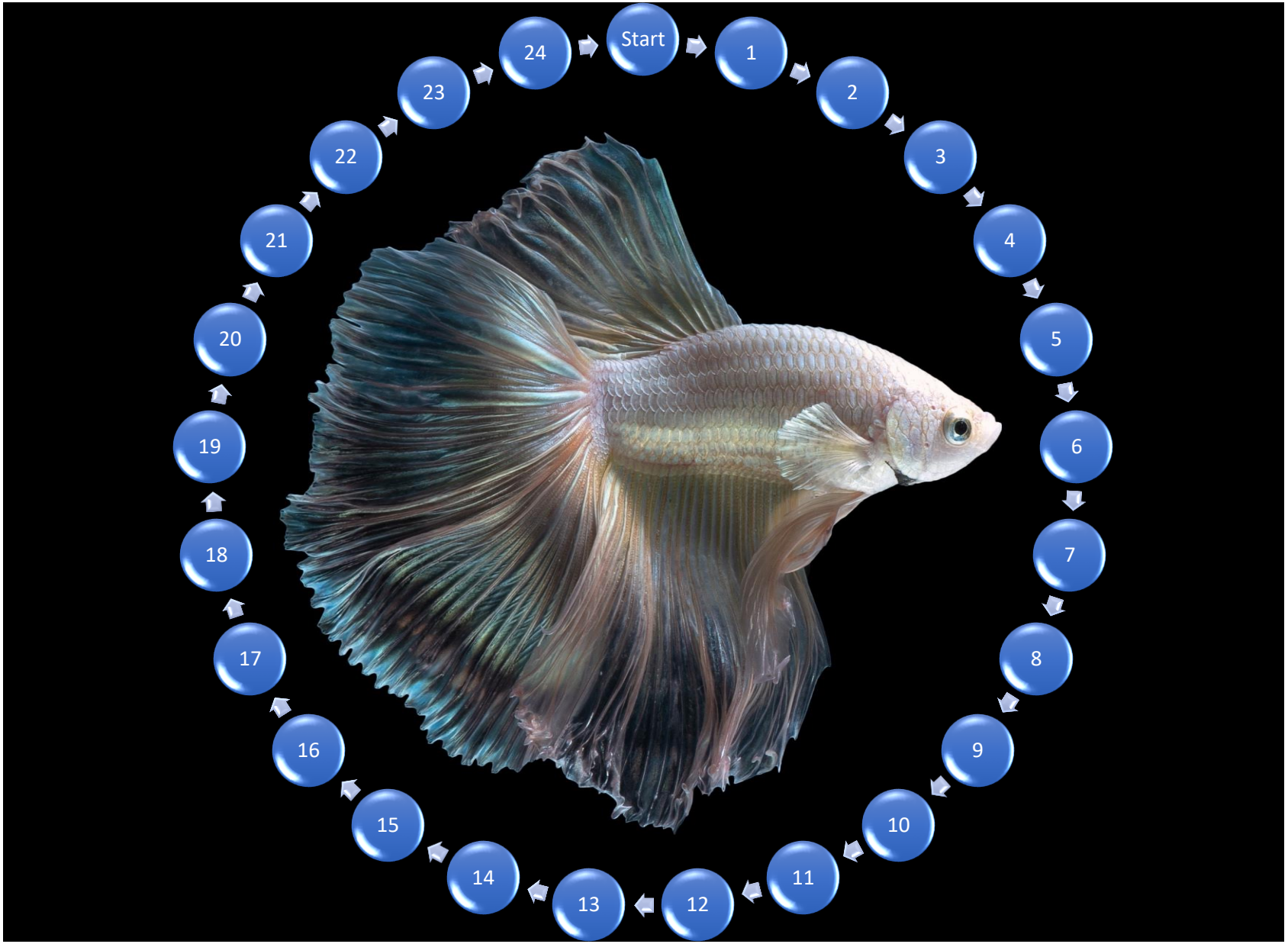


Figure 7 Image from Microsoft Word

This is a mock-up of the game board.

Phishing Game: Game Card 1

Card front

Question Card

From: GlobalPay <VT@globalpay.com> Hide
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

1 Attachment, 7 KB Save ▾ Quick Look

Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services plese download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

update2816.html (7 KB)

Figure 8 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Instructions: Briefly describe all suspicious parts of this email.

From:

Subject:

Date:

To:

Salutation:

Message:

Attachment:

Card back

Answers

6 points
From: Domain looks legitimate, but sender doesn't have a full name
Subject: Subject line is alarming
Date: Timestamp shows email was send at an unusual hour outside of business hours
To:
Salutation: Salutation is generic
Message: (1) Message requires urgent action. (2) Contains spelling errors - "Plese" is misspelled
Attachment: Unsolicited attachment unrelated to request to update login info

Phishing Game: Game Card 2

Card front

Question Card

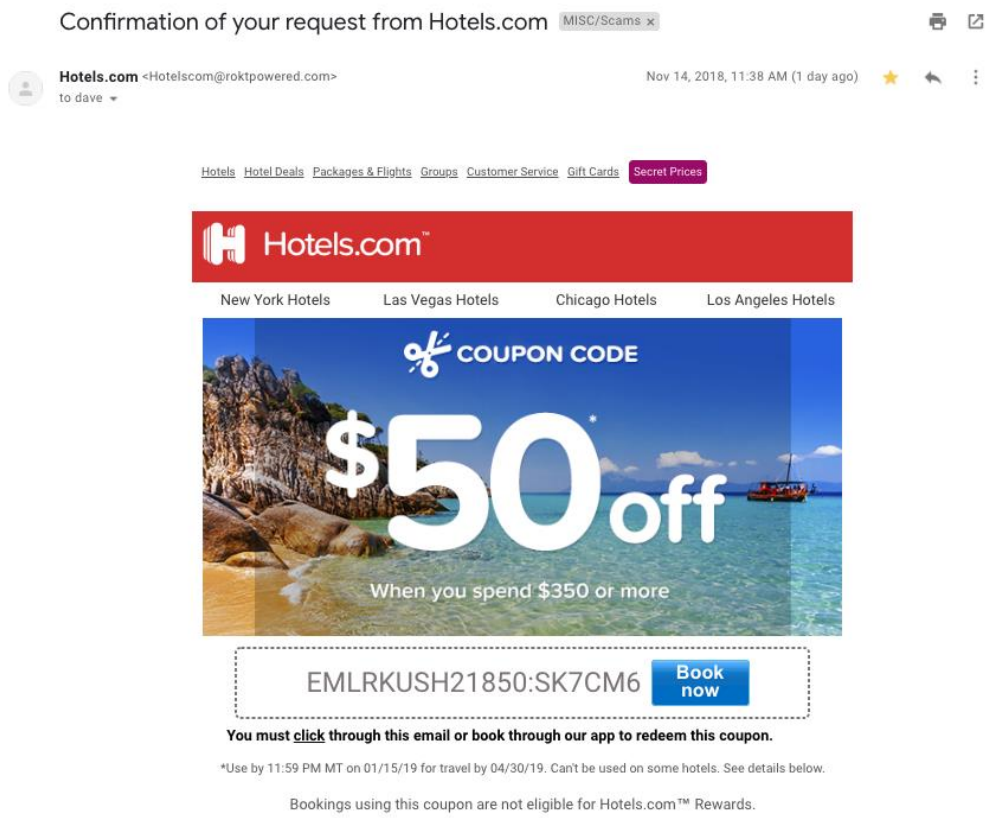


Figure 9 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Instructions: Briefly describe all suspicious parts of this email.

From:

Subject:

Date:

To:

Salutation:

Message:

Attachment:

Card back

Answers

2 points

This phishing email is particularly clever. Most of the email looks legitimate. But there are a few signs.

From: Sender's email domain is @roktpowered.com, not hotels.com

Subject:

Date: Date and time are normal

To:

Salutation: Normal for an advertisement

Message: You must click this email – the use of must is suspicious and requiring the link to access the coupon

Attachment/link: Hovering over the link may reveal the url is not Hotels.com

Phishing Game: Game Card 3

Card front

Question Card

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.

Figure 10 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Instructions: Briefly describe all suspicious parts of this email.

From:

Subject:

Date:

To:

Salutation:

Message:

Attachment:

Card back

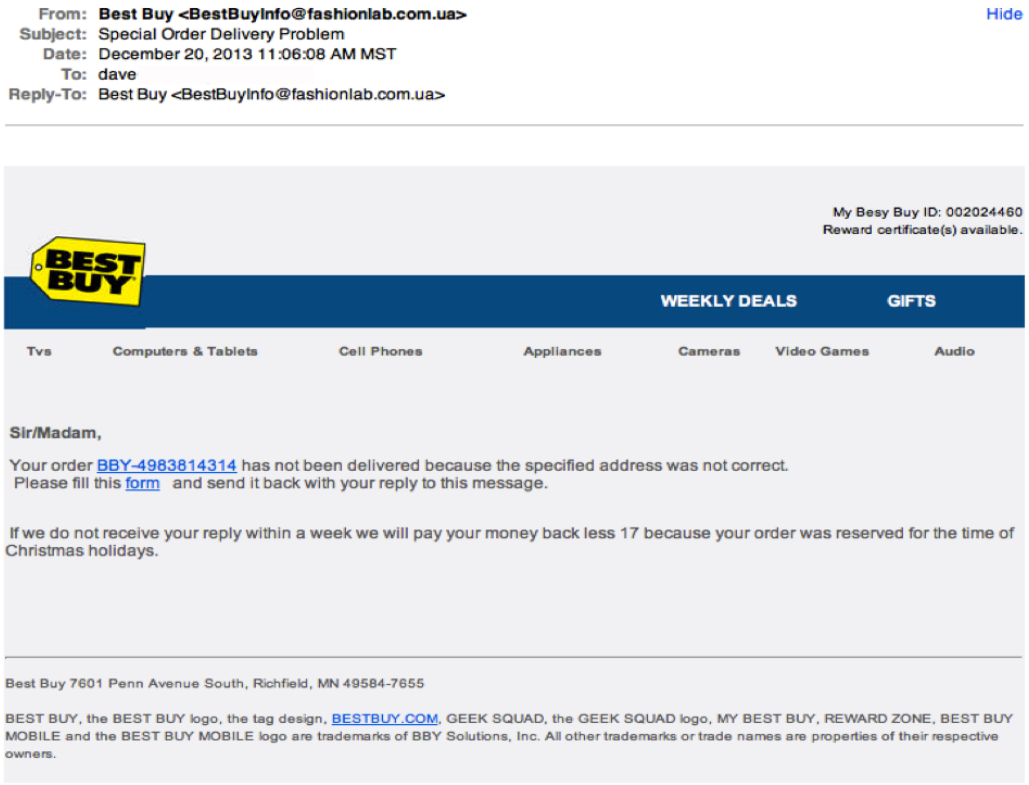
Answers

5 points
From: (1) Sender's email domain is @cbcbuilding.com, not Costco, (2) logo is incorrect
Subject:
Date: Sent outside of normal company hours
To:
Salutation: no salutation
Message: (1) Contains numerous grammatical errors / odd phrasing – e.g. you will be paid your money back lass 21%, (2) Contains punctuation errors – e.g. dont
Attachment:

Phishing Game: Game Card

Card front

Question Card



From: **Best Buy <BestBuyInfo@fashionlab.com.ua>** Hide
Subject: Special Order Delivery Problem
Date: December 20, 2013 11:06:08 AM MST
To: dave
Reply-To: Best Buy <BestBuyInfo@fashionlab.com.ua>

My Besy Buy ID: 002024460
Reward certificate(s) available.

BEST BUY

WEEKLY DEALS GIFTS

Tvs Computers & Tablets Cell Phones Appliances Cameras Video Games Audio

Sir/Madam,

Your order BBY-4983814314 has not been delivered because the specified address was not correct.
Please fill this form and send it back with your reply to this message.

If we do not receive your reply within a week we will pay your money back less 17 because your order was reserved for the time of Christmas holidays.

Best Buy 7601 Penn Avenue South, Richfield, MN 49584-7655

BEST BUY, the BEST BUY logo, the tag design, BESTBUY.COM, GEEK SQUAD, the GEEK SQUAD logo, MY BEST BUY, REWARD ZONE, BEST BUY MOBILE and the BEST BUY MOBILE logo are trademarks of BBY Solutions, Inc. All other trademarks or trade names are properties of their respective owners.

Figure 11 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Instructions: Briefly describe all suspicious parts of this email.

From:

Subject:

Date:

To:

Salutation:

Message:

Attachment:

Card back

Answers

3 points
From: Sender's email domain is @fashionlab.com.au, not Best Buy
Subject:
Date:
To: Generic salutation
Salutation:
Message: Contains multiple grammatical errors
Attachment:

Phishing Game: Game Card

Card front

Question Card

From: **Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com>**
Subject: Information
Date: August 26, 2013 1:25:12 AM MDT
To: dave
Reply-To: Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com>

USPS.COM

Notification

Our courier couldnt make the delivery of parcel to you at 20th August.
Print label and show it in the nearest post office.

Print a Shipping Label NOW

USPS | Copyright 2013 USPS. All Rights Reserved.

Figure 12 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Instructions: Briefly describe all suspicious parts of this email.

From:

Subject:

Date:

To:

Salutation:

Message:

Attachment:

Card back

Answers

4 points

From: (1) Sender's name includes numbers, (2) Sender's email domain is @gulfslipformpaving.com, not USPS

Subject: Vague – this is because the entire email is a link. Clicking anywhere in the email would take you to the link

Date:

To:

Salutation:

Message: Punctuation errors – e.g. couldnt,

Attachment/Link: Tries to force you to use link, no url provided or alternate method of contact

Phishing Game: Game Card

Card front

Question Card

From: "Bank"<payment@epayment.com>
Subject: Re: new payment on your account
Date: March 24, 2014 10:39:01 AM MDT
Reply-To: <bankwiretransferdepartment@gmail.com>

Please find attached bank slip for new payment on your account.

Regards,

Account Department.

ZIP

new payment.zip

Figure 13 from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Instructions: Briefly describe all suspicious parts of this email.

From:

Subject:

Date:

To:

Salutation:

Message:

Attachment:

Card back

Answers

4 points
From: Reply to address is an @gmail account
Subject: urgent / alarming
Date:
To:
Salutation:
Message: Too brief, does not provide information, unprofessional
Attachment: Zip file - suspicious

References

Ellis, D. (n.d.). *7 Ways to Recognize a Phishing Email: Email Phishing Examples*. Retrieved April 20, 2021, from Security Metrics: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Fruhlinger, J. (2020, September 4). *What is phishing? How this cyber attack works and how to prevent it*. Retrieved April 20, 2021, from CSO Australia: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Irwin, L. (2020, June 10). *5 ways to detect a phishing email – with examples*. Retrieved April 20, 2021, from IT Governance: https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

Report a scam. (n.d.). Retrieved April 20, 2021, from ACCC Australian Competition and Consumer Commission: https://www.scamwatch.gov.au/report-a-scam