How To Spot A PHISH

What is Phishing? A technique used to fraudulently obtain usernames, passwords, credit card numbers, and other sensitive information.

Fraudulent emails typically ask you to:

- Open an attachment or,
- Click on a link, redirecting you to a malicious website.
- You may be prompted to enter personal information.

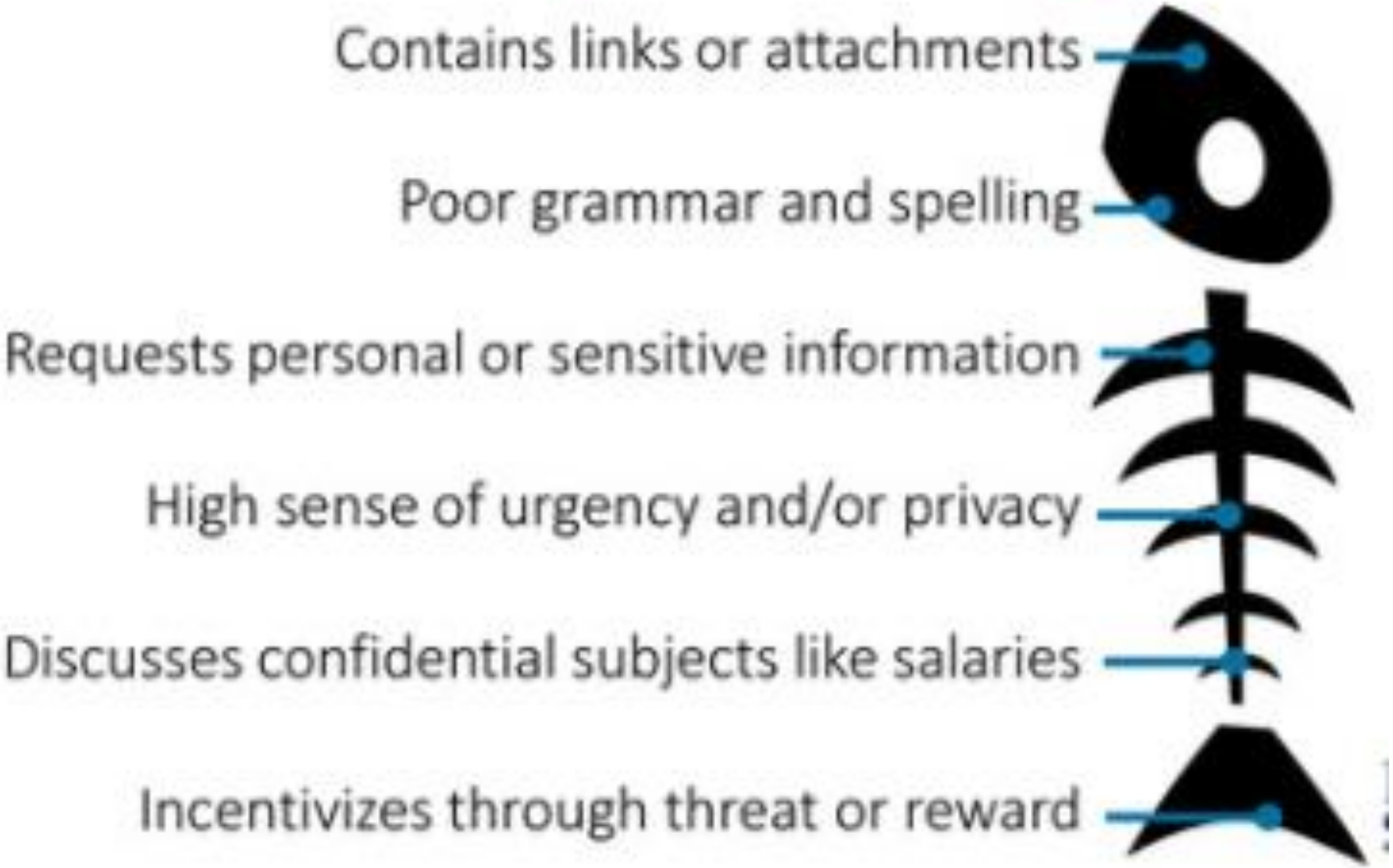
Phishing Bait

Notification from a help desk or system administrator
Asks you to take action to resolve an issue with your account (e.g., email account has reached its storage limit), which often includes clicking on a link and providing requested information.

Attachment labeled “invoice” or “shipping order”
Contains malware that can infect your computer or mobile device if opened. May contain what is known as “ransomware,” a type of malware that will delete all files unless you pay a specified sum of money.

Fake account on a social media site
Mimics a legitimate person, business or organization. May also appear in the form of an online game, quiz or survey designed to collect information from your account.

Anatomy of a Phishing Email



Phishing Email

ALERT

BD belanger, demi (BHES Teacher)
Today, 8:27 PM

Reply all

Due to our recent IP routine check; we have reasons to believe that your account has been violated and access by a third party. Click on SUPPORT and verify your Mailbox to avoid deactivation.

Warm Regards,

Help-Desk Administrator.
With best regards

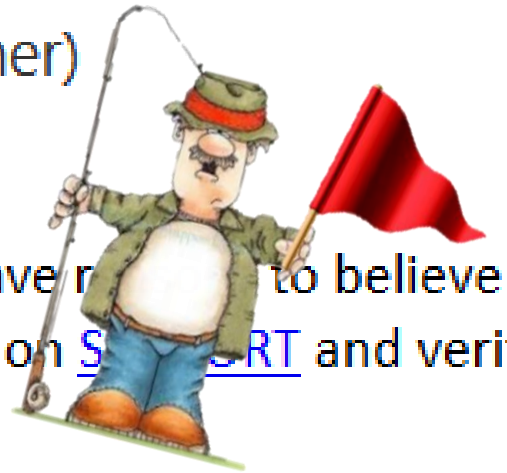
Never Trust the Sender Name

ALERT

Many of these e-mails look like they come from someone you may know.

BD belanger, demi (BHES Teacher)
Today, 8:27 PM

Reply all



Due to our recent IP routine check; we have r to believe that your account has been violated and access by a third party. Click on S RT and verify your Mailbox to avoid deactivation.

Warm Regards,

Help-Desk Administrator.
With best regards

Scammers can actually change the display name of e-mails or actually use names that sound legitimate.

“Urgent”, “Alarm”, or “Alert” e-mails

ALERT

Scammers prey on quick reactions.

If people think there is an immediate problem they will act quickly to resolve it. Therefore they use words like “urgent” or “alarm” to make people react without fully thinking through.

BD

Today, 8:27 PM

Due to our recent IP routine check; we have reasons to believe that your account has been violated and access by a third party. Click on SUPPORT and verify your Mailbox to avoid deactivation.

Warm Regards,

Help-Desk Administrator.
With best regards

If there really is a problem with your school accounts, contact me or the technician directly before following through.

Lack of Personalization

ALERT

BD belanger, demi (BHES Tea

Today, 8:27 PM

Due to our recent IP routine check; we
violated and access by a th party lic
deactivation.

Warm Regards,

Help-Desk Administrator
With best regards

Scammers will often use phrases like “user” or “customer” instead of using your real name.

Most brands prefer to personalize e-mails by putting in your name. Think of all of those shopping and sales e-mails you get! Those typically use your first and last name.

Never click on links

ALERT

BD belanger, demi (

Today, 8:27 PM

A little known fact about web links is that you can easily find out where a link is going without clicking on it.

If you simply hover your mouse over the link, the web address will show in most windows and browsers.

Due to our recent IP routine check; we have reasons to believe that your account has been violated and access by a third party. Click on SUPPORT and verify your Mailbox to avoid deactivation.

http://dorchester2.webnode.com/
Click to follow link

Warm Regards,

Help-Desk Administrator.
With best regards

Never click on links

Subject: Sign-in Alarm

http://crocusterminal.ru/components/office/index.html
Click or tap to follow link.

Dear User,

Your account was accessed from a different location IP Click here and re-login on our database for verification purposes.

Get better protection against virus and spywares

Thanks,
Office 365 Email Administrator ©2017

In the e-mail above, the ".ru" of the web address indicates a Russian website. Unless you know that is where the company is based, don't click on links to foreign countries.

Never Login from an Emailed Link

From: uec_100@hotmail.com
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 2015 23:15:37 +0530

Outlook

Dear E il U r,

This is t nfo that on
and s f you choose n
read a d emails,and yo
con s, contacts and

Update Your Account

Take a minute to update you
Thank You
Outlook Warning! Me

If you get an e-mail that asks you to “re-login” or “verify your login” it is probably a scam.
Most brands don’t need you to “verify your login” if something seems suspicious. It is always best practice to got to the website you are familiar with to login and check on your account.

Nameless Signature

ALERT

BD belanger, demi (BHES Teacher)
Today, 8:27 PM

Reply all

Due to our recent IP routine check; we have reasons to believe that your account has bee violated and access by a third party. Click on SUPPORT and verify your Mailbox to avoid deactivation.

Warm Regards,

Help-Desk Administrator.
With best regards

Most brands prefer to contact users directly, not only using their name, but a personal contact from the brand as well.

E-mails from legitimate sources won't be signed administrator" unless they include a real person's name.

Don’t Open Attachments from Unknown Senders

Wed 1/17/2018 11:40 AM

Walker, Michelle <Michelle.Walker@amerisbank.com>

ACTION NEEDED: Docusign

To

You replied to this message on 1/17/2018 11:49 AM.
If there are problems with how this message is displayed, click here to view it in a web browser.

Michelle used Dropb[illegible]o sh[illegible]some document with you. Click REVIEW DOCUMENT to access the documents or click

Download

Kindly let me k[illegible]f you have any questions

Thanks

Michelle Walker
Ameris Bank | Mortgage Processor
834 Savannah HWY, Charleston, SC 29407
Phone 843-367-7347 Fax 803-567-6222
michelle.walker@amerisbank.com
Please visit us online at www.amerisbank.com

Many common attachments can now contain hidden viruses, including word documents, spreadsheet files, and even PDF files.

Only open attachments from people you know and trust. If you have any doubts, open a new e-mail and ask the sender (do not reply to the e-mail).

Where are the red flags?

PayPal Yesterday at 8:32 PM

To: Morgan Wright

[Paypal Team] : Login to your account and update your information✔

PayPal

This is an automated email, please do not reply

information about your account :

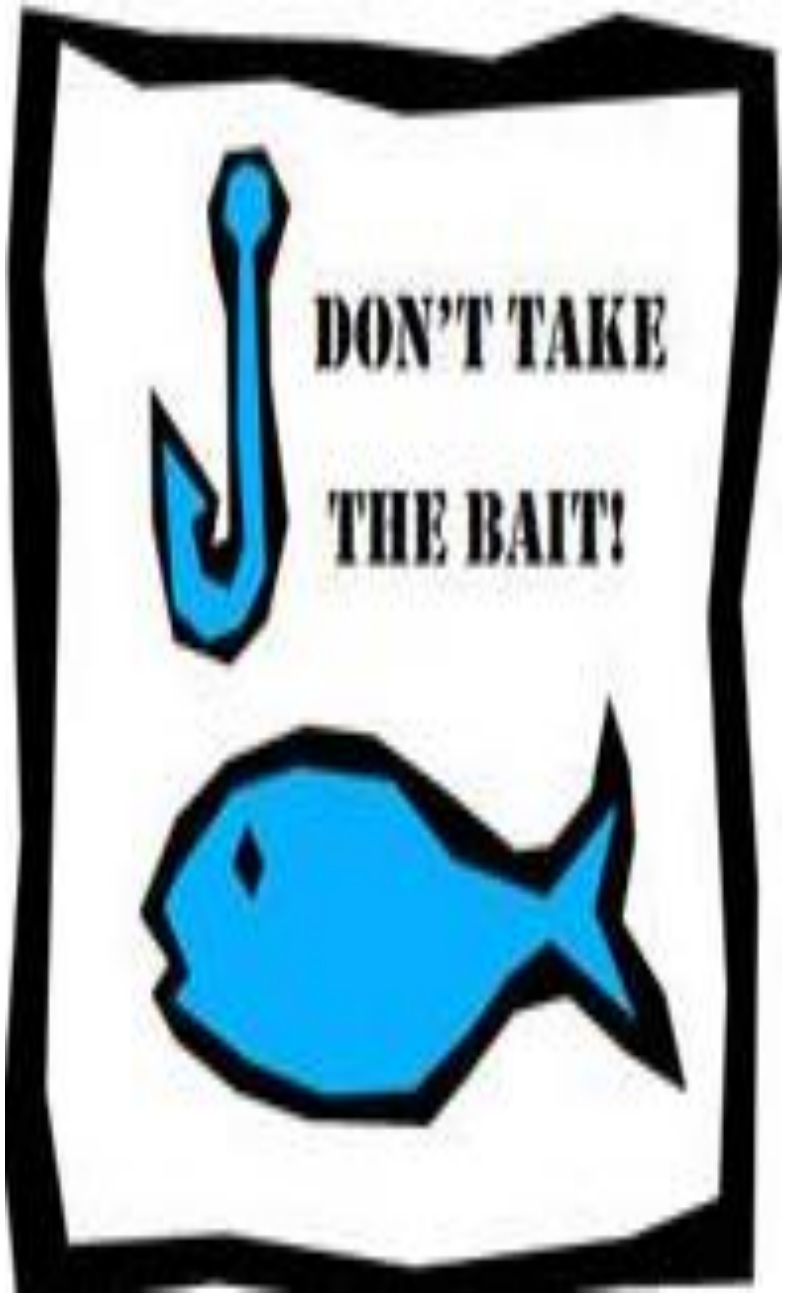
Warning! Your PayPal account was limited!

Your account has been limited temporarily in order to protect it. The account will continue to be limited until it is approved.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.
The process does not take more than 5 minutes.
Once connected, follow the steps to activate your account. We appreciate your understanding as we work to ensure security.

Click here to Confirm Your Account Information.

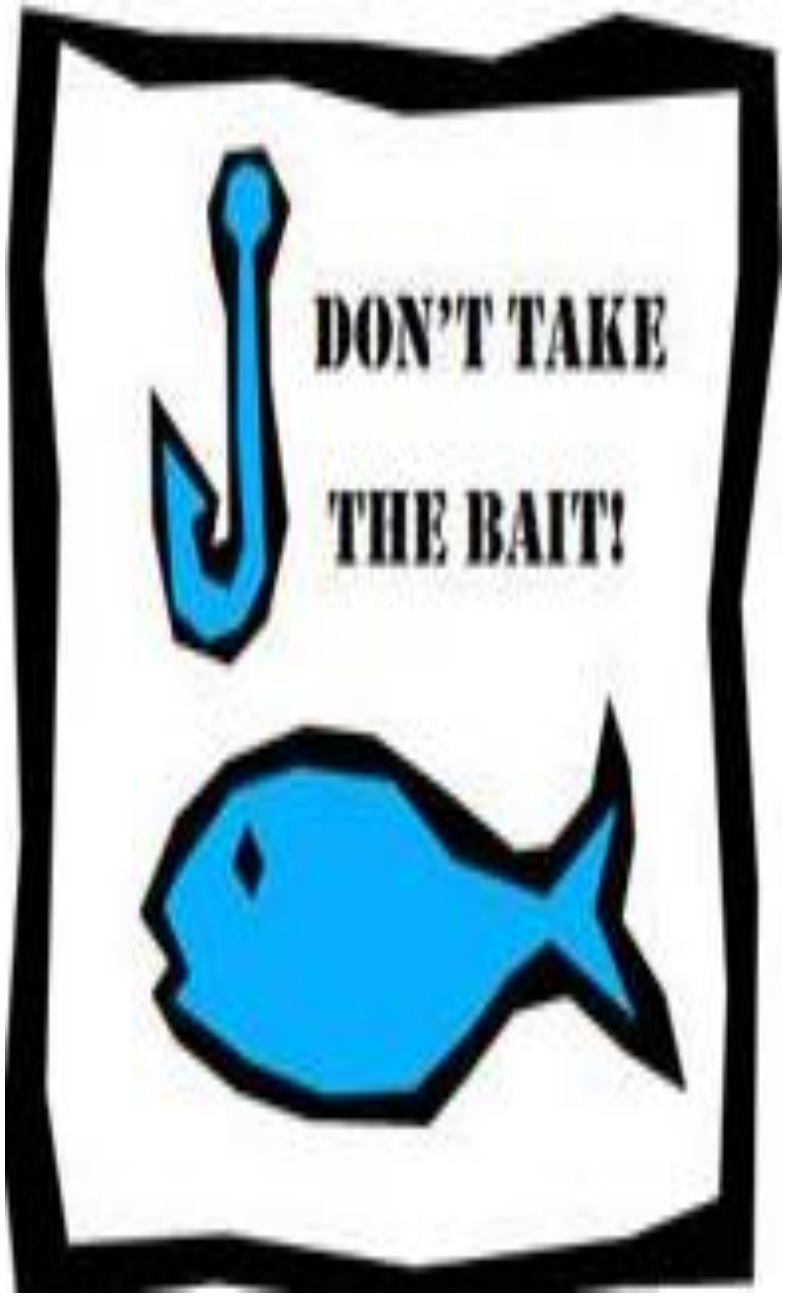
Department review PayPal accounts

PayPal Email ID PP156930



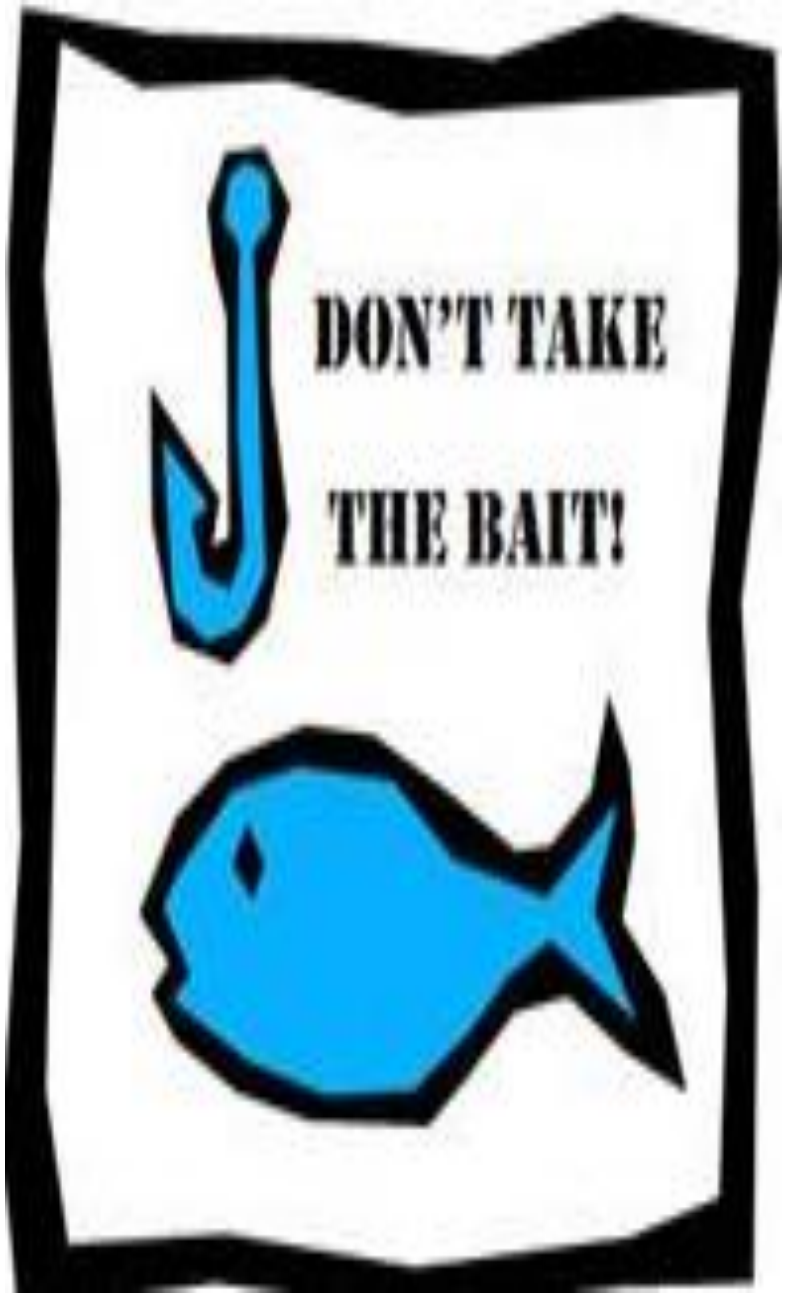
Protecting Yourself

- Be wary of messages asking for passwords or other personal information.
  - **No one from DD2 will ask for your password.**
  - Most reputable businesses and organizations will not ask for this information via email.



Protecting Yourself

- Never send passwords, bank account numbers or other private information in an email.
  - Do not reply to requests for this information.
  - Verify by contacting the company or individual, but do not use the contact information included in the message.



Protecting Yourself

Do not click on any hyperlinks in the email.

- Use your mouse to hover over each link to verify its actual destination, even if the message appears to be from a trusted source.
- Pay attention to the URL and look for a variation in spelling or a different domain

Reporting a Phishing Email

- Do not click on any hyperlinks.
- Do not forward the email to others.
- Alert your site-based ITS and technician immediately.
- Delete the message.

The best advice:
when in doubt, play it safe.
Always feel free to ask me about any suspicious e-mail you receive!