Rensselaer

why not change the world?®

Don’t Take the Bait!

How to recognize a phishing email

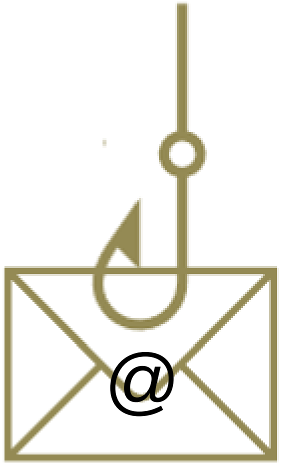
DotCIO-Information Services and Technology

07/09/24

PHISHING EMAILS ARE THEY *REEL*?

Phishing emails are real, and they can *hook* you in by their content. The question is how do you recognize them!

Phishing scams originate from trusted sources to trick a person into entering valid credentials or attempts to *lure* them into revealing their username, password and other personal identifying information (PII)



WHAT ARE THE RED FLAG AREAS TO REVIEW IN AN EMAIL?

Phishing emails target different *lines* in an email such as, **From**, **Subject**, **Date/Time**, **Content** and **Signature**. As well as in their content, indicating a since of urgency or by including links and attachments to *troll* for information.

So, let’s *tackle* each area we should review, to determine if an email is part of a phishing scam, as well as learn the steps to go through after you receive an email like this.

Don’t *drift* from reviewing the following parts of an email:

- From
- To
- Subject
- Content/Signature
- Hyperlinks
- Attachments

FROM:

- I **don’t recognize the sender’s email address** as someone I ordinarily communicate with?
- This was sent from **someone inside the organization** or from a vendor I know, but it **is very unusual or out of character**.
- Is the **domain name** inconsistent? (name after the @)
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I have not communicated with before.

Example 1

Why is this coming from Gmail?

From:Jobandintershipfair<smith.j@gmail.com>

Example 2

Email address is not official?

From:Manager<manager@fakeco.com>

Example 3

Is this from a suspicious domain?

From: Jessica Gray <grayj2@mail.gvsu.edu>

TO: AND SUBJECT:

TO:

- Does this email include a long list of names or just your name?
- You were cc'd on an email sent to one or more people, but you don't personally know them.
  - TO: you@yourorganization.edu, xxxx, yyyy, aaaa, bbbb

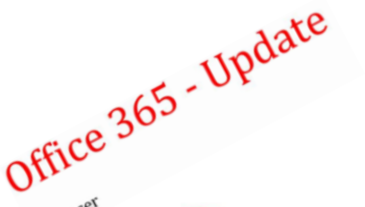
SUBJECT:

- Is this irrelevant or does not match the message content?
- Is there a since of urgency?

Example 1	Example 2	Example 3
Subject: URGENT REQUEST	**Subject: Confirm Purchase**	**Subject: Your account password has expired**

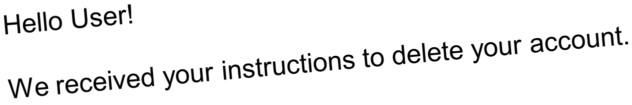
SALUTATION:

- Watch for generic greetings or no greeting at all.
- Vague salutation, like Hello User, “Valued Customer?” or Dear xxxx.
- Greeting is in **Bold**.



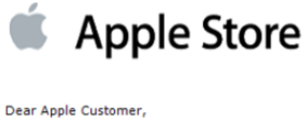
Office 365 - Update

Dear user



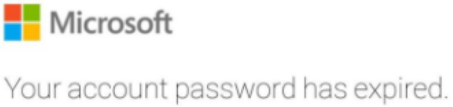
Hello User!

We received your instructions to delete your account.



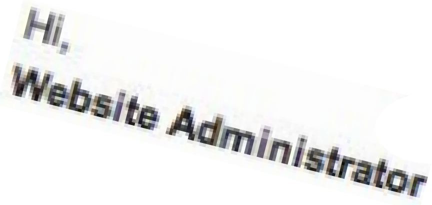
Apple Store

Dear Apple Customer,



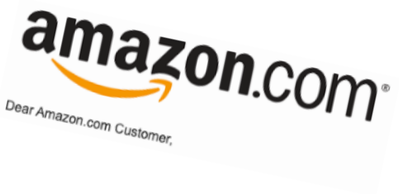
Microsoft

Your account password has expired.



Hi,

Website Administrator



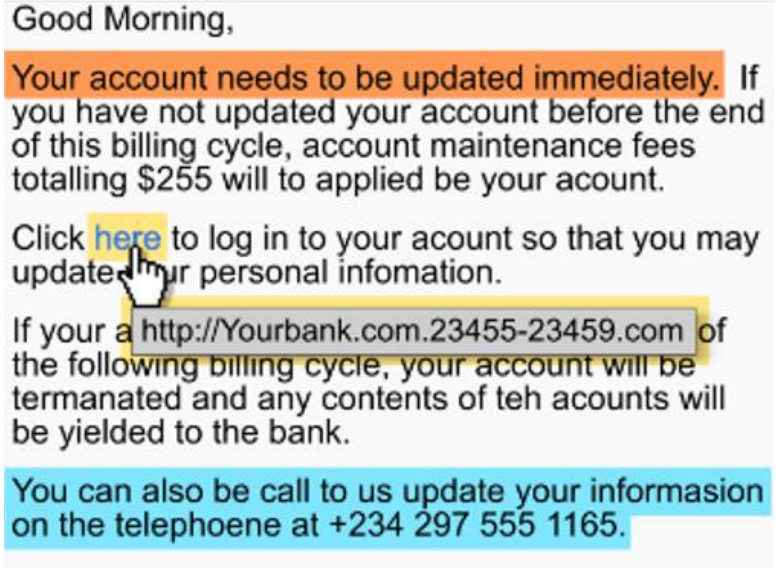
amazon.com

Dear Amazon.com Customer,

CONTENT

- The sender wants you to click on a link or open an attachment that seems odd or illogical to gain something of value.
- Beware of a sense of urgency or fear in the content. For example, “Act soon… “ or “Your account needs to be updated immediately”
- Content seems odd or illogical and asking for personal identifying information (PII) (usernames, passwords, bank account numbers)
- Does the email have bad grammar or misspelled words?

In the example to the right, how many misspellings can you find?



Good Morning,

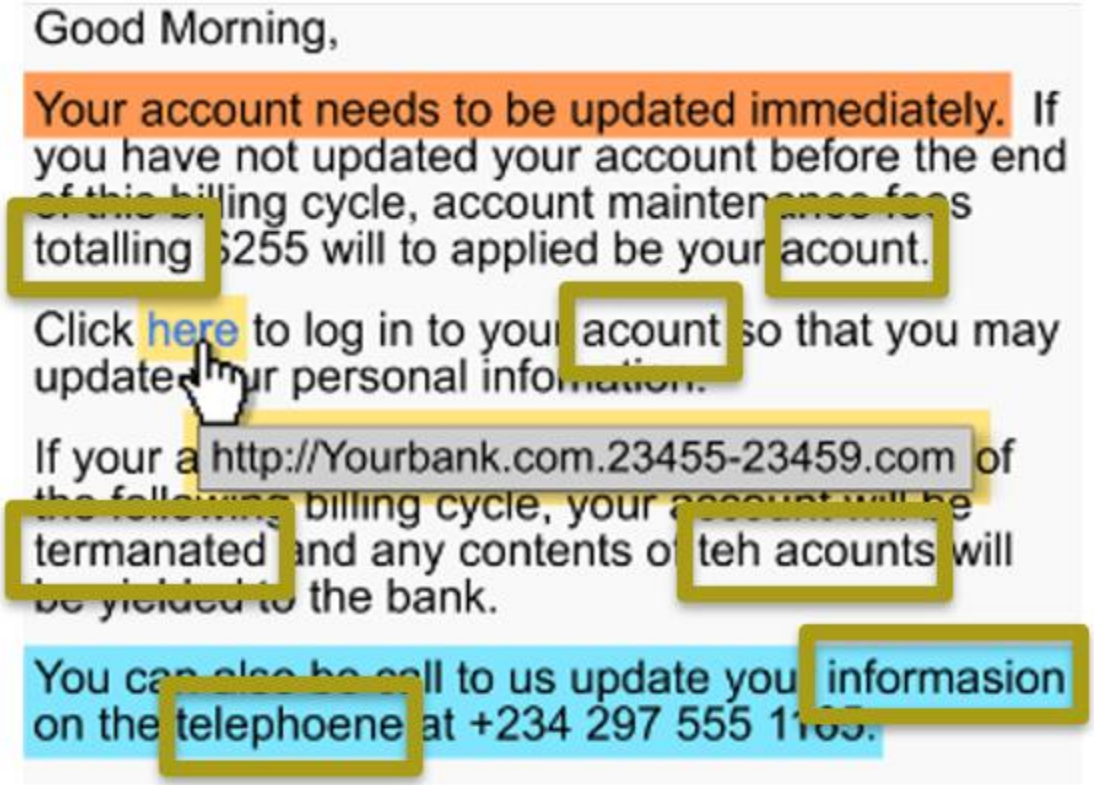
Your account needs to be updated immediately. If you have not updated your account before the end of this billing cycle, account maintenance fees totalling $255 will to applied be your acount.

Click here to log in to your acount so that you may update ur personal infomation.

If your a http://Yourbank.com.23455-23459.com of the following billing cycle, your account will be termanated and any contents of teh acounts will be yielded to the bank.

You can also be call to us update your informasion on the telephoene at +234 297 555 1165.

THERE ARE **SEVEN** MISSPELLINGS



Good Morning,

Your account needs to be updated immediately. If you have not updated your account before the end of this billing cycle, account maintenance fees totalling $255 will to applied be your acount.

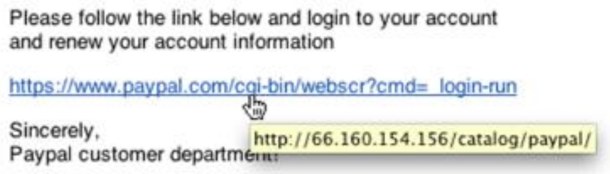
Click here to log in to your acount so that you may update your personal information.

If your a http://Yourbank.com.23455-23459.com of the following billing cycle, your account will be termanated and any contents of teh acounts will be yielded to the bank.

You can also be call to us update you informasion on the telephoene at +234 297 555 1165.

HYPERLINKS

- Move your mouse over hyperlinks and the link address appears. Are they from a suspicious website? If you’re not sure, it’s best to open a browser and copy or type the link to see if this is a legitimate website.
- Is the hyperlink misspelled?
- You received an email that only includes a long hyperlink with no further information and the rest of the email is blank.

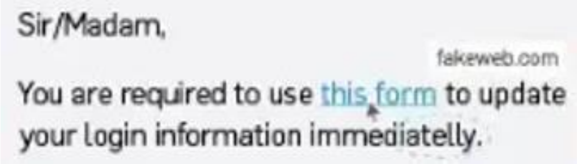


Please follow the link below and login to your account
and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://66.160.154.156/catalog/paypal/

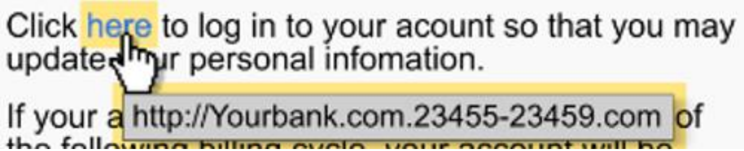
Sincerely,
Paypal customer department



Sir/Madam,

fakeweb.com

You are required to use this form to update your login information immediatelly.



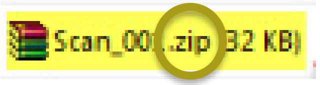
Click here to log in to your acount so that you may update your personal infomation.

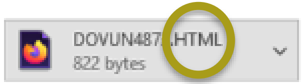
If your a http://Yourbank.com.23455-23459.com of
the following billing cycle, your account will be

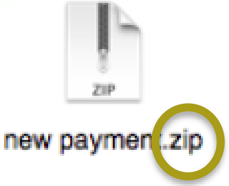
ATTACHMENTS

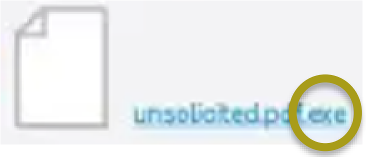
Never click attachments, until you go through the following:

- The email included an attachment that you were **not expecting or that makes no sense** in relation to the email message.
- Attachments **can include viruses and malware** that can steal your passwords, damage files, or spy on you.
- **Check the file type** on the attachment, if it is a .txt file that is safe to click.



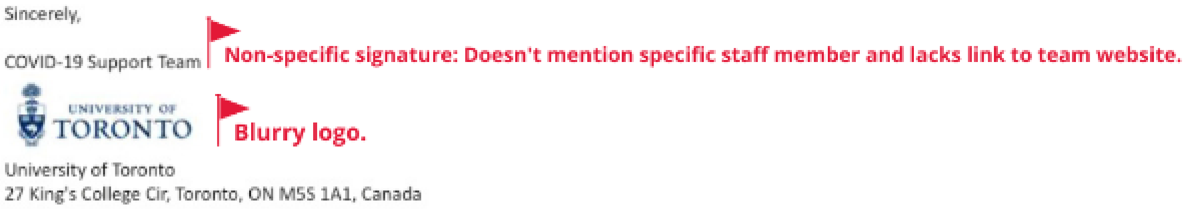






SIGNATURE

- Are you able to contact the company?
- Does the email provide information about the signer?
- Businesses that are legitimate always provide contact information.



Sincerely,

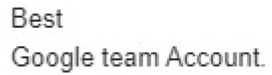
COVID-19 Support Team

Non-specific signature: Doesn't mention specific staff member and lacks link to team website.

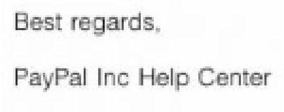
UNIVERSITY OF TORONTO

Blurry logo.

University of Toronto
27 King's College Cir, Toronto, ON M5S 1A1, Canada

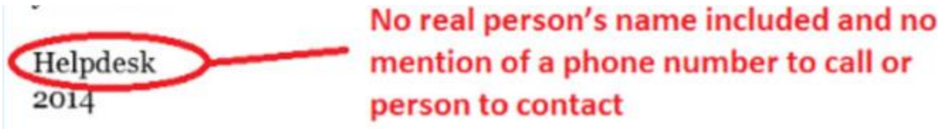


Best
Google team Account.



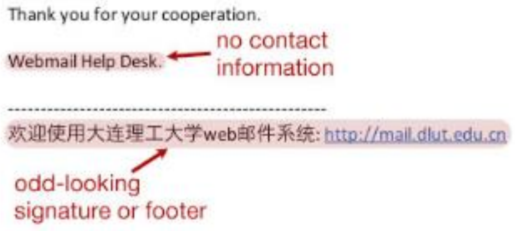
Best regards,

PayPal Inc Help Center



Helpdesk
2014

No real person's name included and no mention of a phone number to call or person to contact



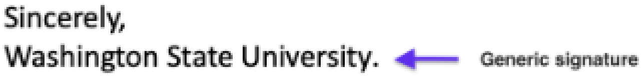
Thank you for your cooperation.

Webmail Help Desk.

no contact information

欢迎使用大连理工大学web邮件系统: http://mail.dlut.edu.cn

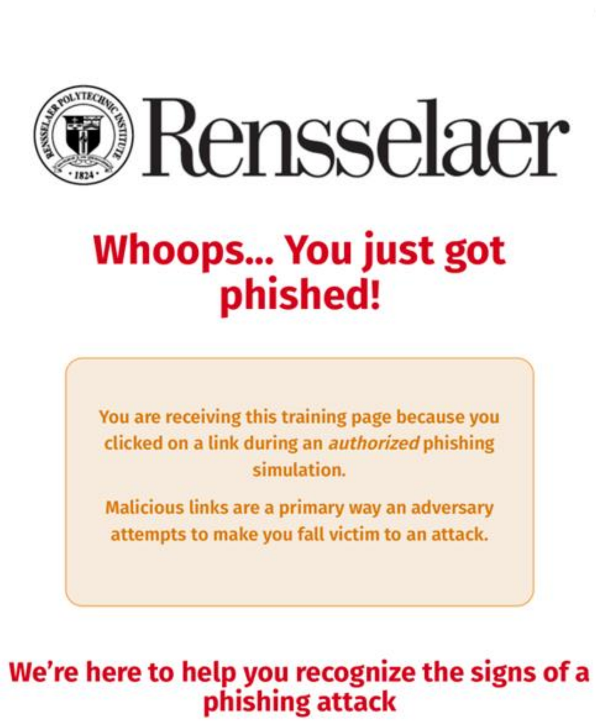
odd-looking signature or footer



Sincerely,
Washington State University.

Generic signature

Phishing email check - WHOOPS… You just got phished!



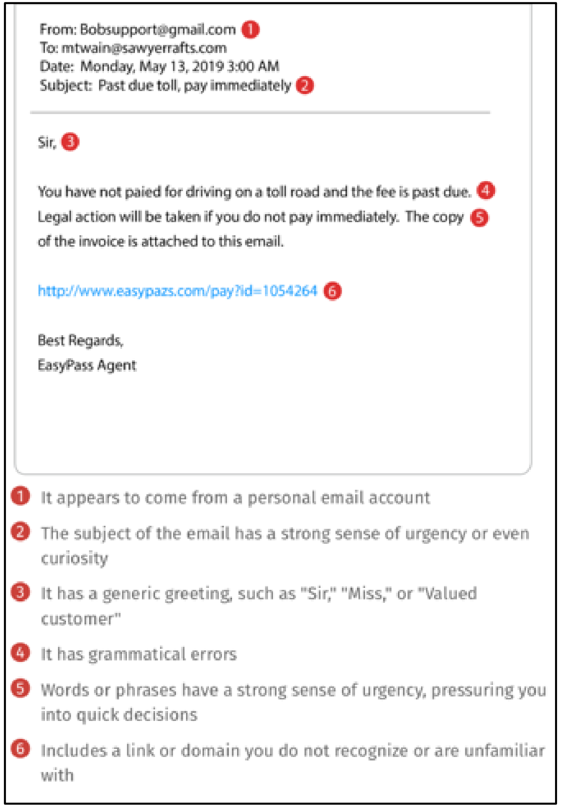
Rensselaer

Whoops… You just got phished!

You are receiving this training page because you clicked on a link during an *authorized* phishing simulation.

Malicious links are a primary way an adversary attempts to make you fall victim to an attack.

We're here to help you recognize the signs of a phishing attack



From: Bobsupport@gmail.com ❶
To: mtwain@sawyerrafts.com
Date: Monday, May 13, 2019 3:00 AM
Subject: Past due toll, pay immediately ❷

Sir, ❸

You have not paied for driving on a toll road and the fee is past due. ❹ Legal action will be taken if you do not pay immediately. The copy ❺ of the invoice is attached to this email.

http://www.easypazs.com/pay?id=1054264 ❻

Best Regards,
EasyPass Agent

❶ It appears to come from a personal email account

❷ The subject of the email has a strong sense of urgency or even curiosity

❸ It has a generic greeting, such as "Sir," "Miss," or "Valued customer"

❹ It has grammatical errors

❺ Words or phrases have a strong sense of urgency, pressuring you into quick decisions

❻ Includes a link or domain you do not recognize or are unfamiliar with

YES, IT IS A PHISHING EMAIL, NOW WHAT DO I DO?

If you are unsure if it is a phishing email, always err on the side of caution and then:

- Go to the RPI Phish Bowl page at https://dotcio.rpi.edu/it-security/phish-bowl and search for the suspicious email.
  - If the suspicious email **is on the list**, use the Report phishing button in outlook which will delete the email (Review the article - https://itssc.rpi.edu/hc/en-us/articles/15784053174797 - Report Suspicious Message from Outlook)
  - If the suspicious email **is not on the list**, and you believe it is a phish, use the Report phishing button in outlook which will delete the email. (Review the article - https://itssc.rpi.edu/hc/en-us/articles/15784053174797 - Report Suspicious Message from Outlook)
  - If the suspicious email **is not on the list and you are unsure if this is a phishing email**, please review this article on how to report this – https://itssc.rpi.edu/hc/en-us/articles/360042031492-Reporting-Spam-Phishing-Email-Attempts

PHISHING TIPS

So, as we *tackled* the many parts of a phishing email, we found out that phishing emails are *reel*.

Be a *leader and* review the following **red flags** when you receive an email you may not be expecting.

- Float your mouse over links in emails and it may show a different address than the one displayed.
- Open a browser and check the links yourself to see if they are legitimate sites.
- Don’t get *hooked* on emails that appear to be official but come from un-official email addresses.
- *Trolling* the email for slight misspellings in the URL, company name, etc. is important to help determine if you are being scammed. For example, paypa1.com instead of paypal.com.
- Beware of anything that gives a sense of urgency, or states that it requires immediate action as they can *lure* you into thinking it’s true.
- Don't click anywhere in suspicious e-mails - even in what may appear to be white space in the content.
- Be aware of too-good-to-be-true offers such as free airline tickets, money or a vacation.
- Don’t open attachments in unexpected, suspicious e-mails or text messages.
- Don’t send passwords, bank account numbers, or other private information in an email.

https://www.kent.edu/secureit/phishing-and-scams

So don’t take the bait!

REFERENCES

- https://www.kent.edu/secureit/phishing-and-scams
- https://www.avast.com/c-phishing - free antivirus download

RENSSELAER POLYTECHNIC INSTITUTE

KNOWLEDGE AND THOROUGHNESS

1824

Rensselaer

why not change the world?®