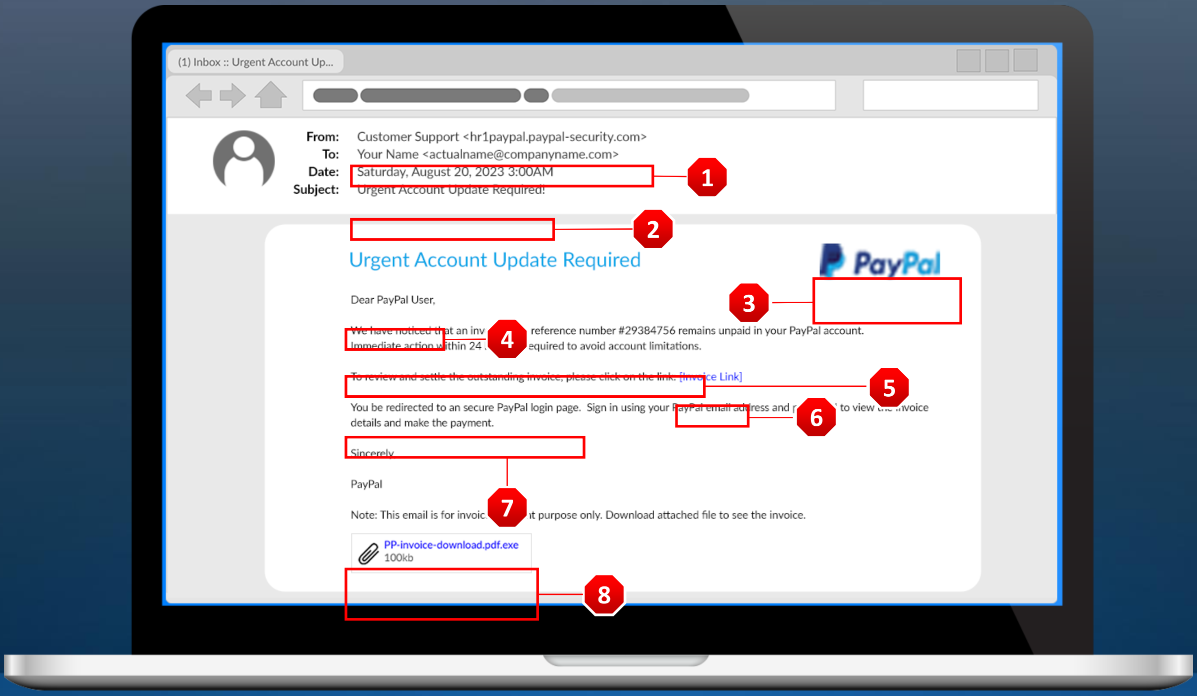
THE ANATOMY OF A PHISHING EMAIL



From: Customer Support <hr1paypal.paypal-security.com>
To: Your Name <actualname@companyname.com>
Date: Saturday, August 20, 2023 3:00AM
Subject: Urgent Account Update Required!

Urgent Account Update Required

PayPal

Dear PayPal User,

We have noticed that an inv reference number #29384756 remains unpaid in your PayPal account. Immediate action within 24 equired to avoid account limitations.

To review and settle the outstanding invoice, please click on the link: [Invoice Link]

You be redirected to an secure PayPal login page. Sign in using your PayPal email address and r to view the invoice details and make the payment.

Sincerely,

PayPal

Note: This email is for invoic it purpose only. Download attached file to see the invoice.

PP-invoice-download.pdf.exe
100kb

1 SENDER'S EMAIL ADDRESS IS WEIRD

Phishers try to mimic legitimate companies or individuals by using similar email addresses. Pay close attention to the sender's email address, as minor variations can be easily to overlooked. For example, instead of "paypal.com," a fake email may come from "paypaal.com" or "paypal-security.com."

Be very cautious of suspicious email addresses with irregular spelling or extensions that differ from the official company domain.

2 TEMPTING SUBJECT LINES

One of the crucial element's cybercriminals use to lure their victims is the subject line. Crafted to create a sense of urgency, curiosity, or familiarity, these subject lines aim to grab attention and convince recipients to open the email. Examples include:

- *Your Account Will Be Suspended!*
- *Urgent: Immediate Action Required!*
- *Security Breach: Change Your Password Now!*

3 LOGO BRANDING AND INCONSISTENCY

Phishing emails often lack proper branding and may use low-resolution logos or altered graphics. Legitimate companies take great care to ensure consistent branding across all their communication channels and not use very low quality or pixelated logos.

Be cautious if an email has inconsistent or poor-quality branding elements, as this could indicate a fake email that is attempting to deceive you.

4 USE OF GENERIC SALUTATIONS AND TONE

Phishing emails often lack personalized greetings and may address you as "Dear Customer" or "Valued User."

Legitimate organizations usually address you by name or use the information they have on file. If the email fails to address you specifically, exercise caution before proceeding. Also note that an email using your name does not make that email legit.

5 URGENT OR THREATENING LANGUAGE

Phishing emails often employ urgency or fear to coerce recipients into taking action immediately. Be cautious of messages that claim your account will be closed, a payment is overdue or you are facing legal consequences if you fail to comply. These tactics are designed to pressure you into making hasty decisions without thinking through the issues. Legitimate businesses communicate important matters in a professional manner and do not resort to panic-inducing language.

6 ASKING YOU TO CLICK SUSPICIOUS LINKS

One of the primary goals of phishing emails is to trick recipients into clicking on malicious links. Hover your mouse over hyperlinks without clicking to reveal the actual URL destination.

If the displayed link differs from the official website or looks suspicious, do not click on it. Additionally, be cautious of shortened URLs that can hide the true destination.

7 POOR GRAMMAR AND SPELLING MISTAKES

Phishing emails frequently contain grammatical errors, misspelled words, or awkward sentences. These mistakes can be indicators of fraudulent emails, as legitimate businesses generally have thorough proofreading processes in place.

Pay attention to the overall quality of the email's language and formatting, as well as any inconsistencies in tone or style.

8 UNEXPECTED EMAIL ATTACHMENTS

Exercise caution when encountering email attachments, especially if they come from unknown sources or are unexpected. Phishing emails often contain malicious attachments that can infect your device with malware or viruses.

Scrutinized the attachments carefully. Especially those in executable file formats (e.g., .exe, .bat) that can run harmful scripts.

www.dpcomputing.com.au