Week 3: Ways to spot a phishing email

Like a fisherman using a lure to hook a fish, identity thieves try to lure you into giving personal information by making what looks like a legitimate request from an organization you trust. These might look like they are from a bank, credit card company, or even from a trusted brand, such as Microsoft. Unfortunately, phishing scams can be highly effective.

Phishers count on people not really taking the time to read their emails before they click on links or download attachments. With the significant amount of messages we get each day, many of us tend to skim each one. It's estimated that the average office workers spends just 10-20 seconds reading individual emails. The odds, then, are in the phisher's favor. But if you slow down just a bit, you can spot a phish pretty quickly. We provide the most common ways to spot a phish, some examples with screenshots, a quiz to test your "phish-detector", and the steps to take when you do receive a suspicious email.

1. **The message asks you to confirm personal information.** The message wants you to confirm sensitive information - legitimate companies ***never*** request usernames, passwords, credit card or bank account information via email. Emails requesting you to confirm personal information that you would never usually provide, such as banking details or login credentials are red flags.

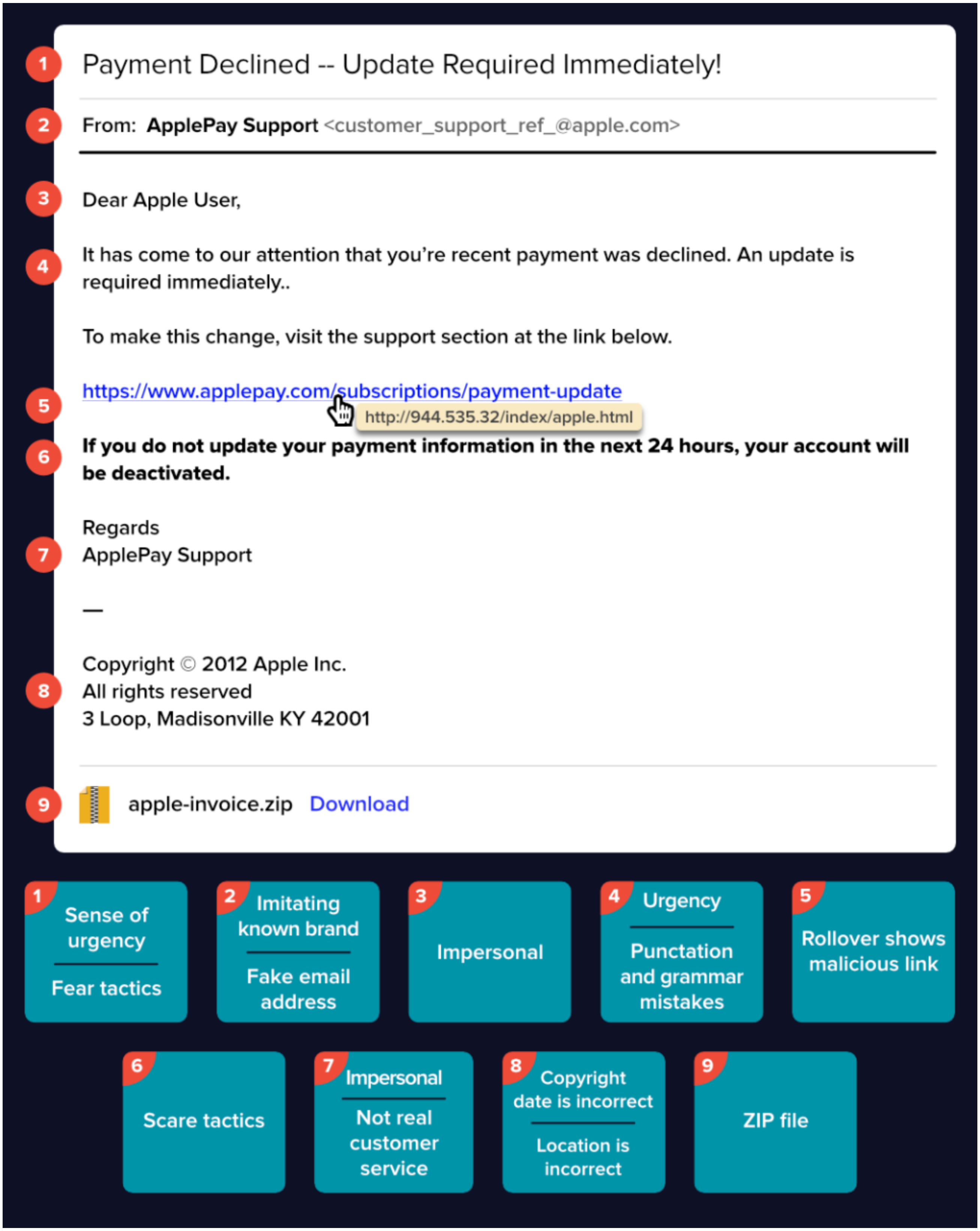
2. **There's a suspicious attachment.** Unexpected emails containing attachments are also big red flags. If you receive an email from a company out of the blue that contains a link or an attachment, you can bet it is a fake and has malicious intent. The attachment could contain a malicious URL or Trojan, leading to the installation of a virus or malware on your PC.

3. **The message is designed to make you panic.** The message contains unrealistic threats or attempts to blackmail. Phishing artists who use intimidation may send messages claiming to be a law enforcement agency, the IRS, or the FBI. Others will send messages claiming to have hacked your computer's webcam and recorded your activities. In either case, the email will threaten jail time or exposure if their demands are not met.

4. **It's poorly written.** Possibly the easiest way to recognize a fake email is bad grammar. An email from a legitimate organization should be well written. Read the email and check for spelling and grammatical mistakes, as well as strange wording.

5. **The web and email addresses do not look genuin**e. It is often the case that a phishing email will come from an address that appears to be genuine. Criminals aim to trick recipients by including the name of a legitimate company within the structure of email and web addresses. If you only glance at these details they can look very real but if you take a moment to actually examine the email address you may find that it's a bogus.

Can you spot all the signs this is a phishing email?



1 Payment Declined -- Update Required Immediately!

2 From: **ApplePay Support** <customer_support_ref_@apple.com>

3 Dear Apple User,

4 It has come to our attention that you're recent payment was declined. An update is required immediately..

To make this change, visit the support section at the link below.

5 https://www.applepay.com/subscriptions/payment-update

http://944.535.32/index/apple.html

6 **If you do not update your payment information in the next 24 hours, your account will be deactivated.**

Regards
7 ApplePay Support

—

Copyright © 2012 Apple Inc.
8 All rights reserved
3 Loop, Madisonville KY 42001

9 apple-invoice.zip Download

1 Sense of urgency / Fear tactics

2 Imitating known brand / Fake email address

3 Impersonal

4 Urgency / Punctuation and grammar mistakes

5 Rollover shows malicious link

6 Scare tactics

7 Impersonal / Not real customer service

8 Copyright date is incorrect / Location is incorrect

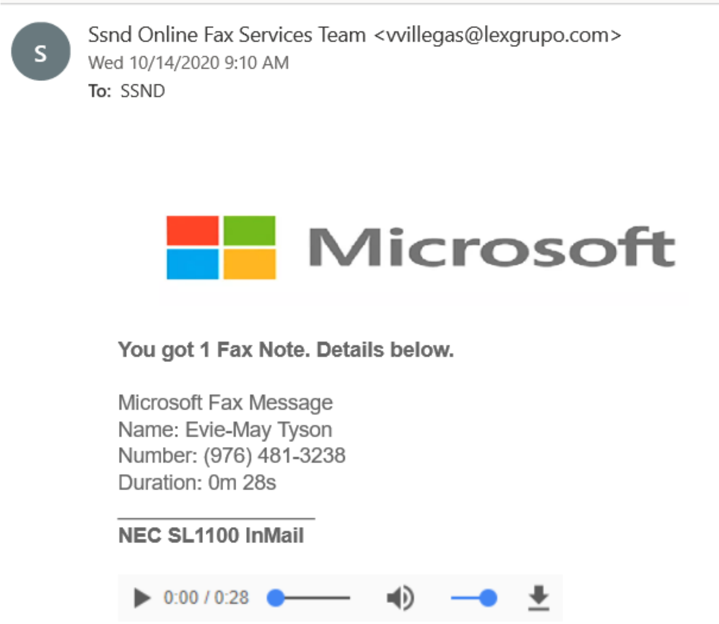
9 ZIP file

Image courtesy of Varonis

Screenshots of examples we've seen in the last month

In this example, the message looks legitimate because of the official Microsoft logo and even makes it look like it comes from SSND with the fake "SSND Online Fax Services Team" name. Upon a closer look though, the email is coming from the domain @lexgrupo.com which doesn't match up.

Once the play button is clicked, the user is redirected to a fake credentials form to try to lure one into entering their username and password.



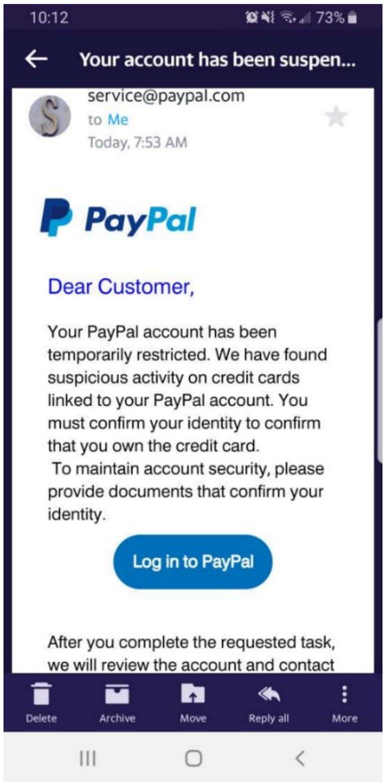
S

Ssnd Online Fax Services Team <vvillegas@lexgrupo.com>
Wed 10/14/2020 9:10 AM
To: SSND

You got 1 Fax Note. Details below.

Microsoft Fax Message
Name: Evie-May Tyson
Number: (976) 481-3238
Duration: 0m 28s

NEC SL1100 InMail



Your account has been suspen...

service@paypal.com
to Me
Today, 7:53 AM

Dear Customer,

Your PayPal account has been temporarily restricted. We have found suspicious activity on credit cards linked to your PayPal account. You must confirm your identity to confirm that you own the credit card.
To maintain account security, please provide documents that confirm your identity.

Log in to PayPal

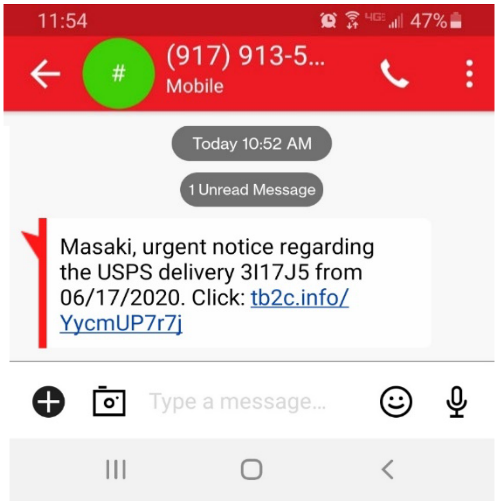
After you complete the requested task, we will review the account and contact

PayPal is one of the top ten spoofed brands. Scammers sends messages to individuals whether or not they have PayPal accounts.

You can immediately recognize this as a spoof if you don't have a PayPal account. Other ways to tell it's a scam is by the subject line "Your account has been suspended" and by the "Dear Customer" greeting.

- PayPal will never ask you to enter your password unless you're on the login page.
- Emails from PayPal will always address you by your first and last name or by your organization name.

Phishing scams are not limited to emails; they can also arrive via text message. The USPS, UPS, and FedEx brand are used by scammers to try an lure one into sharing personal information, whether it be passwords or credit card information. If you get one of these, do not click/tap on the link. Instead, if you think it is legitimate, contact the company where you placed your order.



(917) 913-5...
Mobile

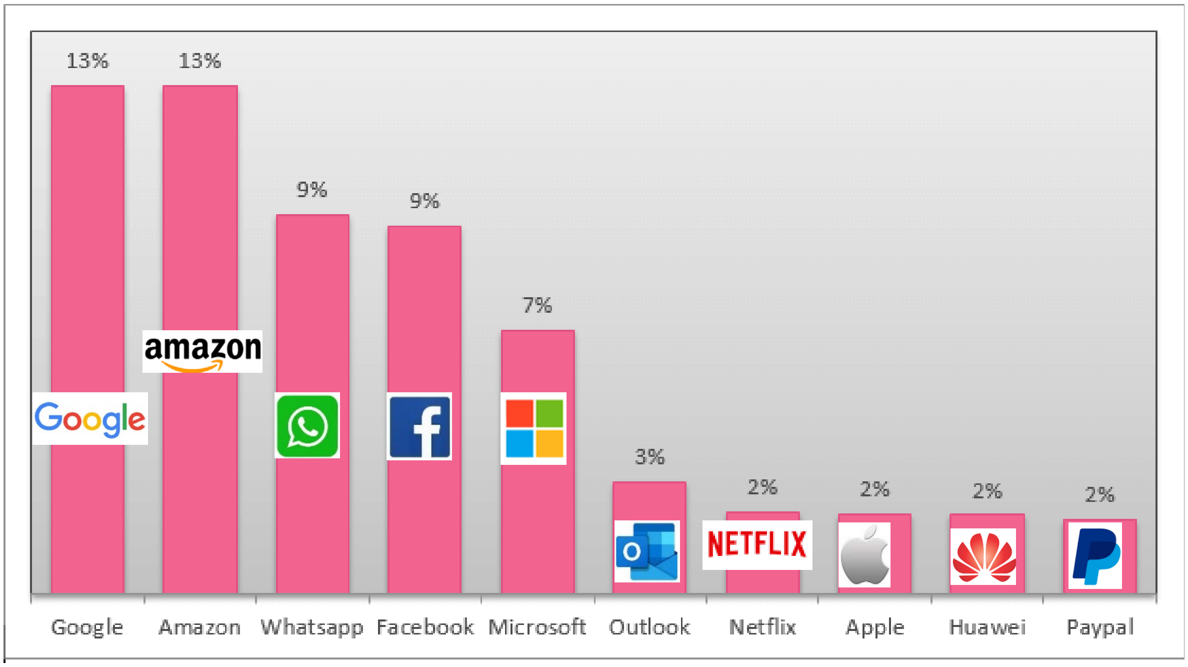
Today 10:52 AM

1 Unread Message

Masaki, urgent notice regarding the USPS delivery 3I17J5 from 06/17/2020. Click: tb2c.info/YycmUP7r7j

Top ten most impersonated brands in phishing attempts

If you receive an email that looks to be from any of these brands be extra cautious.



Statistics (Q2, 2020) courtesy of [Checkpoint]()

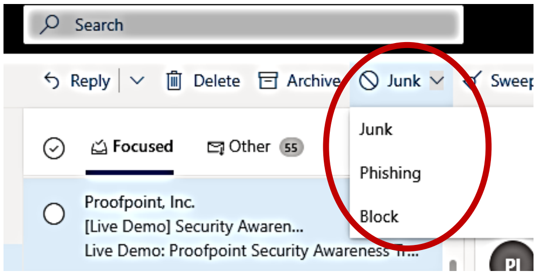
Test your phish-detector

Google – owner of Gmail, a major target for phishing – thinks it can help people spot suspicious emails. They have created a handy quiz to test people's knowledge. Many of you will feel confident, but beware there are some tricky ones!

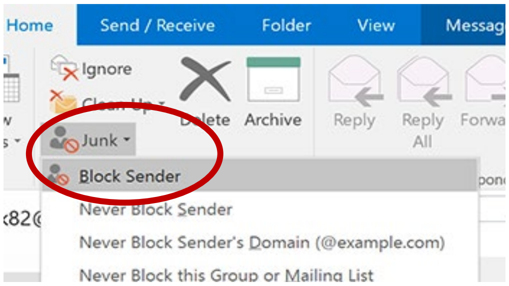
Interestingly, these are based on real life attacks, so are able to really test your abilities to spot phishing attempts in the wild. [Test your ability to spot a phish!]()

Handling scam messages

If you receive a phishing or junk message, you can easily mark the messages as such via the toolbar or by right-clicking for further action.



Outlook Online (webmail) Junk Mail Menu



Outlook 2016 (desktop version) Junk Mail Menu

If you've accidentally clicked a suspicious link or shared personal information, please reach out to us immediately at 1-800-373-7521 so we can change your password, scan the computer, and take any additional steps needed.