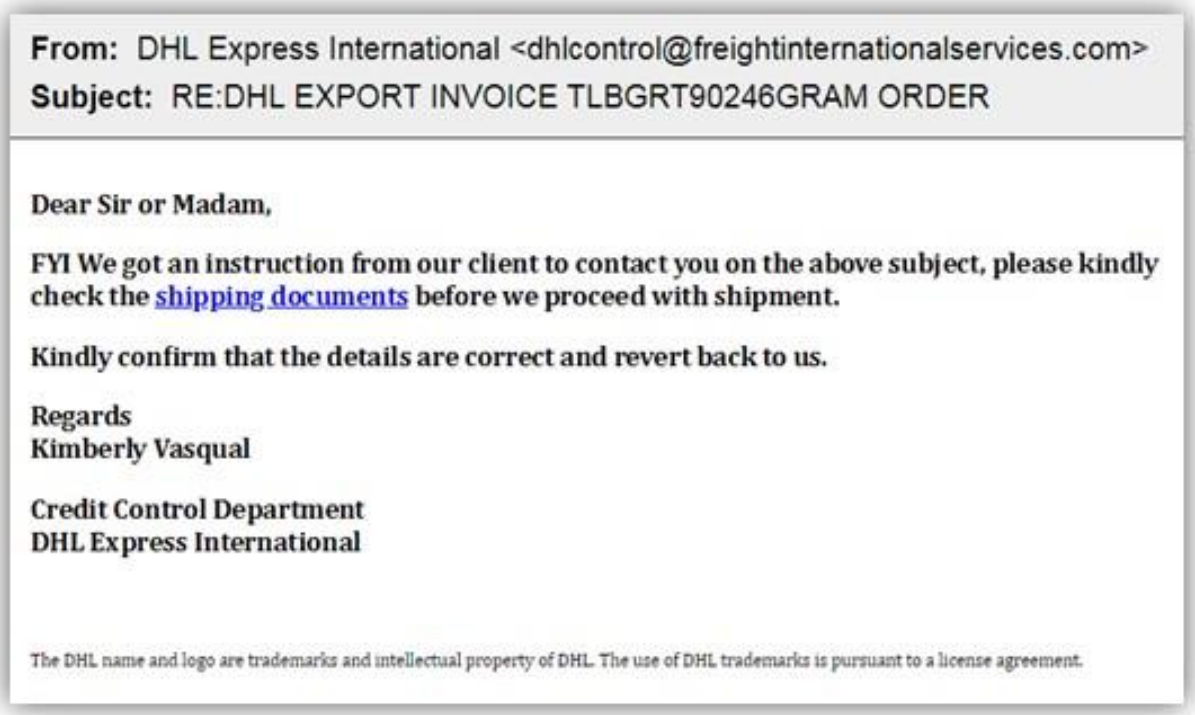
August 2019 Phishing Exercise Recap: Shipping Documents
August 28, 2019

The Office of Information Technology's (OIT) August 2019 phishing scenario invoked curiosity upon the recipient to "check the shipping documents before we proceed with shipment." This email used curiosity tactics by using phrases such as "we got instruction from our client to contact you" to get employees to click on the "shipping documents" link in the email. A close examination of the email shows the look-alike DHL sending domain and email address. Over 810 employees reported this phishing email to the PhishTrap, and 412 employees clicked on the link.



From: DHL Express International <dhlcontrol@freightinternationalservices.com>
Subject: RE:DHL EXPORT INVOICE TLBGRT90246GRAM ORDER

Dear Sir or Madam,

FYI We got an instruction from our client to contact you on the above subject, please kindly check the shipping documents before we proceed with shipment.

Kindly confirm that the details are correct and revert back to us.

Regards
Kimberly Vasqual

Credit Control Department
DHL Express International

The DHL name and logo are trademarks and intellectual property of DHL. The use of DHL trademarks is pursuant to a license agreement.

Package/shipping delivery phishing emails are easy bait for attackers to catch employees. The sender invokes a strong sense of curiosity to get you to click on the link. The link may lead to a malware download or a fake website prompting for login credentials. The best defense is to not react in haste.
To avoid falling victim to phishing emails, OIT recommends all employees:

- **Review and assess before clicking on the links.** Do not click on the links in an email. When ordering items online, ask the vendor **in advance** for the delivery company, or tracking number. If you order a package or expect a delivery, check your account with the vendor, such as, Amazon for shipping details
- **Enroll in Two-Factor Authentication (2FA)**

All employees must enroll in 2FA by September 30, 2019. 2FA is an added layer of security that requires log on authentication using the first factor, your user name and password, and the second factor, your mobile phone, tablet, or landline to confirm your login requests. To learn more about 2FA, please visit https://mcblogs.montgomerycollege.edu/itprojects/2fa.

- **Report** all suspicious emails to the Phishtrap for analysis using the Report Phishing tool located on the Microsoft Outlook toolbar or in the Outlook mobile app for iPhone and Android. IT Security will analyze the content and web links and if legitimate, will send the email back to you.

OIT encourages all employees who need assistance in spotting a phishing email to take the Cybersecurity e-courses within MC Learns. The e-courses are short videos that provide employees with the skills needed to detect malicious emails.