corsica technologies
www.corsicatech.com

PHISHING EMAIL EXAMPLES

One of the best ways to avoid getting tricked into a bad click on a phishing email is to know the common red flags of this type of attack. While not every email will include obvious markers -- and some are much more sophisticated than others -- it's beneficial to be aware of the most common signals.

Below we review 4 different examples, highlighting the red flags contained within the different messages. Take a look.

DROPBOX PHISHING EMAIL:

Suspicious Sender Name/Domain Name

TIP:
Do a search! A quick internet search confirms that "dropbox" and "dropboxmail" are the only legitimate Dropbox domains ever used in their emails.

From: Dropbox [mailto:filesharing@dropboxservice.com]
Sent: Thursday, November 16, 2017 11:40 AM
To: contact@dropboxservice.com
Subject: You've got a new pending document

Not Personalized to the Recipient

Hi,

The document received at 09:12 PM GMT-07:00 on Wednesday Nov 15, 2017 from your contact **is secure and ready for download.**

Preview or Direct download

Thank you.

P.S. Learn how to protect your account.

Vague Body Copy

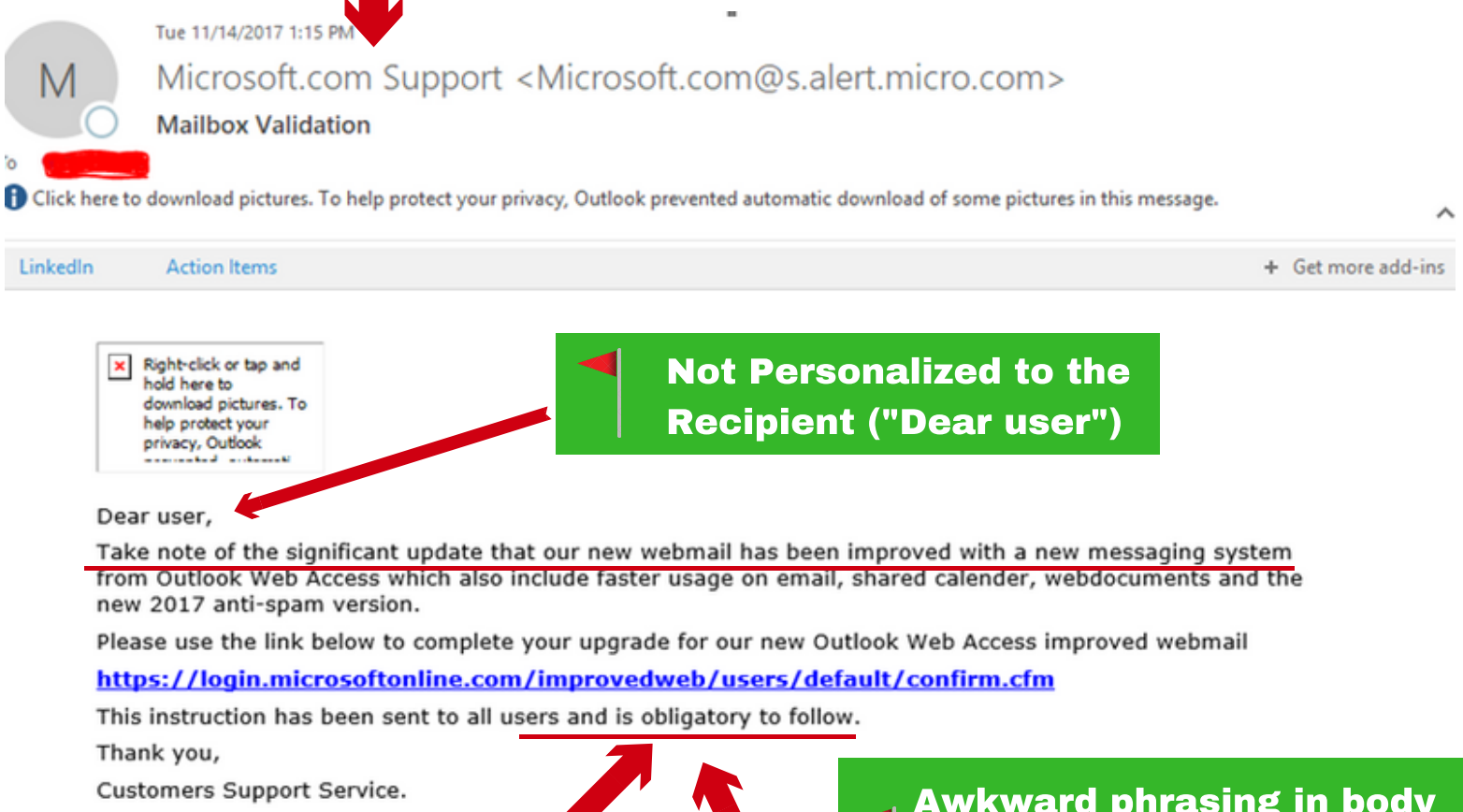
TIP: Even if you feel that this may be a legitimate document share, close this email and navigate on your own to your Dropbox account. Log into the site at the known URL and check from there for any new documents.

O365 PHISHING EMAIL:

Suspicious Sender Name/Domain Name

TIP:

It's important to carefully review the sender's name, as even minor differences can be a signal of a spoofed email. For example, using "Microsoft.com" as the sender's name instead of just Microsoft.



Not Personalized to the Recipient ("Dear user")

Awkward phrasing in body copy (see underlined sections)

There is an attempt to create a sense of urgency, by indicating that this is required.

This URL is suspect due to the lengthy text after "login.microsoftonline.com".

TIP:

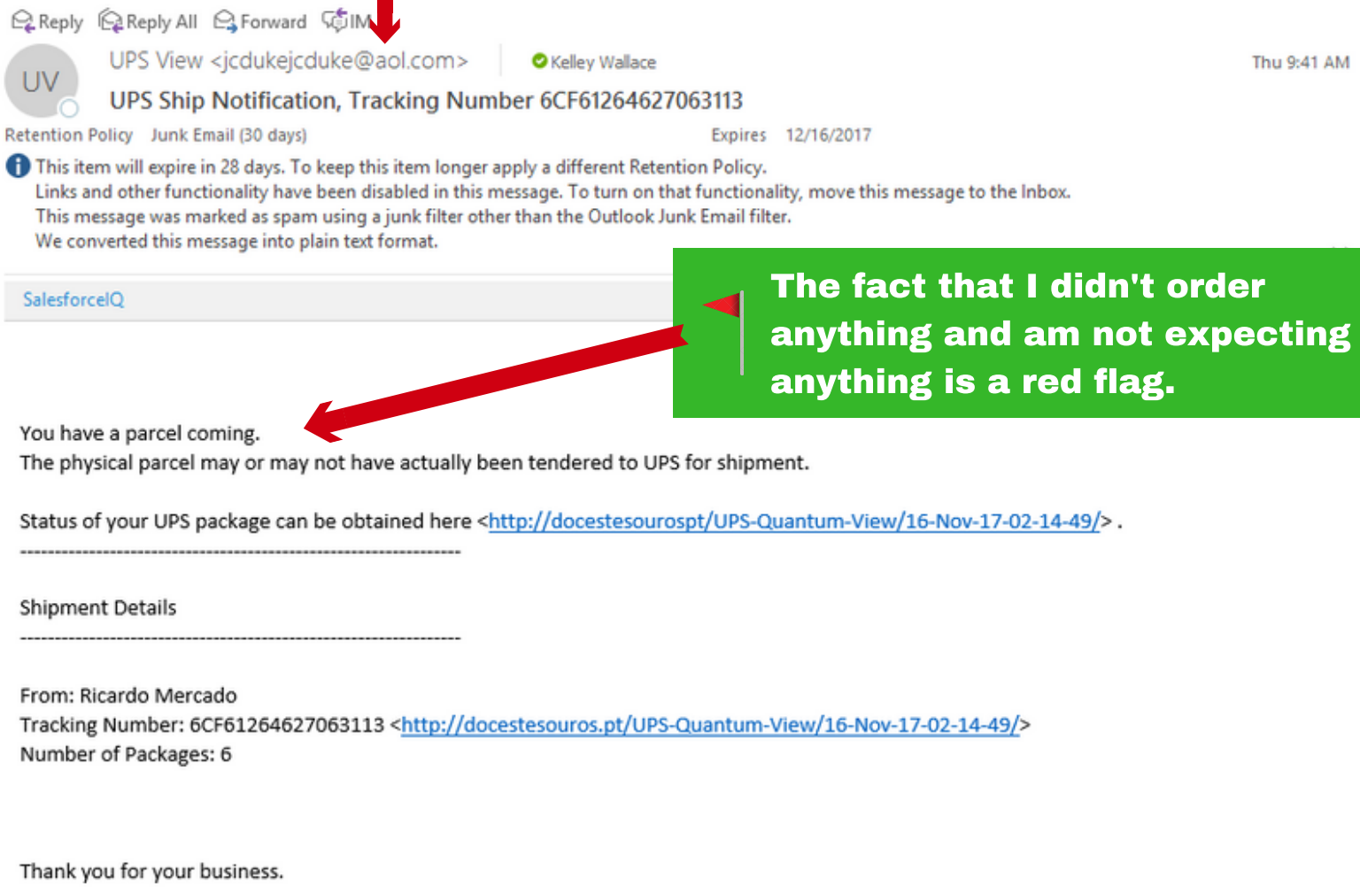
Best practice is to avoid following links in unverified or unsolicited emails. If you must check the claim in an email, stay in control of where you land by navigating on your own to your Office 365 account.

UPS SHIPMENT NOTIFICATION PHISHING EMAIL:

Sender Name/Email Domain Not a Match

TIP:

Always keep your anti-spam filters up-to-date. This will filter out those emails that have been flagged already, keeping your inbox free and avoiding any accidental clicks.



Reply Reply All Forward IM

UV

UPS View <jcdukejcduke@aol.com> Kelley Wallace Thu 9:41 AM

UPS Ship Notification, Tracking Number 6CF61264627063113

Retention Policy Junk Email (30 days) Expires 12/16/2017

This item will expire in 28 days. To keep this item longer apply a different Retention Policy.
Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
This message was marked as spam using a junk filter other than the Outlook Junk Email filter.
We converted this message into plain text format.

SalesforceIQ

You have a parcel coming.
The physical parcel may or may not have actually been tendered to UPS for shipment.

Status of your UPS package can be obtained here <http://docestesourospt/UPS-Quantum-View/16-Nov-17-02-14-49/> .

Shipment Details

From: Ricardo Mercado
Tracking Number: 6CF61264627063113 <http://docestesouros.pt/UPS-Quantum-View/16-Nov-17-02-14-49/>
Number of Packages: 6

Thank you for your business.

The fact that I didn't order anything and am not expecting anything is a red flag.

Most end-users who are cyber aware will spot this as an obvious phishing attempt; but simple curiosity will entice some users to click to find out what they're getting.

TIP:

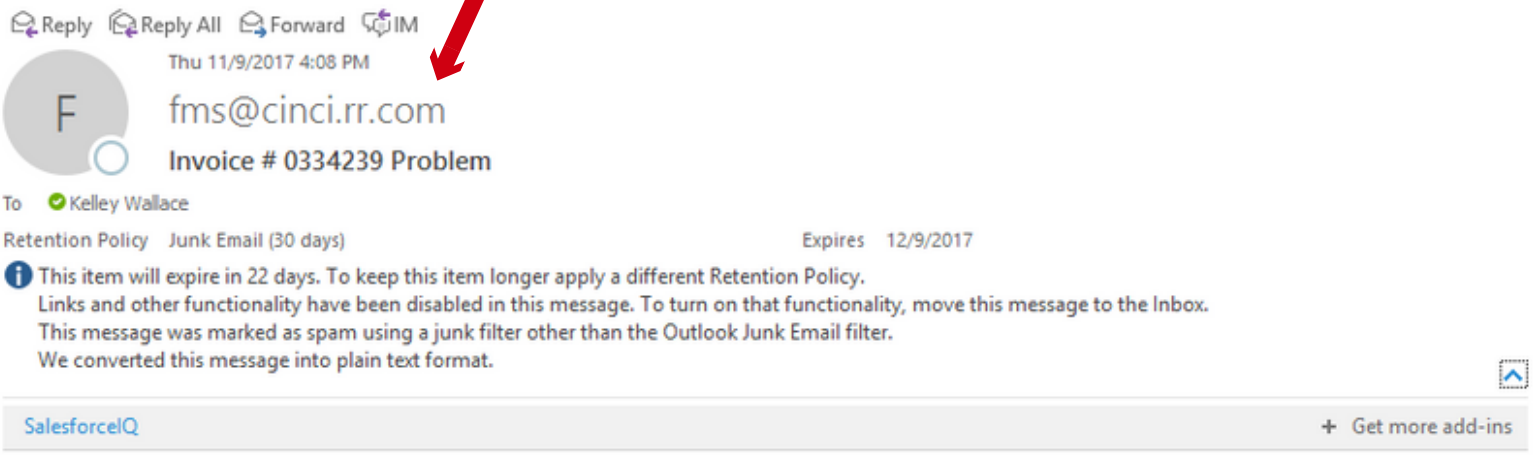
Understand social engineering tactics and how they are being used to target you. When you can recognize the psychological tricks, you can avoid becoming a victim.

OVERDUE INVOICE PHISHING EMAIL:

TIP:

Having established SOP's around any financial transactions can save your business from falling victim to the many phishing and spear phishing scams out there. Recommended best practice is to always verify a request to transfer funds directly with the person the email appears to be from.

Vague sender name / unknown domain



Good Morning,

Called you a few times without success. Decided to reach you by email. I need to know the status of this invoice below, itâ€™s way past due.
http://apgproperty.ca/Invoice-number-747853/

Warmest Regards,

rmerc@mercconstructioninc.com

The signature is listed as an email and that email differs from the sender, as does the domain name.

The body copy is intentionally vague and attempts to create concern by referencing an invoice as "way past due". This is designed to get an emotional reaction by the recipient, who will click out of concern that there is a problem with one of their accounts.

TIP:

A cautious end-user is your best defense against phishing emails. If there is anything at all about an email that seems odd or "off", trust your gut. Even emails that appear to be from a known source should be carefully evaluated.