Introduction to Phishing

Annual Mandatory Training

2021

AdvocateAuroraHealth

Advocate Health Care Aurora Health Care

This training will enable you to recognize email traps and avoid phishing scams.

What Is Phishing?

Phishing is a social engineering activity:

- Phishing tricks users to provide sensitive information to cyber criminals via email (*the bait*)
- The emails appear to be from legitimate companies or your best friend or boss
- The primary goal is to acquire credentials, financial information, or other sensitive data

Phishing Is a Craft

Phishing emails prey on emotions: greed, curiosity, or fear.

The emails look like they come from a trustworthy individual or credible organization.

They also look realistic. This is why it's so tough to identify phishing emails.

Why Are Phishing Emails Harmful?

Phishing is associated with virus infections, ransomware, identity theft, data theft, and more. Scammers who send phishing emails can use your computer to attack your organization.

Are Phishing Emails Just Spam?

Phish

Phish are targeted and deceptive emails sent to you in order to gain information, access, or money.

The intent is malicious.

Spam

Spam is unsolicited email that attempts to sell you a product or service.

It's mainly a nuisance, but not necessarily harmful.

How Phish and Spam Are Alike

They're both unwanted emails and how you interact with either type is important.

Phishing Needs Your Help to Succeed

Phishing emails have changed a lot over the last decade. They look more legitimate than they did just several years ago.

While foreign royalty doesn't really need your help in transferring funds, people still fall for schemes like this.

Emails Deserve a Hard Look

We're all generally cautious with email, but it pays to be extra cautious.

Each part of an email is a decision point. How you interact with the email is important.

Let's take a look at some questions you can ask yourself before deciding what to do about the email.

How Do I Identify Phishing Emails?

Choose a topic. Review all highlighted text for each topic to continue.

Sender

The header can offer clues to help you recognize a scam.

Context

Every email has a purpose.

Content

It's the small details.

Sender

The header can offer clues to help you recognize a scam.

To: <undisclosed-recipients>

From: avothsupport [mailto: marigoldbank_support@yahoo.com] On Behalf of Webmail.marigoldbank-payment.com

Subject: Quoting Marigold Bank Support

Dear Valued customer,

We are currently verifying our subscribers email accounts in other to increase the efficiency of our webmail futures. During this course you are required to provide the verification desk with the following details so that your account could be verified.

You can easily update your account at our Customer Self-Help Site.

Kindly verify your information so as to avoid cancelation of your email account

Thanks,

Julianna Wallingford
Marigold Bank Help Desk

Does the Sender use a public email address (Google, Yahoo, QQ, Zoho, eclipso, etc.)?

Legitimate companies and organizations will not use public email addresses for official business.

Do I have a prior relationship with this company or person?

Be suspicious if you've never worked with this person or organization before or if you've never provided your email address.

Does the Sender identity match the purpose of the email?

If you've never conducted business with the Sender, there is a good chance it's a phish.

Is the To: field addressed to undisclosed-recipients or a large number of recipients?

A legitimate company with whom you've worked with before is going to send email only to you. Be suspicious of unexpected emails sent to groups.

Exceptions are e-newsletters and mailing lists: Unless you've subscribed to this content, it is likely to be a phish.

Is my email address listed in the From: field?

The From: field is easily manipulated to show a false sender name. This technique, called email spoofing, is done to get past email filters. If it looks like the email is coming from you, it's either a phish or spam.

Context

Every email has a purpose.

To: Me
From: Dingo Bank Accounts
Subject: Update your username and password

DINGO BANK

Dear Customer,

During our regular maintenance and verification procedures, we detected a slight error regarding your most recent transactions. This might be due to the following reasons:

1. A recent change in your personal information.
2. Multiple failed logins in your account.
3. An inability to accurately verify your selected option of payment due to an internal error in our system.

For your safety, we have locked your online card account until you verify your information.

Reply to this email with your bank account number and password and we'll immediately set your account to remain active.

Regards,

Dingo Bank

Please note: If we don't receive your account verification within 48 hours, we will further lock down your account until we will be able to contact you by email or phone.

Why are they asking for that?

Don't give up personal information. Email is not a secure way to share sensitive or confidential information. Legitimate businesses will not ask you to send passwords or any other personal information through email.

Is the issue or request really as urgent as the Sender suggests?

Scammers prey on your emotions. They will be pushy or make threats or promises so you'll respond immediately without thinking.

Am I being promised money for little or no effort on my part?

Many offers are meant to compromise your security. Don't interact with emails promoting an offer that's too good to be true.

You can't win a contest you didn't enter. And foreign royalty doesn't need your help in managing their funds.

To: Me
From: Lottery Information Desk
Subject: EU / Commonwealth Lottery Promotions (London)

Your email address was selected to claim the sum of GBP 500,000.00 in the recent lottery.

To claim your prize, please contact our agent in Lagos, Nigeria.

Contact person: Mr. Marshall Ellis. Email: marshallsm11@mail.co.nz

Phone: +234 1 442 1841

Congratulations on your win! We look forward to making your acquaintance!

Vincent Kilkenny, Coordinator

Am I being promised money for little or no effort on my part?

Many offers are meant to compromise your security. Don't interact with emails promoting an offer that's too good to be true.

You can't win a contest you didn't enter. And foreign royalty doesn't need your help in managing their funds.

To: Me
From: ZPSGlobal <ukb3is.ilert@qquio.com>
Subject: About your attempted delivery

Dear Client,

This is an automatic notification from ZPSGlobal

We attempted to deliver your item at 07:30 A.M. The delivery attempt failed because no recipient was present at the shipping address. Due to this, we've returned the item to our warehouse.

You may arrange for redelivery by visiting the link below. If you do not arrange for redelivery within 72 hours, it will be returned to the sender.

Label Receipt Number: 29J92-0W90-90214QW19

Class: Corporate Package ServicesStatus: eNotification Sent

Status: eNotification Sent

To download the shipping receipt in Adobe PDF, visit:

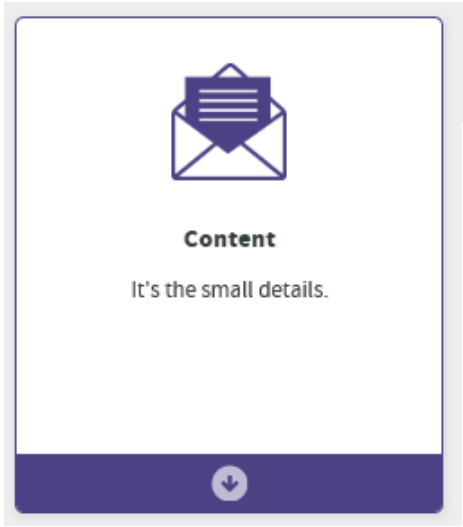
https://www.zpsglobal.com/xd/receipts/29J92-0W90-90214QW19.pdf

Thank you,

ZPSGlobal

Am I expecting a package?

These phishing emails claim there was a shipping issue with your package, but clicking that link could take you to a malicious website or attachment.



To: Me
From: notifications@epayroll.cc
Subject: Your new pay rise notification
Attachment: new_payrise_notification29.zip

Hello,

After assessing last year's pay rise structure as provided under the terms of employment, it was discovered that yo
are due for a 12.64 per cent (%) salary rise starting January, 2017.

Your salary rise documents are inclose as an attachment.

If you find these terms agreeable, or you request details be updated to your payroll account, please access the
Payroll Benefits website at the following hyperlink: https://epayroll.cc/h82kY9l

Yours very truly,

Payroll and Benefits

Is there an attachment?

Be wary of attachments you didn't expect. An attachment can be malicious even if you know the sender.

Is the salutation or greeting blank?

Some phishing emails will simply address you as "Valued Customer", while others use greetings like "Hello" and "Good day". Be wary of generic greetings, but analyze the rest of the content and email tone to judge if it's real.

Are there misspellings, typos, or unfamiliar language?

An email from a professional organization should be well-written. If the grammar is incorrect and the tone does not match the nature of the email, it may be a phish.

Does the website link look credible or malicious?

Make hovering over web addresses a habit. This allows you to see the real URL. Even if a link looks valid, don't click it. You could be redirected to a malicious website.

To: Me
From: Dingo Bank Accounts
Subject: Update your username and password

Greetings,

In an effort to verify our customer email accounts and increase efficiency in computer-based banking, we are asking customers to provide the following details.

Reply to this email with your bank account number and password and we'll immediately set your account to remain active.

dingobank

Does the email contain a graphic like a logo?

Company logos are used in many emails. These graphics can be faked by scammers, so don't rely on them to judge the safety of an email.

Investigate It

If the email looks suspicious, but comes from a source you would typically trust, don't be afraid to **investigate**. Call or send a **new** message to the person who you think sent the email. Never reply directly to the email.

Don't rely on customer service at organizations to verify an email. It's better to type in the known URL for the organization in your browser.

Report It

Report suspicious emails you receive at work to your Information Security group, Help Desk, or designated abuse email address.

At home, you can send a new message to the sender or institution to report abuse.

Delete It

Deleting an email can rid the threat from your inbox, but you could also miss reporting a widespread phishing attack on your organization.

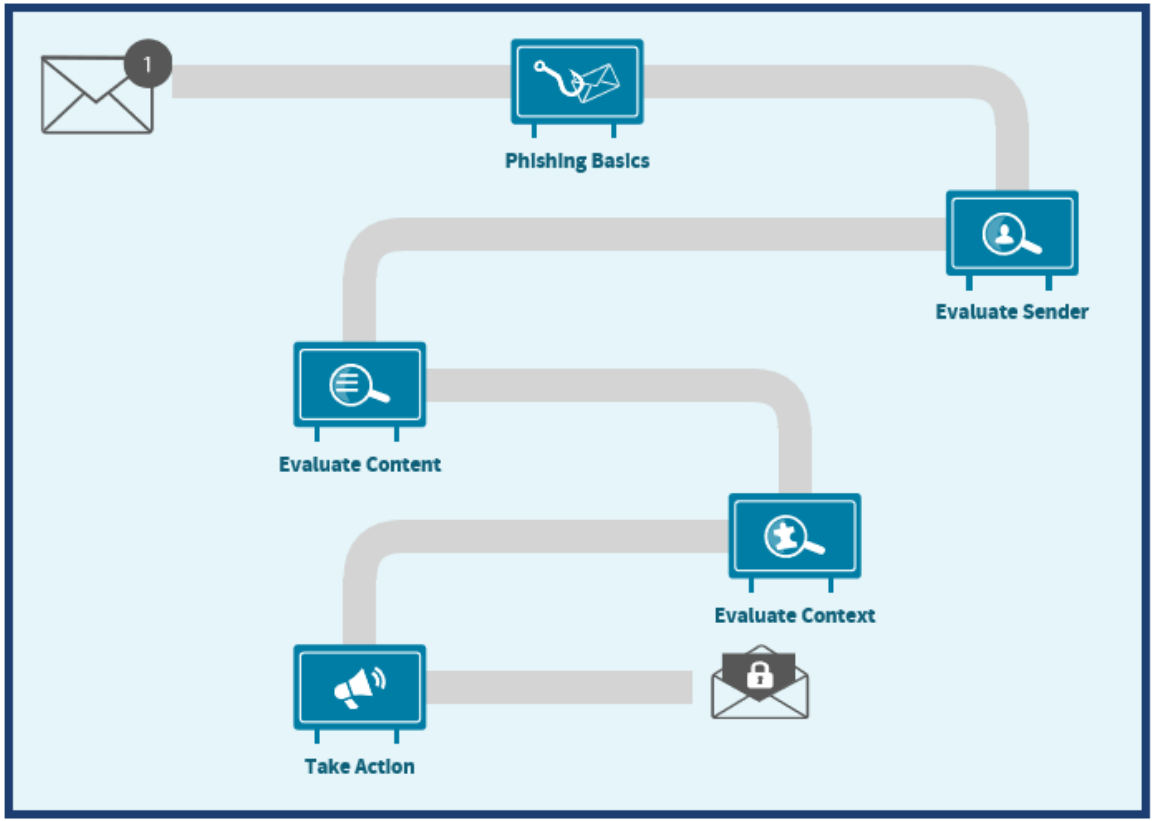
Lesson 1 Quiz

Handling Safe Emails and Phish

Let's see what you've learned!

What would you do if you received these emails? Review the email and choose the safest option. You'll need at least **4 correct answers** to move on.

Path to Email Security



What is Phishing?

What makes an email a phish?

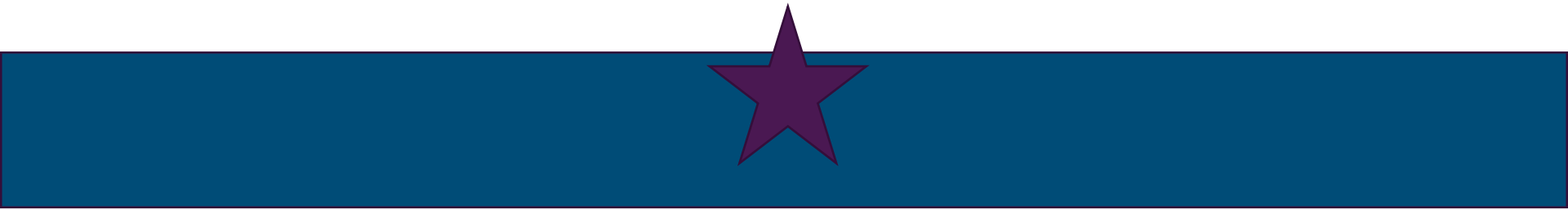
The sender wants to trick you into giving them information or device access

The sender wants to sell you something you don't want

The sender isn't careful. There are often spelling errors and typos.

All of the above

None of the above



Subject: I remembered the name!

Hey! I am sorry I could not remember the name yesterday in the break room, but last night I remembered the name of the house movers: They're called MacGrath Moving. They moved us about ten years ago and I know they're still in business. Good luck with the move!

See you at the meeting at 1500.

Cheers!
J.

Based on what you know, is this email likely risky or safe?

Safe

As you evaluate this email, assume you work in a department that handles product sales.

From: Rusty Thomas <purchasing.department.Smithton.Water@gmail.com>
Subject: Net30 term Order

Good day, we need the supply of some product, before we proceed, I would like to set up a Net 30 account with your company. Kindly enclose back with your Net30 term credit application. Looking forward to reading from you shortly.

Regard

Rusty Thomas
Smithton Water Purchasing Department

purchasing.department.Smithton.Water@gmail.com

What should you do with this email?

Report the email as phish to your security team

As you evaluate this email, assume you don't typically handle invoices for your company.

Please find the below mentioned / attached invoice details for your reference and kindly confirm the below status:

1. Have you received the invoice & confirm that all the material has been received safely.
2. If received, has all the work been completed or not.
3. If completed, have you booked for payment.

ZHENGZHOU OFFICE
4 BUILDING FORTUNE PLAZA. NO 342 JINGSAN ROAD, JINSHUI
DISTRICT CHINA 450008

SUB TOTAL
$8,195.15

Note : Please reply if there is any issue regarding material or Invoice within 3 working days or by telephone so that we can clarify if any problem is there.

Kindly treat this matter on priority.

With Kind Regards
Cheung Bohai

Based on what you know, is this email likely risky or safe?

Risky