What is Phishing?

Phish are targeted and deceptive emails sent to you in order to gain information, access, **or money**.
The intent is malicious:

- 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 is 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.

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 does not really need your help in transferring funds, people still fall for schemes like this.

Emails Deserve a Hard Look

We are 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.
The following samples highlight common tactics used in Phishing mail which you can review to help identify Phishing mail you may receive. These tactics are designed to make an email appear to come from a legitimate source, with the goal of convincing the reader to click on a URL or an attachment that contains malicious content. **INVESTIGATE IT!**

For example:

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 verification desk with the following details so that the 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

Here are some questions you can ask yourself (and INVESTIGATE IT) before deciding what to do about the email.

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

Roll your mouse over the senders name.

- Legitimate companies and organizations will not use public email addresses for official business.
- Does the Sender identity match the purpose of the email?

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

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

A legitimate company with whom you have worked with before is going to send email only to you. Be suspicious of unexpected emails sent to groups.
THERE ARE EXCEPTIONS! Organizations, like PDCA, do send group emails and use E-newsletters, Club Bulletins. Unless you have subscribed to this specific type of email, 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, and is done to get past email filters. If it looks like the email is coming from you, it is either a phish or spam.
Put your mouse over the FROM name. Does it match? Is it a familiar email address? If not, delete the email.

For example:

To: <undisclosed-recipients>
From: me
Subject: * Payment SUCCESSFUL

Hello,
We have Direct Bank Transfer in the amount 13.217!
This is for commissions made for the first two weeks of last month.
Click here to activate Bank Transfer
This is a gentle reminder You only have 2 days left to activate.
Thank you,
Meryem

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

Dear Customer,
During our regular maintenance verification procedures, we detected a slight error regarding your most recent transactions. This might be due to reason:

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

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

Investigate It

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 will 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. Do not interact with emails promoting an offer that is too good to be true.

You cannot win a contest you did not enter. Foreign royalty does not need your help in managing their funds. DELETE THE EMAIL.

The PUG DOG CLUB OF AMERICA will NOT ask you to pay for something outside of dues and fundraising.

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. DO NOT CLICK THE LINK. If you are expecting a package, go to your original order and use that link to track the item.

For example:

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

Dear Client,
This is 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 shipping receipt Adobe PDF, visit:
https://www.zpsglobal.com/xd/receipts/29J92-0W90-90214QW19.pdf
Thank you,
ZPSGlobal

Investigate It

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 is real.

Is there an attachment?

Be wary of attachments you did not expect. An attachment can be malicious even if you know the sender.

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.
**This is very important and can help you identify many unsafe emails.

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, do not click it. You could be redirected to a malicious website.

Does the email contain a graphic like a logo?

Company logos are used in many emails. These graphics can be faked by scammers, including PDCA's logo, so do not rely on them to judge the safety of an email.

For example:
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 immediately set your account to remain active.
dingobank

Investigate It

If the email looks suspicious, but comes from a source you would typically trust, do not be afraid to **investigate**. **Never reply directly to the email.** Call or send a **new** message to the person who you think sent the email. Open a new browser and search for the company or person.
Do not rely on customer service at organizations to verify an email. It is better to type in the known URL for the organization in your browser, NEVER use links in the email.

If it concerns PDCA, ASK before doing anything. Contact any board member or email PDCA as PDCAinformation@gmail.com.
We will let you know if the email is valid or not.