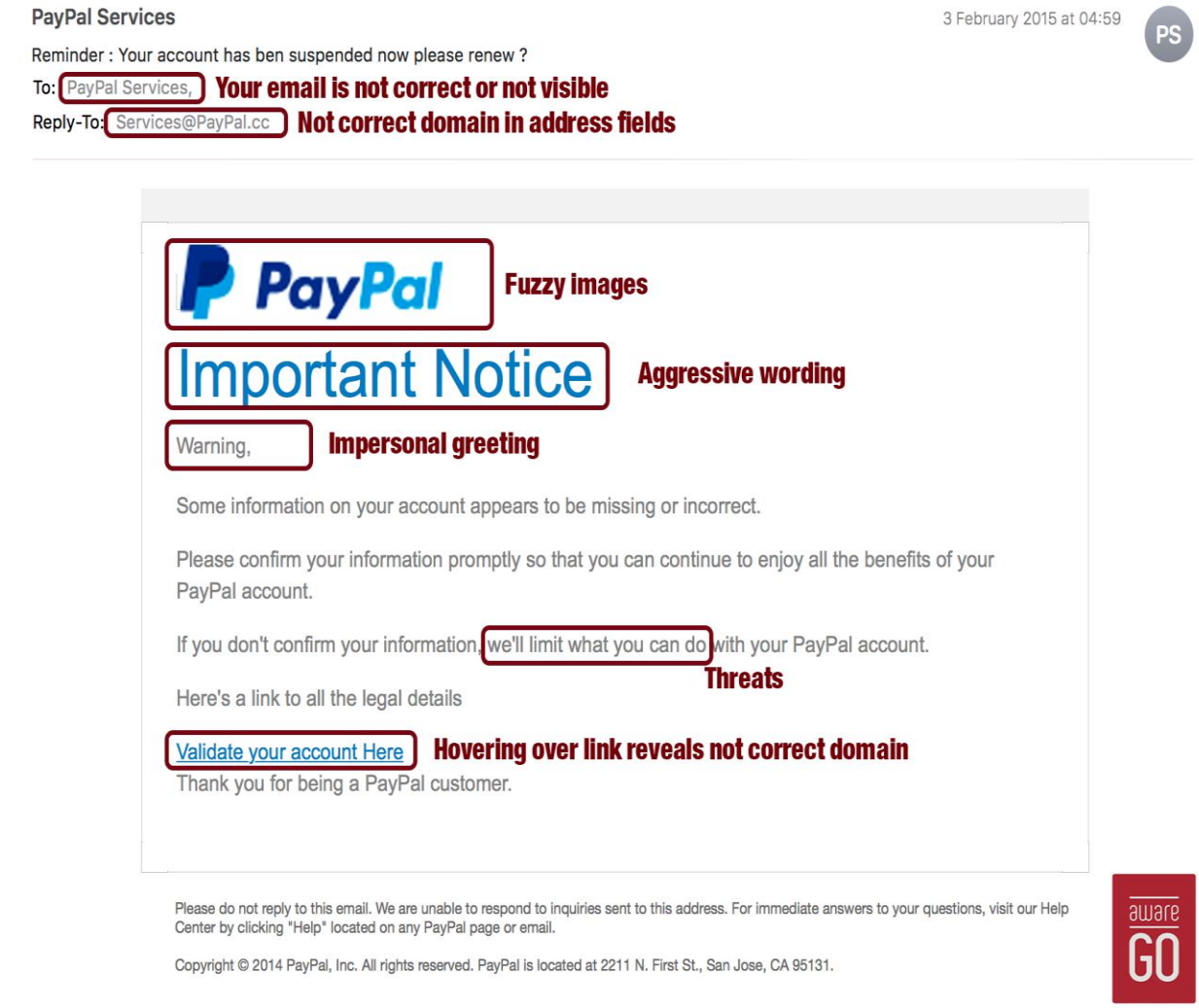
PLAYBOOK FOR HOW TO IDENTIFY PHISHING EMAILS AND ACT RESPONSIBLY, A USER GUIDE.



CYBERSHIELD

WHERE AWARENESS UNLOCK SECURITY

MARCH 4. 2024

In general concern most of security awareness training provides an exclusive way on how to respond to illegitimate or phishing emails or SMS without providing prior knowledge on how to know theses phishing emails, this play book provides practical experience in explaining the key aspects on how to identify and react to phishing emails.

Here is your trust playbook from CyberShield team, that provides you with break through way to understand this aspect and act accordingly to ensure your financial posture and privacy or business remains vigilant all time.

Version 1.

6 march 2024

Dar es salaam Tanzania

Now consider the three cases emails obtained from different sources and note any commonality and difference.

Case 1.

Dear godwin,

We hope this message finds you well and that you're making great progress in your learning journey with Power Learn Project's Learning Management System. We're excited to confirm that the lesson content you recently requested has been successfully processed and to download it, please click the following link: Lesson Content Link .

Lesson Details:

Course Name: Software Development
Module Name: Web development
Week Name: Week 1 - Introduction To HTML
Lesson Name: An Introduction To HTML for Beginners
Date of Download: Wed, 21 Feb 2024 14:11:02 UTC

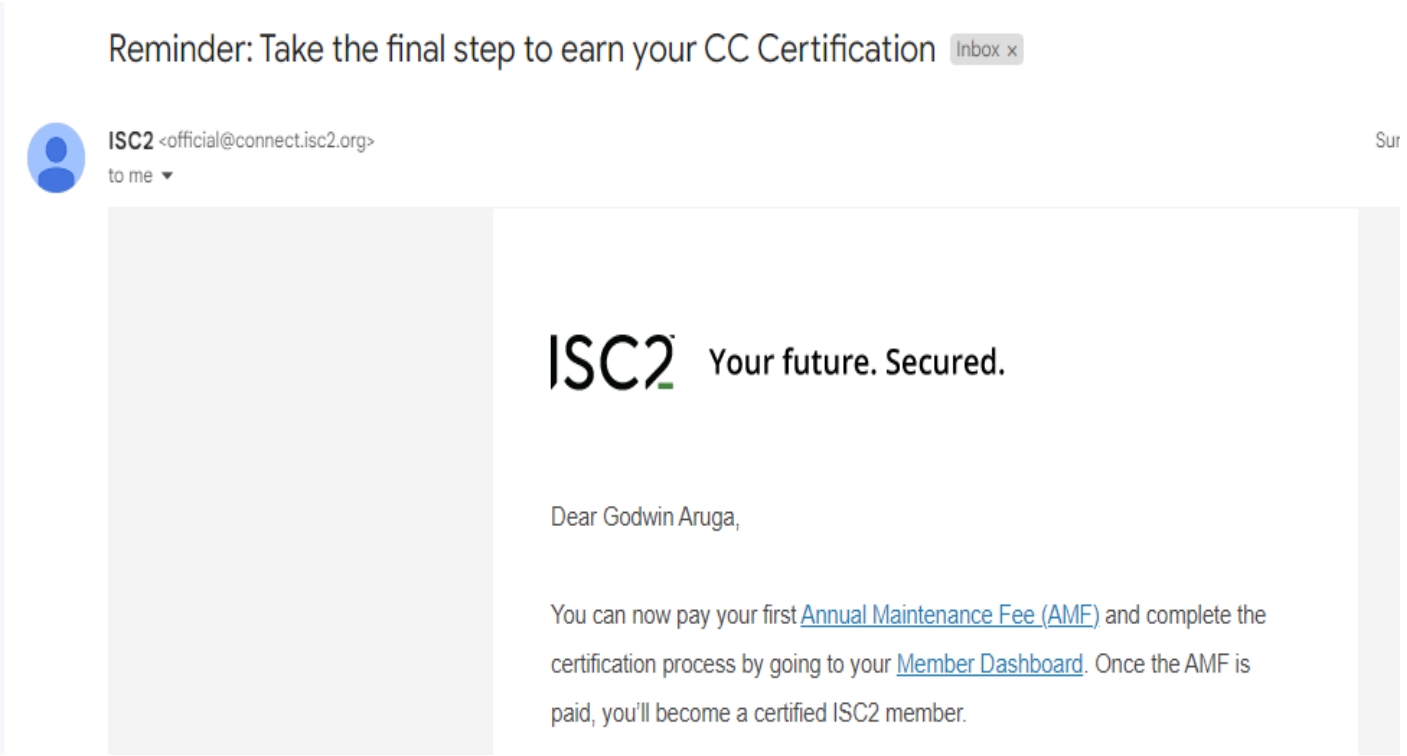
You now have access to this valuable lesson material, which you can review at your own pace. We encourage you to engage with the content thoroughly, as it plays a crucial role in your learning experience.

Should you have any questions or require further assistance with the lesson, please don't hesitate to reach out to our dedicated support team at plpknowledge@powerlearnproject.org or +254 700 611 875. We're here to ensure that your learning experience is smooth and enjoyable.

Thank you for choosing the Power Learn Project Scholarship Program for your learning needs. We wish you continued success in your studies.

Best regards,
Power Learn Project.

Case 2.



Reminder: Take the final step to earn your CC Certification Inbox ×

ISC2 <official@connect.isc2.org> Sur

to me

ISC2 Your future. Secured.

Dear Godwin Aruga,

You can now pay your first Annual Maintenance Fee (AMF) and complete the certification process by going to your Member Dashboard. Once the AMF is paid, you'll become a certified ISC2 member.

Case 3.

Dear valued customer

we are pleased to inform you that our system is currently under critical failure, thus we are looking for an effective maintenance schedule from tonight, to keep you with our adequate services at time being kindly use the following link CYBERSTORE LTD to make necessary payment and purchases at our store. keep using your credential and user name with no explicit.

best regards

customer support team

WALK WAY:

Its my hope that the three emails are legitimate or illegitimate in either way lets walk from key aspect to identify the status.

1. sender name: pay attention to the sender name, the first two email have names: official@connect.ISC2.org, and support@plpproject.org while no name for the third email, so what!, don't trust the sender display name. Check the "from" email address. Does it look like it matches the sender display name? If something seems off, trust your instincts and delete the message.

2. Look attachments - but don't click. If there are any words with links, you can hover your mouse over them in order to view the full link embedded in the message. If it's untrustworthy or the link has been shortened somehow for example the CYBERSTORE LTD attachment link is directing to http://www.cyberstoremx.ac.tz/login?php%3Eget-post, while the legitimate is http://www.cyberstore.ac.tz. do not click the link. Just the simple act of clicking a link can infect your device with malware and compromise your account.

3. Check for typos or grammar mistakes. Typos, especially multiple instances in one message, are becoming less common but still can give away a phishing attempt.

4. Analyze the "from" email address. In an attempt to make tip #1 less effective, scammers will often spoof email addresses of trusted organizations. Look for typos, oddly placed characters, and unusual word combinations in the "from" email address.

5. Analyze the greeting. Is it a generalized greeting, or a properly customized greeting with your name? consider the two cases, the greetings are so specific to Godwin, while third email sounds dear valued customer.

6. Analyze the signature. Do you know the sender? Can you verify outside of this message that they've sent it to you? for both two cases email have signature at the end unlike the third email

7. personal information required. Legitimate organizations will never ask for personal credentials or information via email, pay attentions to the nature of information required by the sender.

8. Beware of urgent or threatening language in the subject or message. If a package is being held, an account has been suspended, or you won't believe the embarrassing photo of you, this may be a phishing attempt.

9. Trust your instincts. If something doesn't feel quite right, it probably isn't. If the message is purporting to be from a known/trusted source, follow up with that individual or organization by phone or other means outside of the suspicious message.

Generally, taking this theory for butler account compromise. When a Butler user's account is compromised, scammers use their Butler email address to send out phishing attempts. For this reason, some of the phishing attempts circulating campus do come from legitimate Butler email addresses. Therefore, don't rely only on the sender's email being legitimate alone to determine if a message is safe or not.

When Butler IT knows about a phishing attempt circulating campus, we will post information about it on our status page. To access the status page, go to ask.butler.edu and click on the Status widget. On the Alerts page, you will see information about any phishing attempts circulating campus. If no information is posted and you are unsure about an email, contact the IT Help Desk for assistance before you open attachments or click on links.

"Even you pay attention to all those suggested above, attackers can still use sophisticated techniques and bypass all identification means, thus your required to Be cautious and act responsibly, remember security matters as much as it happens"

Aruga GS