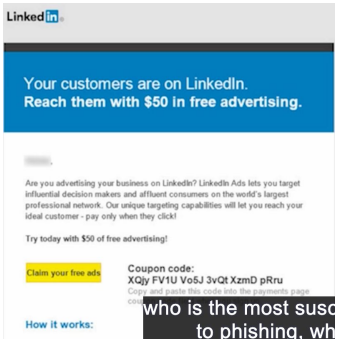
Nicolas Barraclough
11/22/2020
CS373 - Defense Against the Dark Arts

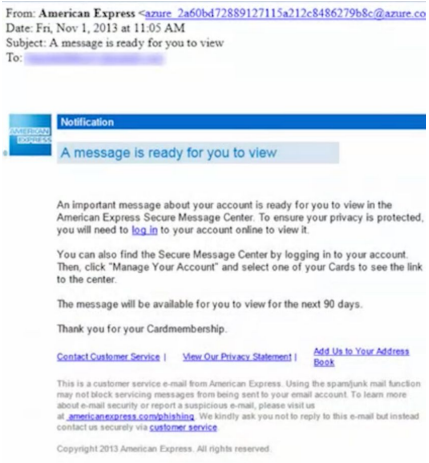
Week 8 Write-Up

Phishing Quiz

The phishing quiz let us take a look at many different suspicious-looking emails in an attempt to determine if the email was legitimate or phishing. I will note my thoughts on each email below:

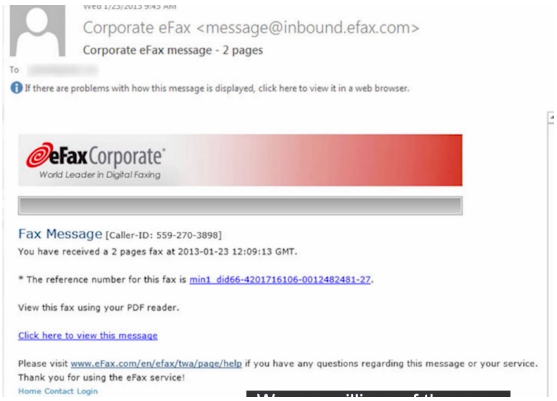
1. LinkedIn - At first glance, this email looks legitimate, but a little suspicious given that LinkedIn doesn't normally give out coupon codes nor do they really have a need to. In effort to avoid false-positives, I would mark this as spam at the very least or given more detective analysis, I might mark it as phishing just to be safe





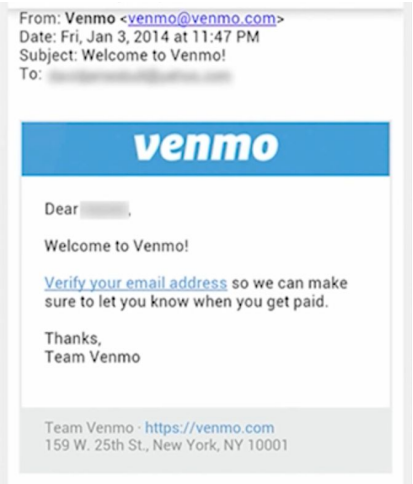
2. American Express - This email was obviously a phishing email. To start, the email address that this was sent from does not appear to have any relation to AmEx. Second, the email is asking for a call to action where the user is requested to enter specific account information. Major red flag - definite phishing email.

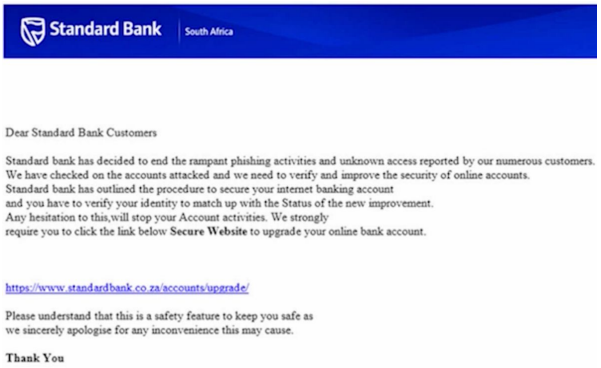
3. US Airways - Again, this email has a sender that should immediately raise a red flag. Second, flight confirmations typically include the customer's name and do not require the reservee to click a link to continue on to the reservation details. This is a phishing email.



4. eFax - This email looks legitimate right off the bat. It displays the user's caller ID, fax reference numbers, and times of the faxes. However, all of the links in the email contain the same URL. The URL is to an index page, not a PDF document. I would say this is a legitimate email.

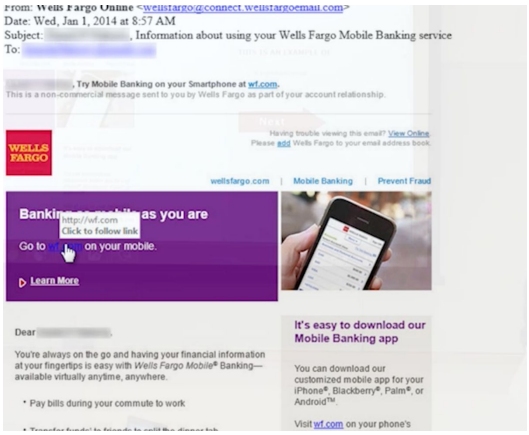
5. Venmo - The only thing that would make this email stand out as non-legit, is if I had received without having recently set up an account with Venmo. To clarify, I already have Venmo set up with my account already verified. If I received this email I would know that my account is already verified. If I received this email without ever setting up a Venmo account, I would know that it is not legitimate. Without any context of if the receiver had previously set up an account and had not already verified, I would say this is legitimate.

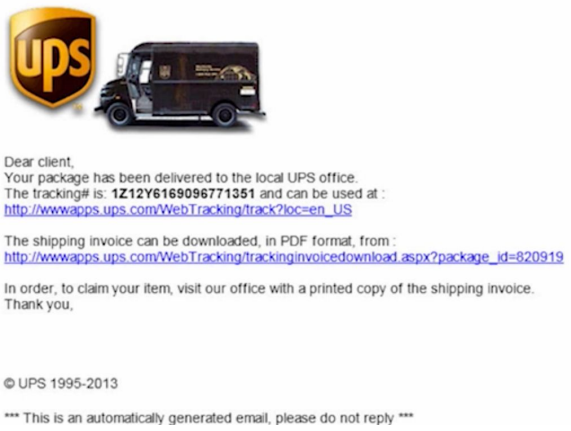




6. Standard Bank - Okay, this one is obviously phishing. If I received this and I have not had any association with Standard Bank in South Africa, I can be 100% certain that this is a phishing email.

7. Wells Fargo - The only thing that looks suspicious in this email is the sender address, and the amount of links within the email. But, if you are a Wells Fargo customer, I guess this is a pretty common email to receive. My thoughts and the class consensus is that this email is legit.





Dear client,
Your package has been delivered to the local UPS office.
The tracking# is: **1Z12Y6169096771351** and can be used at :
http://wwwapps.ups.com/WebTracking/track?loc=en_US

The shipping invoice can be downloaded, in PDF format, from :
http://wwwapps.ups.com/WebTracking/trackinginvoicedownload.aspx?package_id=820919

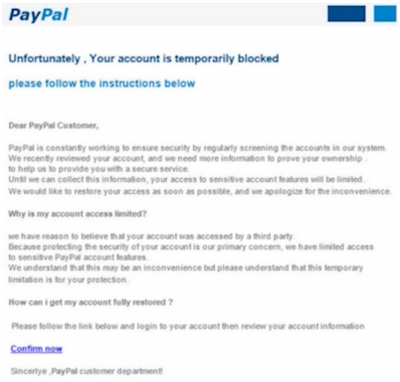
In order, to claim your item, visit our office with a printed copy of the shipping invoice.
Thank you,

© UPS 1995-2013

*** This is an automatically generated email, please do not reply ***

8. UPS - I order packages that are delivered via UPS and I have never gotten an email like this one. If I was not expecting a package, I would know automatically that this is a phishing email. If I did have a package, I would take a look at the links provided in the email (without clicking on them) and immediately know that this is a phishing email.

9. PayPal - If this email is read and analyzed for all of it's typos, it would be fairly easy to tell that this is a phishing email. The email is riddled with errors which should be a dead giveaway in any context that the email is not legitimate.



PayPal

Unfortunately , Your account is temporarily blocked

please follow the instructions below

Dear PayPal Customer,

PayPal is constantly working to ensure security by regularly screening the accounts in our system.
We recently reviewed your account, and we need more information to prove your ownership ,
to help us to provide you with a secure service.
Until we can collect this information, your access to sensitive account features will be limited.
We would like to restore your access as soon as possible, and we apologize for the inconvenience.

Why is my account access limited?

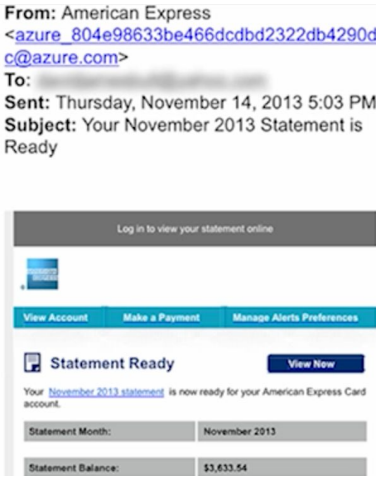
we have reason to believe that your account was accessed by a third party.
Because protecting the security of your account is our primary concern, we have limited access
to sensitive PayPal account features.
We understand that this may be an inconvenience but please understand that this temporary
limitation is for your protection.

How can I get my account fully restored ?

Please follow the link below and login to your account then review your account information

Confirm now

Sincerlye ,PayPal customer department



From: American Express
<azure_804e98633be466dcdbd2322db4290dc@azure.com>
To: [redacted]
Sent: Thursday, November 14, 2013 5:03 PM
Subject: Your November 2013 Statement is Ready

Log in to view your statement online

View Account | Make a Payment | Manage Alerts Preferences

Statement Ready — View Now

Your November 2013 statement is now ready for your American Express Card account.

Statement Month:	November 2013
Statement Balance:	$3,633.54

10. American Express (mobile) - This email has the same suspicious sender address as the previous AmEx email, so a red-flag is raised there. The rest of the email actually appears to be legitimate. If the links go to places that are associated to American Express, I would guess that this email is legit.

Summary of Phishing Quiz:

Key takeaways of this quiz is to be safe rather than sorry. A false negative is better than a false positive. If an email looks suspicious, it is safe to assume that it is. Most phishing emails contain a call to action for the user to go to a link or download something in order to provide necessary information. The safest thing to do with a call to action is to go to the website of the company and find the call to action within the account rather than the email.

In the remainder of the lecture, we learned about spam terminology & common methods and anti-spam tools.

Terminology:

- Spam: Unsolicited emails typically sent in bulk where the receiver is not usually targeted.
- Spamtrap: A honeypot, usually an email address, that's used to collect spam.
- Botnet: A collection of devices with internet connection, each of which is running bots. They are typically used for attacks that require a large number of individual devices like in a DDOS attack.
- Snowshoe spam: A strategy for spamming where the spam emails are spread out over various domains and IP addresses to weaken anti-spam filters.
- Phishing: Emails sent with malicious intent in hopes of tricking users into either revealing personal or confidential information or allowing access to a network.
- Spear phishing: Same as general phishing, except with specific targets.
- Realtime Blackhole List: A list of IP addresses that spam typically originates. Useful for blocking with a blacklist.
- Bayesian logic: Using the knowledge of prior events to predict future events.

Tools:

- DIG: Command-line(CL) tool for investigating DNS records.
- WHOIS: CL tool for searching IP/Domain registration information.
- GREP, AWK, SED: Various CL tools used for data parsing and file content manipulation.
- Spamhaus.org: The world leader in supplying realtime highly accurate threat intelligence to the Internet's major networks.