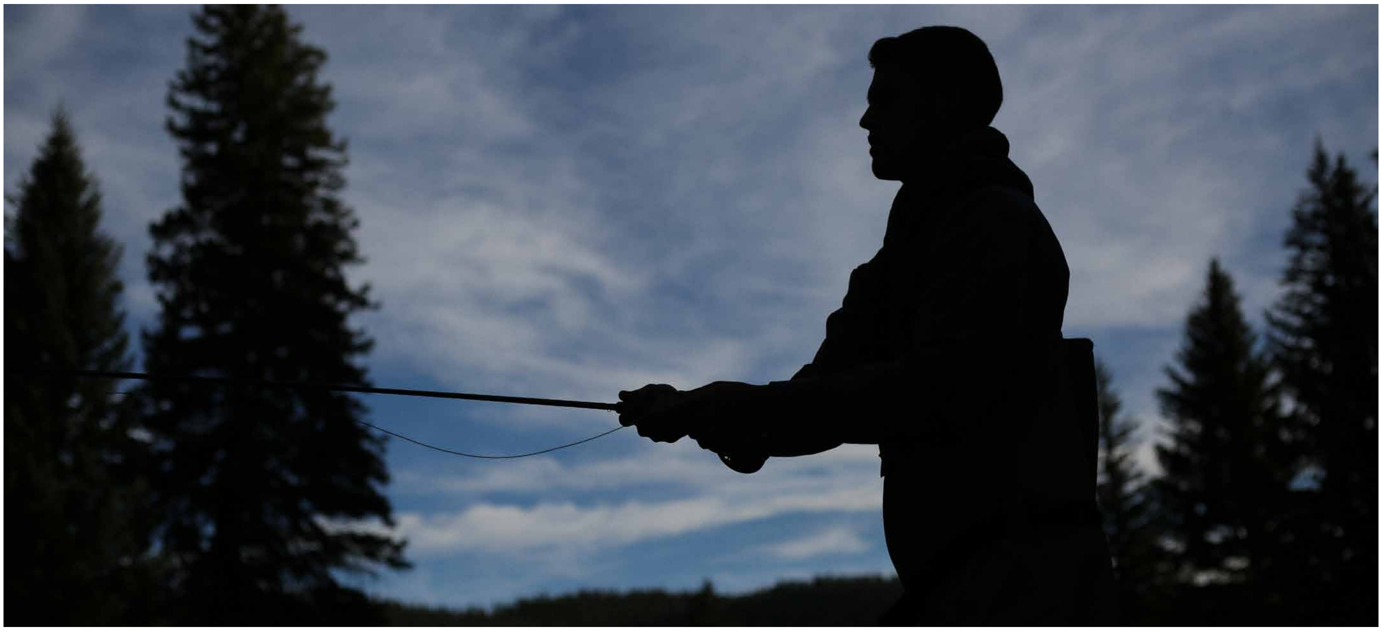
CRDS

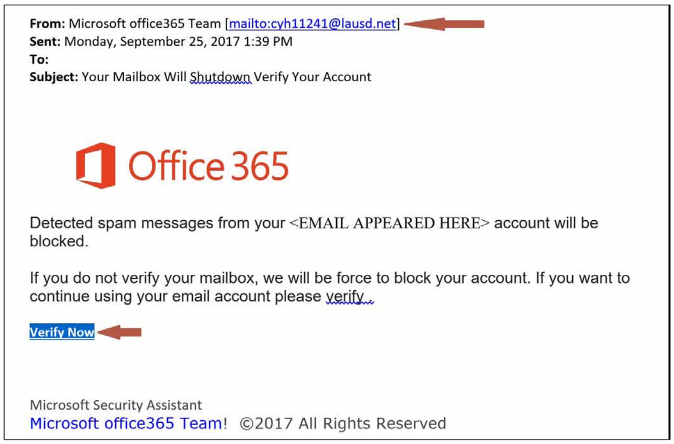
TECHNOLOGY GROUP INC.



There are approximately 156 million phishing emails sent out every day. Spam filters catch 90% of those emails, but about 16 million of them get through to users. Studies show that each day some 80,000 people provide the information requested and give phishers their personal data. Below you will find examples of common phishing formats that you can pass along to your staff so that they don't get caught.

Phishing Email 1:

This type of phishing email is intended to collect a user's Microsoft Office login data. It spoofs an email from Microsoft and includes a link where users are directed to input their login information.



From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify .

Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved

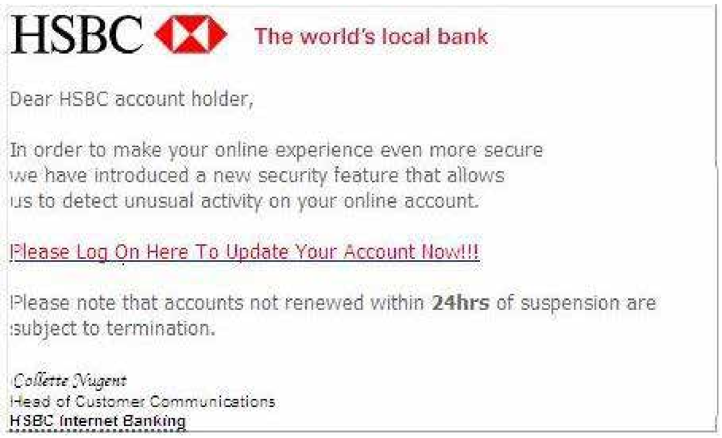
How to spot it:

The email sender is noted as "Microsoft office365 Team" but upon closer look at the sender's email, it shows an email address not associated with Microsoft. Users should always double-check sender information prior to taking any action proscribed in an email and should never log in to Office 365 from an email link.

Phishing Email 2:
This type of phishing email is intended to collect login information for a third-party software or website. Sometimes these emails can also try to get other login information once a user has clicked on the link, by asking them to sign into their email provider.

How to spot it:
As with the previous type of phishing email, it is important to check the validity of the sender. Most importantly, a user should never log in to a third-party software or website from a link provided in an email. This is almost certainly a spoof email intended to get your personal information. In the very rare instance that it is not, there is nothing to be lost by manually loading the website and logging in that way.

Common companies that are used for these type of emails are Dropbox, Paypal, Netflix, Apple accounts, and bank accounts.


HSBC The world's local bank

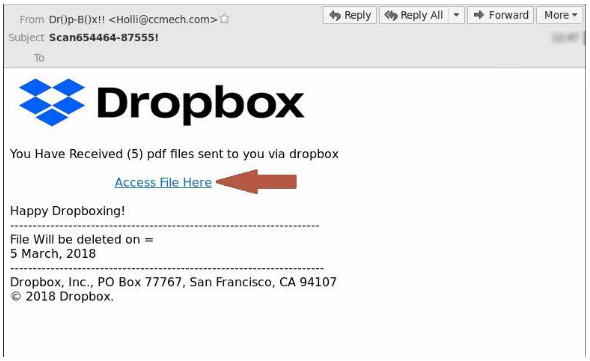
Dear HSBC account holder,

In order to make your online experience even more secure we have introduced a new security feature that allows us to detect unusual activity on your online account.

Please Log On Here To Update Your Account Now!!!

Please note that accounts not renewed within **24hrs** of suspension are subject to termination.

Collette Nugent
Head of Customer Communications
HSBC Internet Banking


From Dr()p-B()x!! <Holli@ccmech.com>
Subject **Scan654464-87555!**
To

Dropbox

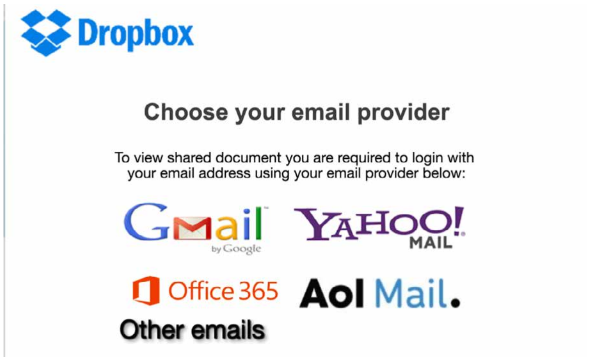
You Have Received (5) pdf files sent to you via dropbox

Access File Here

Happy Dropboxing!

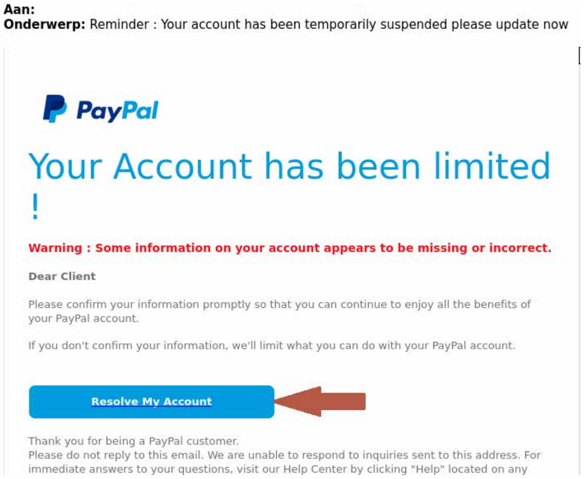
File Will be deleted on =
5 March, 2018

Dropbox, Inc., PO Box 77767, San Francisco, CA 94107
© 2018 Dropbox.


Dropbox

Choose your email provider

To view shared document you are required to login with your email address using your email provider below:


Aan:
Onderwerp: Reminder : Your account has been temporarily suspended please update now

PayPal

Your Account has been limited !

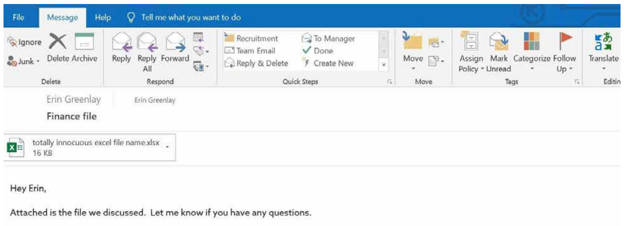
Warning : Some information on your account appears to be missing or incorrect.

Dear Client

Please confirm your information promptly so that you can continue to enjoy all the benefits of your PayPal account.

If you don't confirm your information, we'll limit what you can do with your PayPal account.

Thank you for being a PayPal customer.
Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any



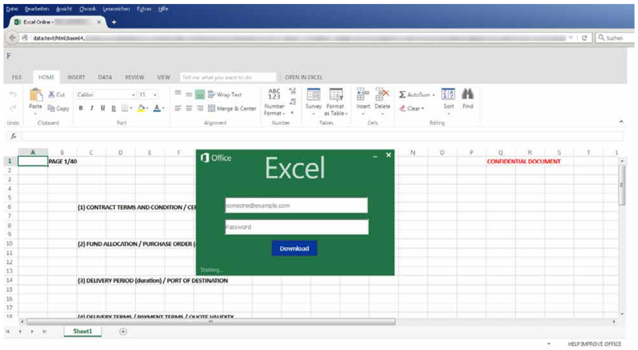
Erin Greenlay | Erin Greenlay

Finance file

totally innocuous excel file name.xlsx
16 KB

Hey Erin,

Attached is the file we discussed. Let me know if you have any questions.



PAGE 1/40

CONFIDENTIAL DOCUMENT

(1) CONTRACT TERMS AND CONDITION / CE

(2) FUND ALLOCATION / PURCHASE ORDER (

(3) DELIVERY PERIOD (duration) / PORT OF DESTINATION

(4) DELIVERY TERMS / PAYMENT TERMS / QUOTE VALIDITY

someone@example.com

Password

Phishing Email 3:
This type of phishing email is intended to look like it comes from someone within your organization. These emails tend to be very sophisticated, using the email signature of the individual they are posing as, and even naming the attachment as something that your organization would distribute. It is likely with this type of email that they have done more than a cursory investigation into your organization and likely have information about who the principals or C-suite staff are.

The way these emails work is the sender poses as someone from within your organization and attaches a file to the email. When you go to open the file it will redirect to a web page, because the file is "encrypted" and request that you enter your login credentials to access it.

These emails are intended to get your Microsoft Office login so that they can access your account and use your email. The intent, once they have email access, is generally to approve payments for invoices which are fraudulent, or change the bank account information for an existing vendor, and extract payment via EFT or wire transfer.

How to spot it:
Encrypted documents (whether Word, Excel or PDF) do not require your login credentials to access them. A password or encryption key should be provided by the sender in a separate email, or another format.

The email address of the sender will likely not match the person within your organization's email address. But, if the individual's account has been compromised, it might. Be sure to follow up with your coworkers if you receive a file that you were not expecting and verbally confirm any new vendors, or any changes in vendor bank account information, before processing payments.

Be cautious and vigilant:
If you feel an email might be suspicious, attach the email to a support request email to CRDS. By attaching the email you are providing it in its original format and CRDS can trace the sender information. CRDS staff will let you know if an email is legitimate and, if it is not, can block the associated location and email domain to prevent further emails from the sender.

If you have any questions or concerns, or feel you may have been successfully phished, please get in contact with our support team right away at 1.800.737.3417 or support@crdsgroup.com.