WHITEPAPER

PHISHING: DON'T GET HOOKED

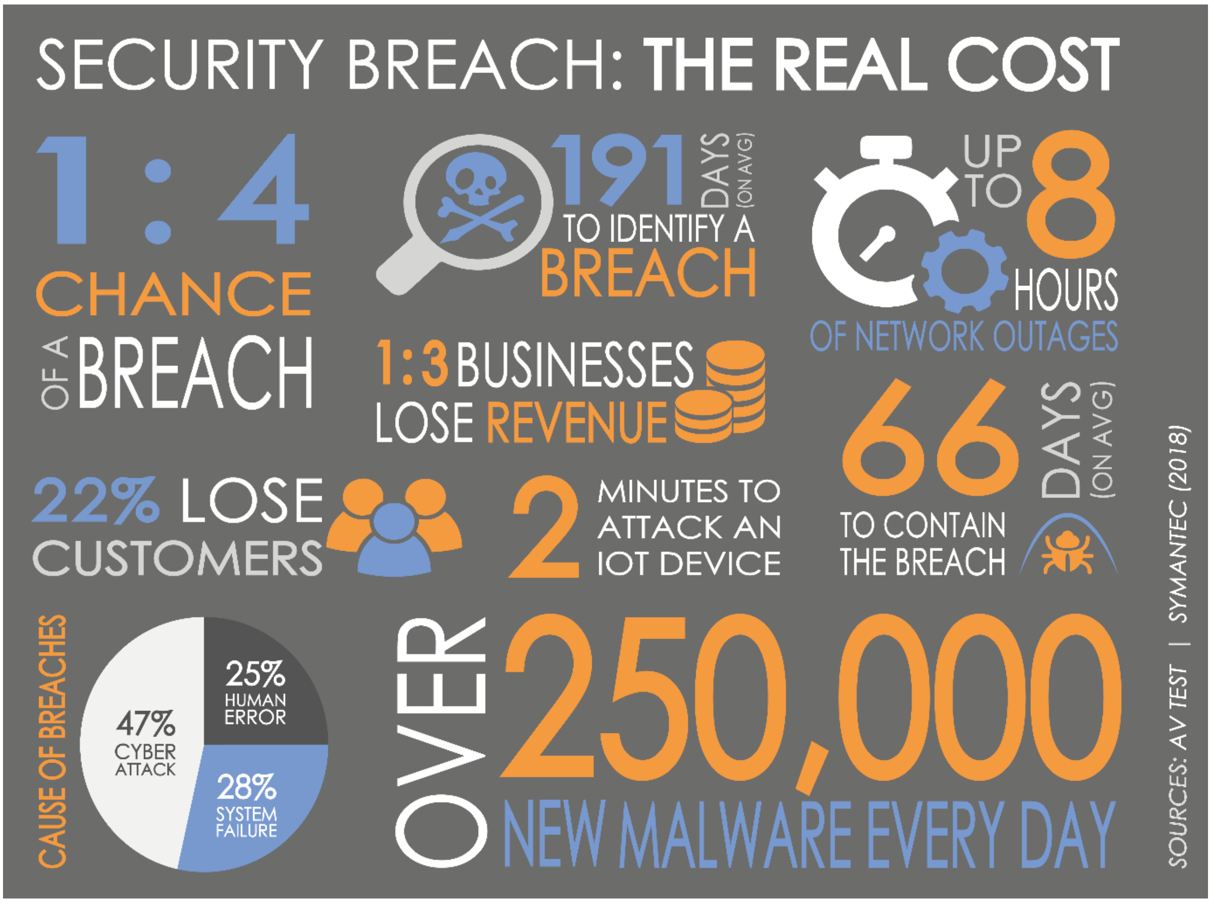
HOW TO SPOT THE RED FLAGS

seriun®

PHISHING: DON'T GET HOOKED

Phishing attacks can strike at any time and leave a company in turmoil. They are the easiest way hackers gain access to confidential or sensitive information. Most cyber-attacks begin with email phishing.

Once a cybercriminal gains access to your business – he has full reign to deploy other attacks and cause real damage. There are some scary statistics out there around security breaches (as depicted in the infographic below). The facts are that cyber-attacks are prolific and growing in number by the day, and they can take a significant amount of time to detect, meanwhile the damage is done.



Looking at **phishing** specifically, 95% of phishing breaches are due to human error. So, if your employees don't know the red flags of a phishing email, your company is at risk. On average it takes someone 16 minutes to click a malicious link in a phishing email, yet twice as long for a phishing campaign to be reported to the IT department – according to a recent study by Verizon.

50% of malware is installed via email, so the longer it takes to report or detect, the more extensive the damage could be.

Phishing scams are becoming harder to spot as they grow in sophistication and can convincingly mimic a credible source or a reputable company. They always have a call to action encouraging the recipient to download an infected file or click a malicious link. All it takes is one click and suddenly your personal/financial information could be gathered and stolen.

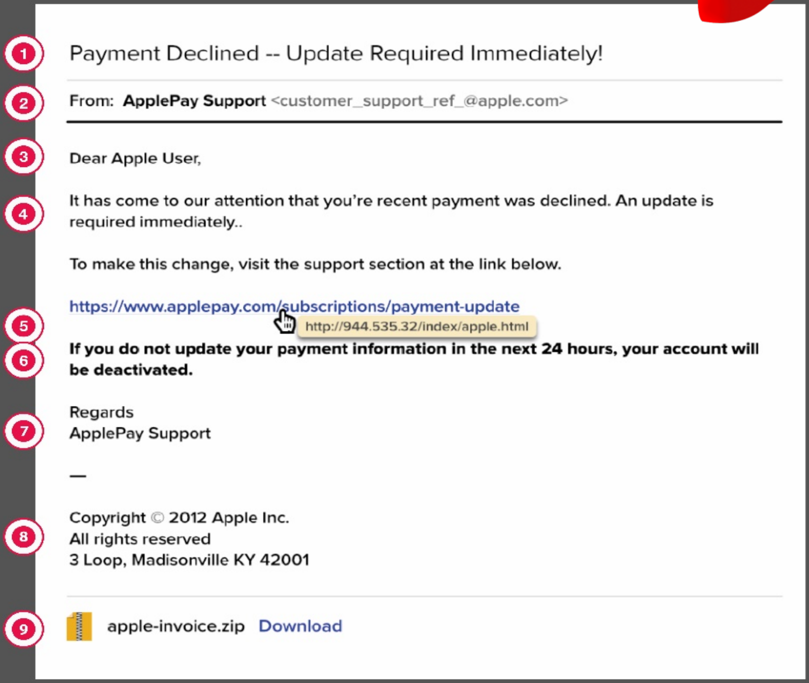
HOW TO DETECT A PHISHING ATTACK

The infographic below looks at the most common red flags in a typical phishing email. Please take time to review them in detail and the explanations that follow.

PHISHING - THE RED FLAGS

From malicious links that take you to fake web pages to infected attachments, phishing emails can hook you and reel you in, obtaining your private information and your money - doing irrecoverable damage to your business!

COULD YOU SPOT A FAKE?



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.**

7 Regards
ApplePay Support

—

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

9 apple-invoice.zip Download

1 Sense of urgency — Fear tactics

2 Imitating a known brand — Fake e-mail address

3 Impersonal

4 Urgency — Punctuation & grammar mistakes

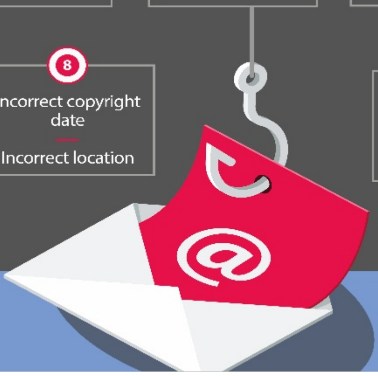
5 Rollover shows malicious link

6 Scare tactics

7 Impersonal — Not real customer service

8 Incorrect copyright date — Incorrect location

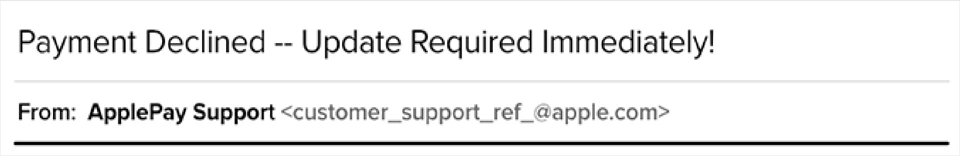
9 Zip file



seriun trusted tech partner

Subject line

There is often a sense of urgency created in the subject line using scare tactics. A financial theme is quite common for the topic i.e. 'Your account has been compromised'. The hope is that the recipient will respond without a second thought, and long before they realise it was indeed a scam.



Payment Declined -- Update Required Immediately!

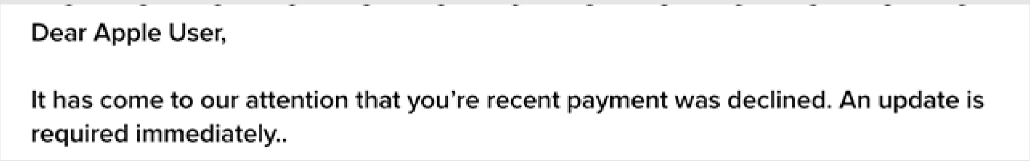
From: **ApplePay Support** <customer_support_ref_@apple.com>

'From' field

A successful phishing campaign must convince the recipient it was from a credible source. It must have a similar look and feel to that of the company it is mimicking, it must also be written in a similar style – the cybercriminal(s) will have done sufficient research to execute this. On closer inspection you will notice the sender name and email address (as in the example above) are not in the correct format how Apple would normally be presented.

'To' field

Be wary if an email comes through which addresses you impersonally with either 'Dear Customer' or 'Dear User'. Even though many legitimate businesses still send out emails en masse when they are promoting an offer or new product, they will still address you by name, especially if requesting an information update for their records.



Dear Apple User,

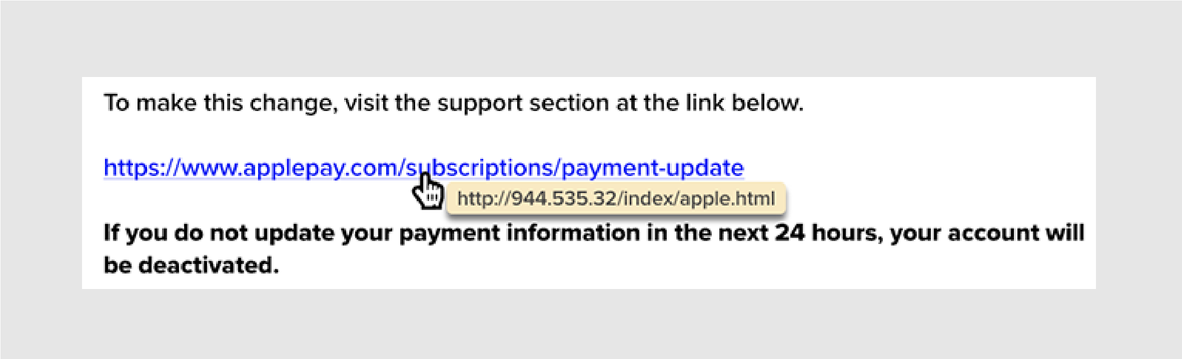
It has come to our attention that you're recent payment was declined. An update is required immediately..

Body copy

As well as in the subject line, intense language will often be used in the main body of a phishing email. The content will revolve around an urgent plea that attempts to get the recipient to respond without thinking, i.e. 'Deadline for payment is 5pm'. It is also common for fraudulent emails to be peppered with grammatical errors and punctuation mistakes.

Malicious link(s)

One of the main ways to spot a phishing attack is to scrutinise the link(s). They will usually have been formatted to look convincing i.e. 'Update your details here' or formatted to look like it relates to the message and the company the email is purporting to be from (as in the example overleaf). Or the link may have been shortened using an online service like bit.ly. All you need to do is hover over the link with your mouse to reveal the actual address, where you will see it would take you to a different site than stated.



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

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

http://944.535.32/index/apple.html

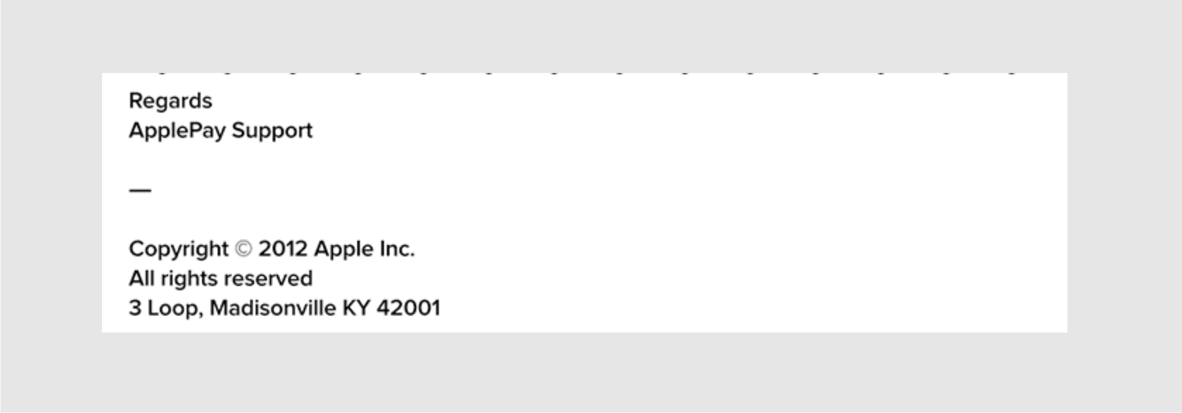
If you do not update your payment information in the next 24 hours, your account will be deactivated.

Scare tactics

Definitely worth another mention is that scare tactics and intense language are common in phishing emails and can be found throughout the email. The type of content you could expect to see such ploys would be in requesting your immediate response to update your details or make payment within a certain timeframe – usually with a consequence if you don't (as in the example above). The cybercriminal(s) hope the recipient will click their link(s) out of panic or confusion.

Email sign-off

Similar to the greeting, you will often notice the sign-off is impersonal too – making use of a general title rather than giving the personal touch and disclosing a person's name and details.



Regards
ApplePay Support

—

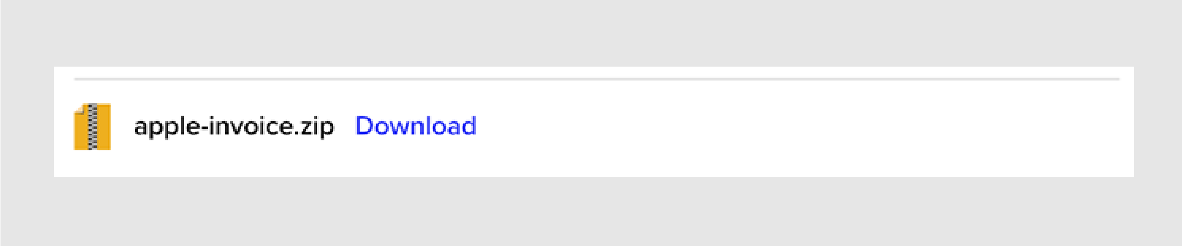
Copyright © 2012 Apple Inc.
All rights reserved
3 Loop, Madisonville KY 42001

Footer

Take a close look at the footer in the email. A phishing email may state an incorrect copyright date or a location that doesn't marry up with the legitimate company details.

Attachment(s)

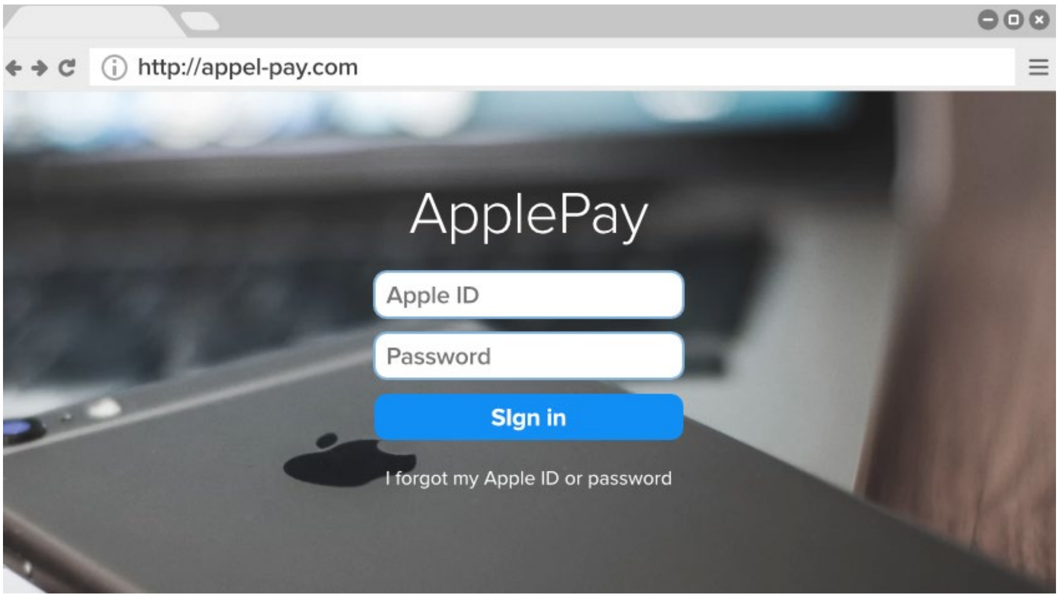
Phishing emails also can include malicious attachments that contain downloadable or compressed files that may infect your computer. Be wary, if it looks suspicious, it probably is.



apple-invoice.zip Download

MALICIOUS LANDING PAGES

If you do click on a phishing link, you may be directed to a malicious landing page, like the one below:



There are many tell-tale signs that a web page is malicious:

- **Web address:** Despite a malicious landing page doing its best to replicate a legitimate web page, including a very similar URL – there will be some errors there for you to spot i.e. misspellings and unsecure connections. Always make sure there is a padlock icon in the address bar of the page you are in when disclosing personal or financial information.
- **Missing navigation bar and footer:** These pages are often basic, all they are designed to do is to steal your information so are uncomplicated and often won't include the header and footer. You can see they are missing from the 'Apple' sign-in page example above.
- **Misspelling:** Like with a phishing email, you will often find fraudulent landing pages will contain misspelled words, watch out for small oversights like in the above example, where 'Apple Pay' is misspelled as one word.
- I**nformation collection:** The objective of a phishing campaign is to deceive the recipient into freely giving away their personal/financial information. If you click a malicious link you will probably be taken to a landing page like the example above, which will likely have a form to collect your data that differs from the legitimate company equivalent. In the example above, the form requests users to enter their Apple ID password, which is not requested on the actual Apple page.

WHAT YOU CAN DO

To help build your defences and stand strong against cybercrime, in particular phishing attacks, you need to employ best practice methods. It is highly recommended that you install data protection and antivirus software for added security. However, it's all good and well protecting your network but if a phishing email gets inside your organisation, it's your army of people that need to be prepared.

It is paramount that your team undergo **social engineering training** to improve their knowledge in how to spot a phishing attack. This comes as part of **Cyber Essentials Certification**, which all businesses really should obtain to demonstrate your commitment to cyber security, make you more attractive to prospects, as well as giving you added protection.