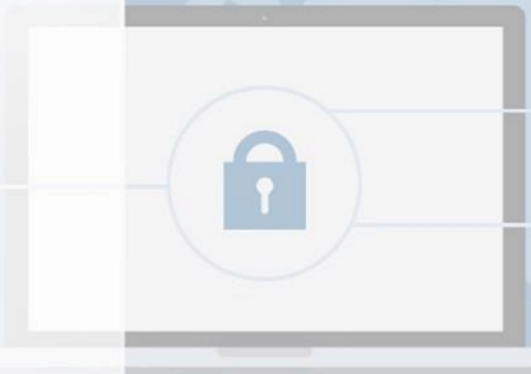
CYBER SECURITY

Identifying, Understanding and Mitigating the Latest Security Threats to Hit Nonprofits

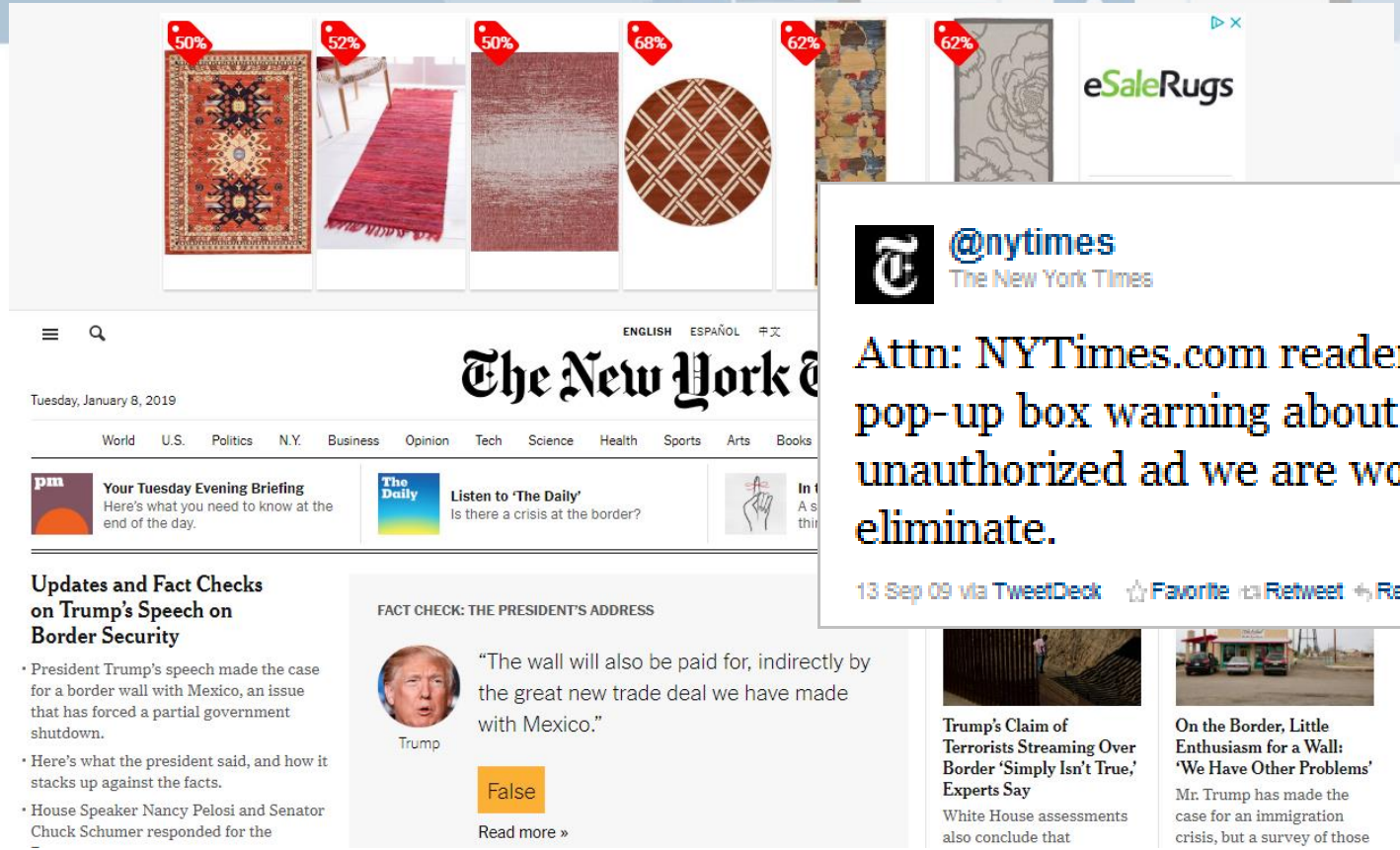
Top Security Threats

- Malvertising
- Phishing / Spear Phishing / Whaling
- Cryptojacking / Ransomware
- Internal Threats
- External Threats



Malvertising

Malvertising



Malvertising

- Advertising Blockers (plugins, extensions for browsers)
  - AdBlock
  - AdBlocker Ultimate
  - uBlock Origin
  - Ghostery
  - AdBlock Plus
  - *many more*

Malvertising

- Internet Browsers with built-in blockers
  - Opera / Opera Mini / Opera Touch
  - Firefox Focus
  - Microsoft Edge
  - Brave Browser
  - Ghostery Privacy Browser
  - Slimjet
  - *and a few others*

Malvertising

- DNS Web Filters
  - OpenDNS
  - CleanBrowsing DNS
  - SafeDNS
  - Norton ConnectSafe
  - Comodo Secure DNS
  - Quad9
- VPN Services
  - NordVPN
  - ExpressVPN
  - BulletVPN
  - PrivateInternetAccess
  - CyberGhost VPN
  - TunnelBear VPN

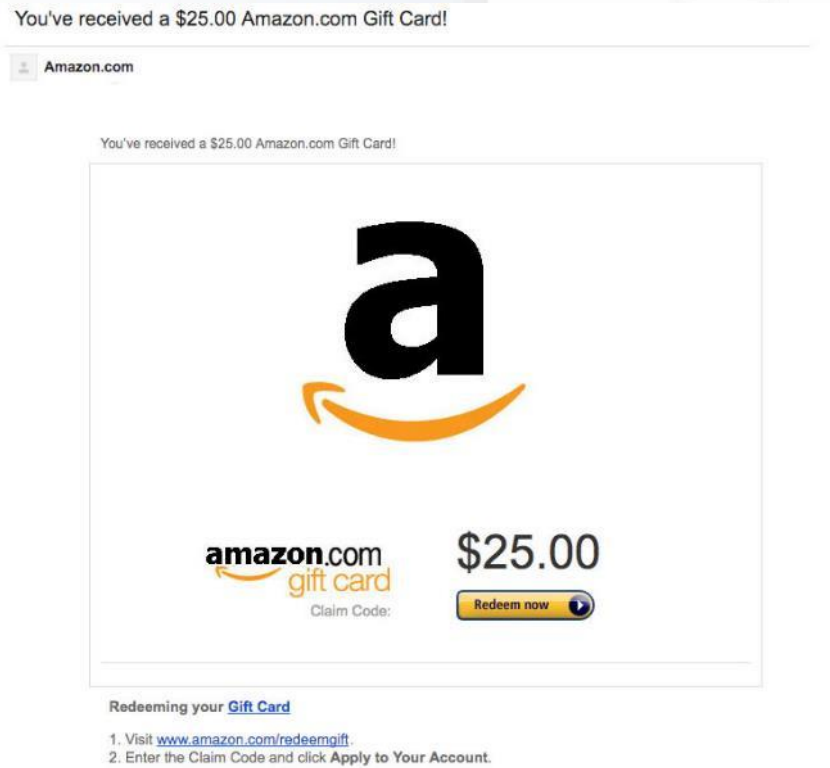
Malvertising

- Applications / Appliances / Hardware
  - 1Blocker (iOS, Mac)
  - AdLock (Windows $22, Android $11)
  - Disconnect.me
  - Sophos UTM Home*
  - clearOS*

** May require additional IT service/support*

(The Lookalike)

Phishing



Phishing

(The Internal Request)

Company Update: Employee Action Required

IT Department

All,

We've been alerted of a potential breach of our company email server. At this time it doesn't appear that any sensitive information was compromised, but we need to take preventative measures to limit our risk.

If you haven't done so already please click here to reset your email password.

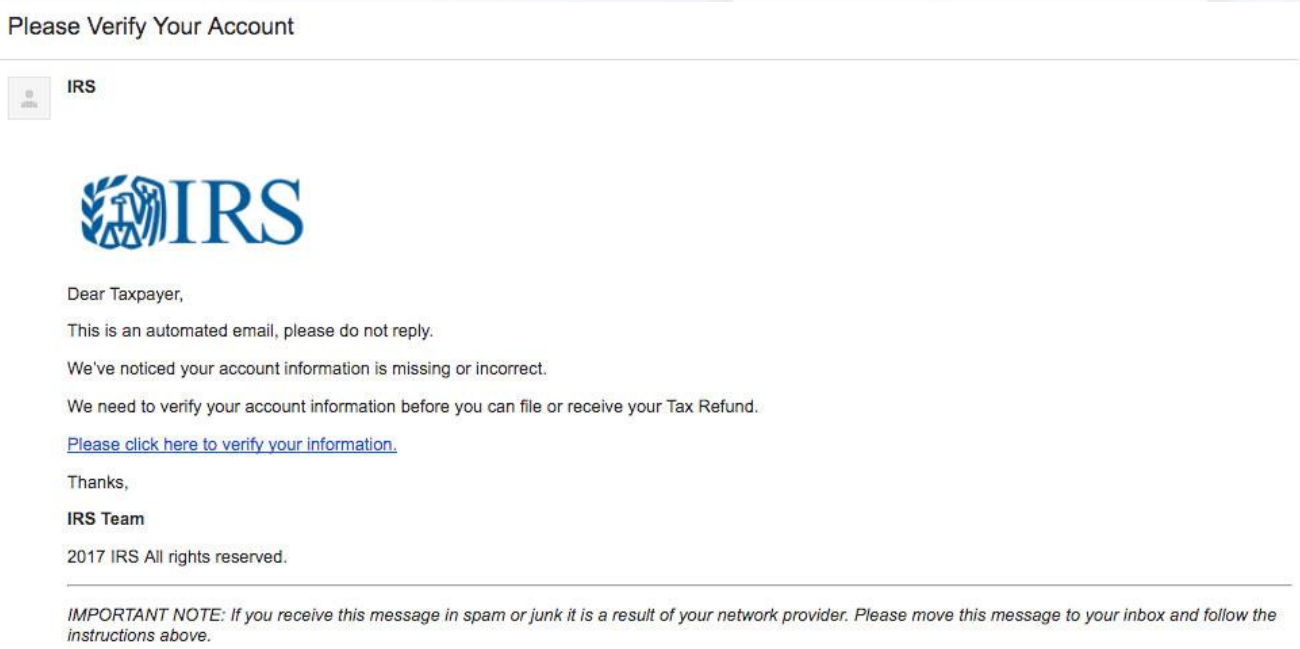
We will keep you updated with any new information regarding this issue. If you have any questions please feel free to contact IT directly.

Thank you!

IT Department

(The Government Threat)

Phishing



Please Verify Your Account

IRS

IRS

Dear Taxpayer,

This is an automated email, please do not reply.

We've noticed your account information is missing or incorrect.

We need to verify your account information before you can file or receive your Tax Refund.

Please click here to verify your information.

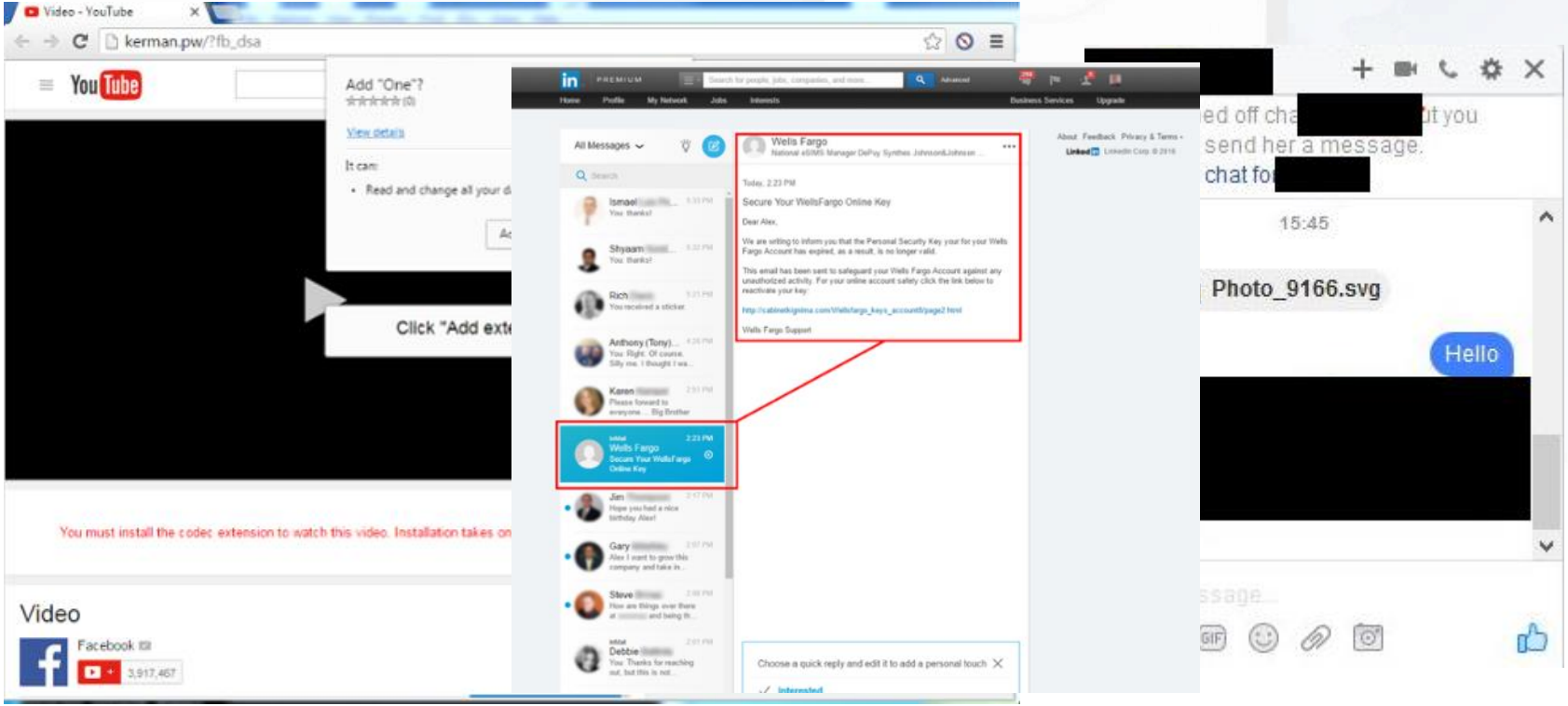
Thanks,

IRS Team

2017 IRS All rights reserved.

IMPORTANT NOTE: If you receive this message in spam or junk it is a result of your network provider. Please move this message to your inbox and follow the instructions above.

Phishing


Video - YouTube
kerman.pw/?fb_dsa
YouTube
Add "One"?
View details
It can:
Read and change all your d
Click "Add exte
You must install the codec extension to watch this video. Installation takes on
Video
Facebook
3,917,467
Wells Fargo
Secure Your WellsFargo Online Key
Dear Alex,
We are writing to inform you that the Personal Security Key your for your Wells Fargo Account has expired, as a result, is no longer valid.
This email has been sent to safeguard your Wells Fargo Account against any unauthorized activity. For your online account safety click the link below to reactivate your key:
Wells Fargo Support
Choose a quick reply and edit it to add a personal touch
send her a message.
15:45
Photo_9166.svg
Hello

(Spoofing Attack)

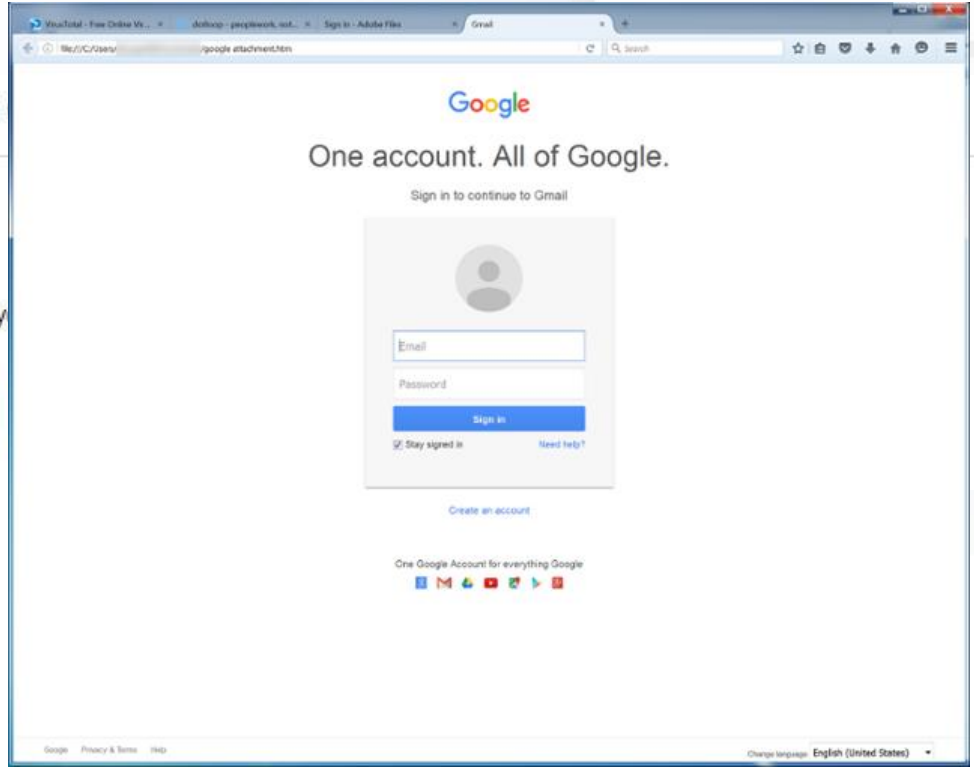
Phishing

Jeff has shared a

Google Docs

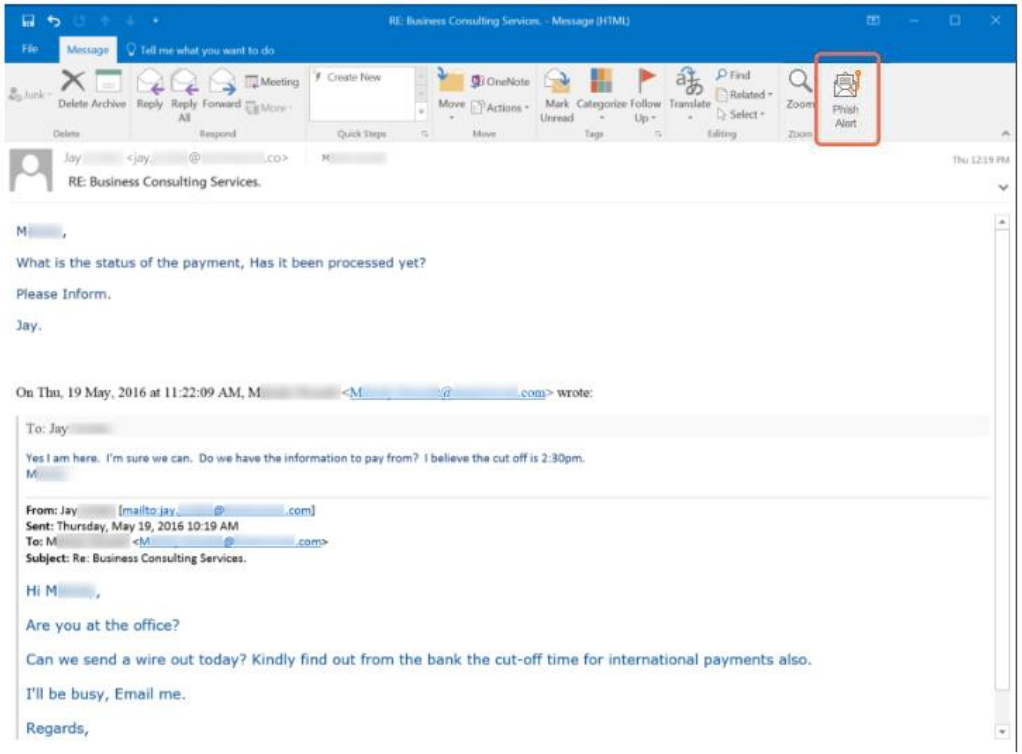
Jeff has invited y

Open in Docs

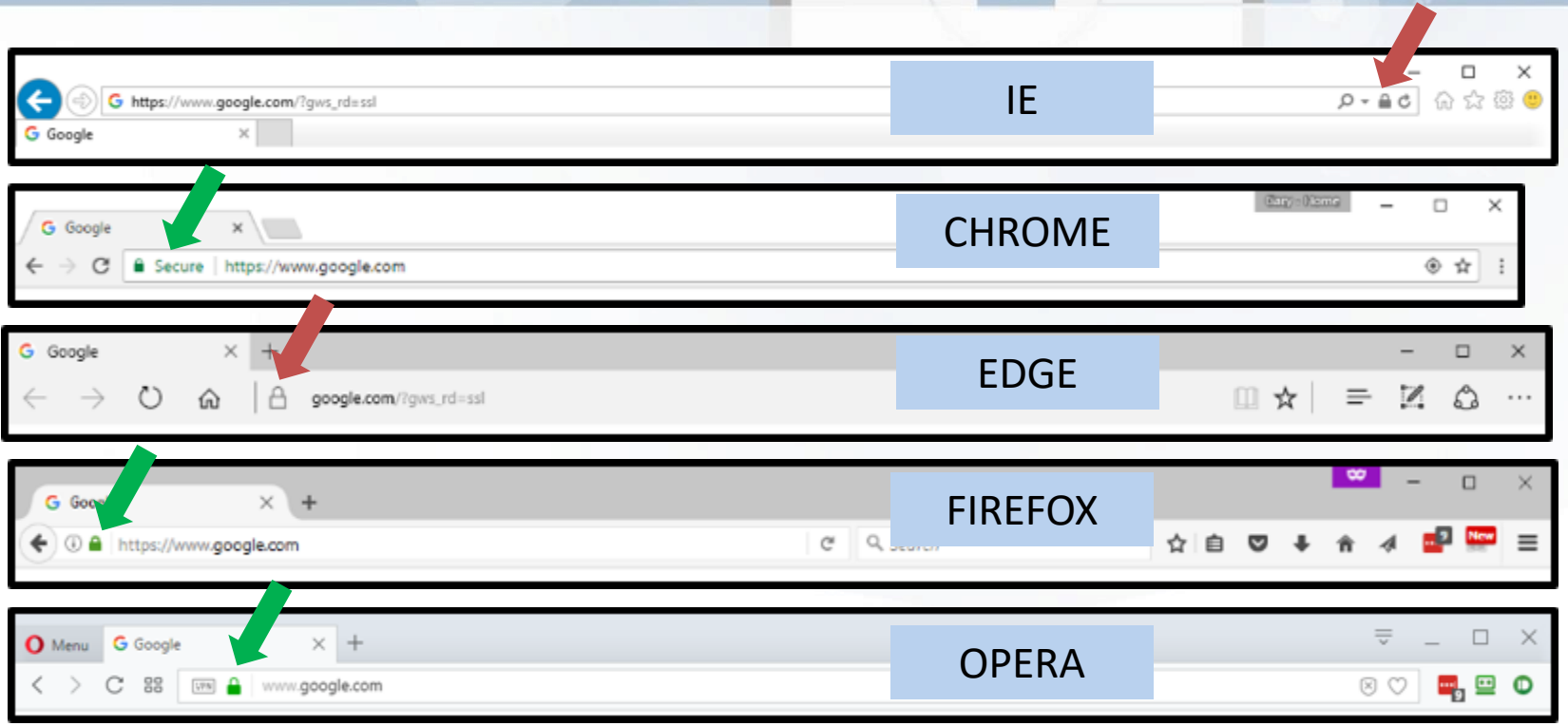


(Spear Phishing / Whaling)

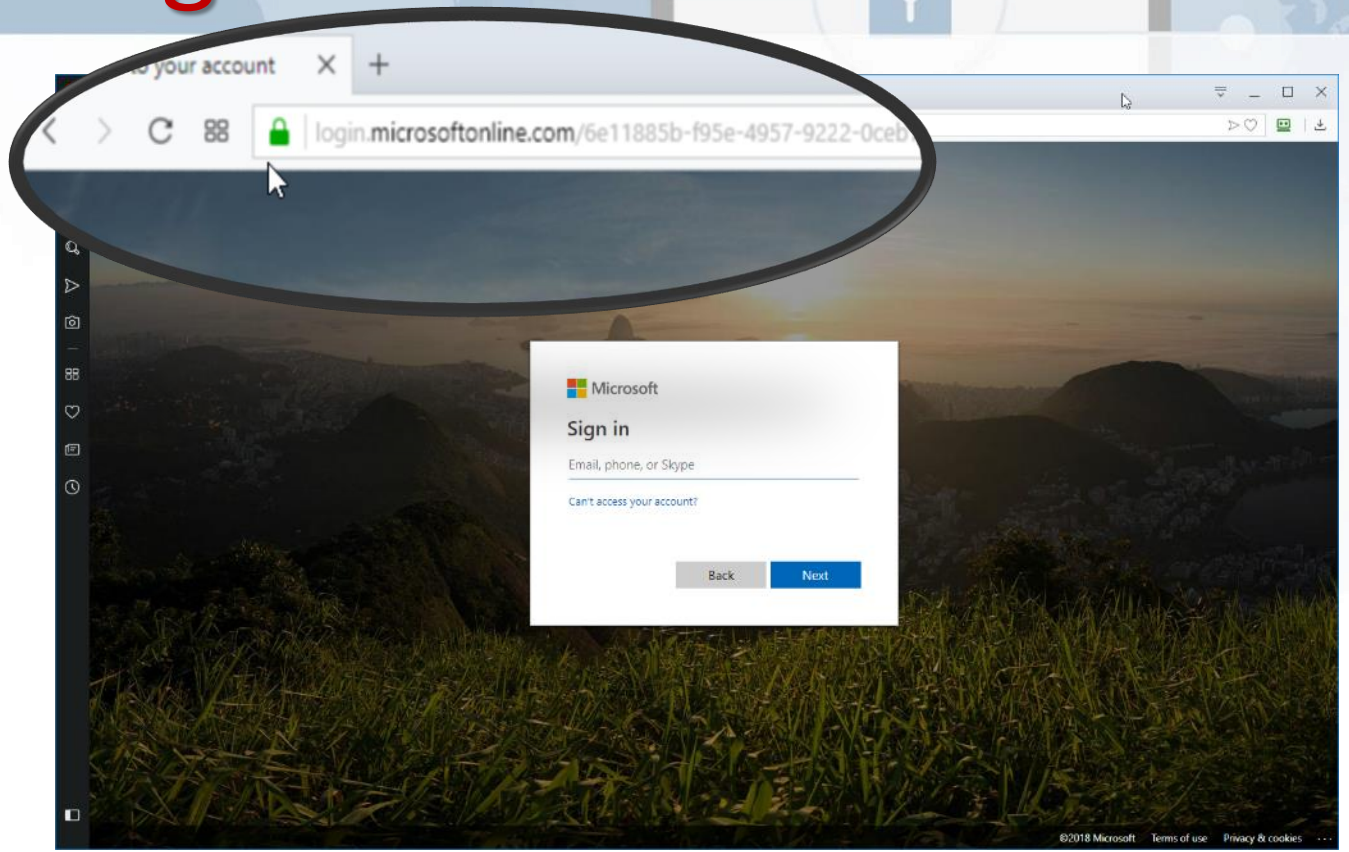
Phishing



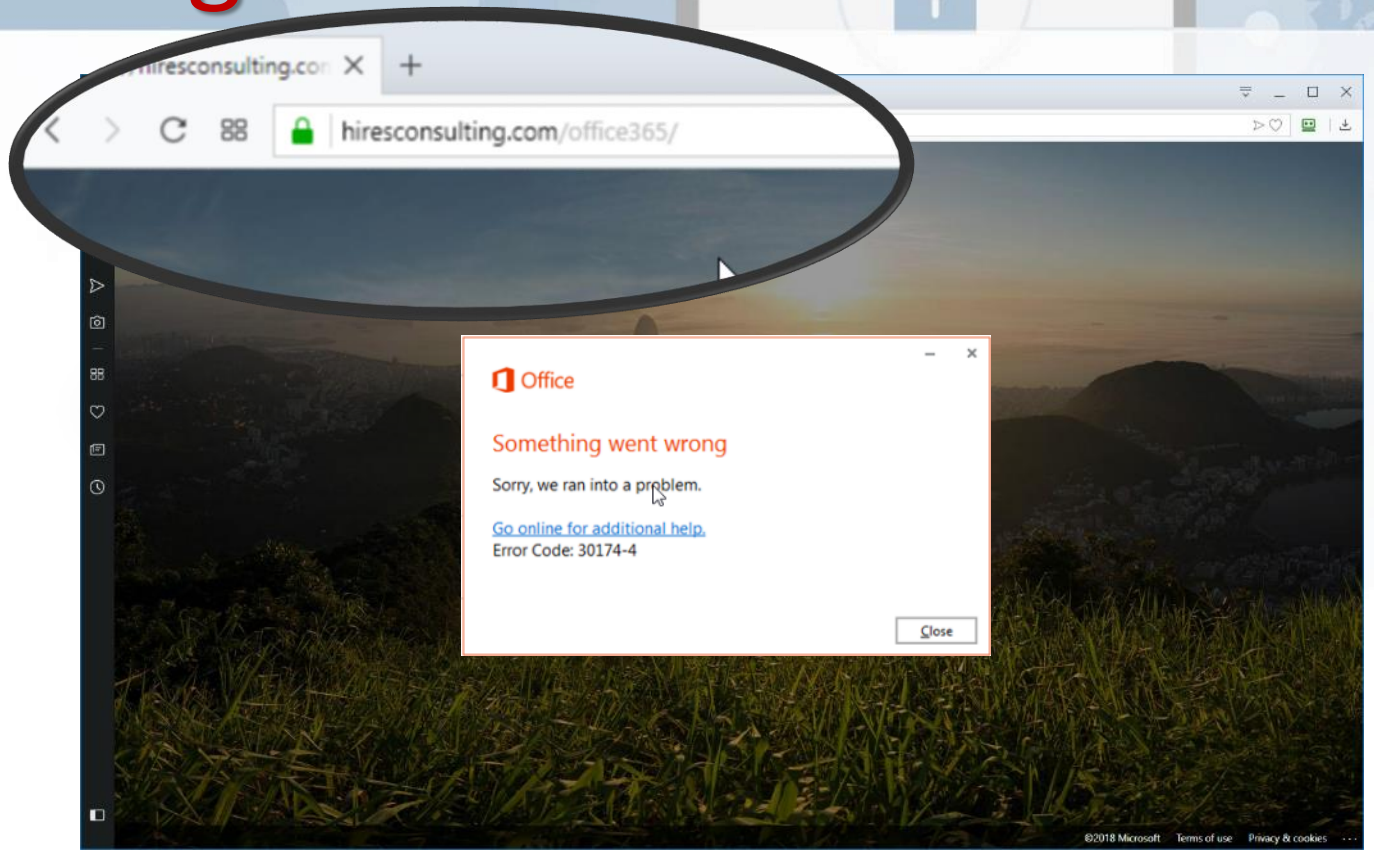
Phishing


IE
CHROME
EDGE
FIREFOX
OPERA
https://www.google.com/?gws_rd=ssl
Google
Secure
https://www.google.com
google.com/?gws_rd=ssl
Menu
www.google.com

Phishing


your account
login.microsoftonline.com/6e11885b-f95e-4957-9222-0ceb
Microsoft
Sign in
Email, phone, or Skype
Can't access your account?
Back
Next
©2018 Microsoft
Terms of use
Privacy & cookies

Phishing


hiresconsulting.com/office365/
Office
Something went wrong
Sorry, we ran into a problem.
Go online for additional help.
Error Code: 30174-4
Close
©2018 Microsoft
Terms of use
Privacy & cookies

Phishing

23 New Messages

From: cbmtech.com [mailto:support.com-quarantine-inbound@marsoft.com]
Sent: Friday, June 23, 2017 8:11 AM
To: support@cbmtech.com
Subject: 23 New Messages

Office 365

Dear support@cbmtech.com

There are 23 new messages in your Email Quarantine since you received your last Notification.

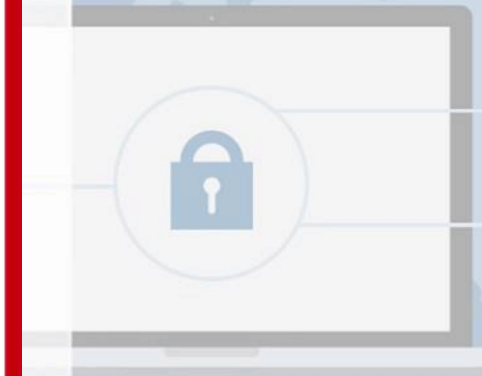
Messages will be automatically removed from the quarantin

http://www.baktigroups.com/oj.php
Click or tap to follow link.

To see all quarantined messages view your email quarantine or continue below

Continue

Note: This message has been sent by a notification only system. Please do not reply



Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

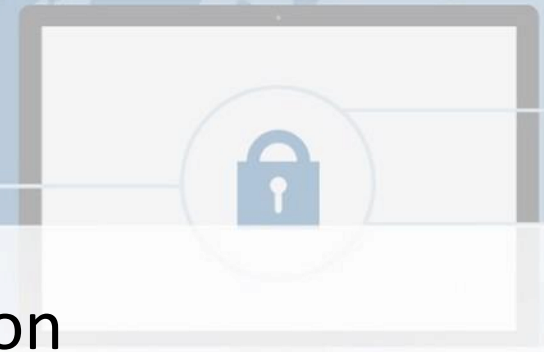
CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

Phishing

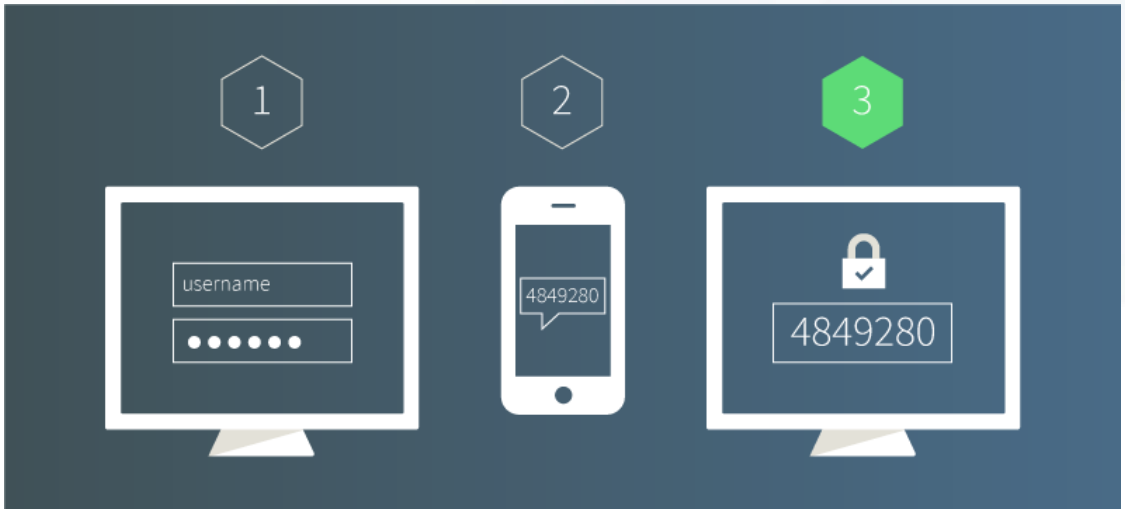
Phishing



- Two-Factor Authentication
- Multi-Factor Authentication
- Strong & Unique Passwords for EACH & EVERY LOGIN
- Check/Monitor for Breaches
- Password Managers
- Different/Aliased Email Accounts
- Wrong Passwords

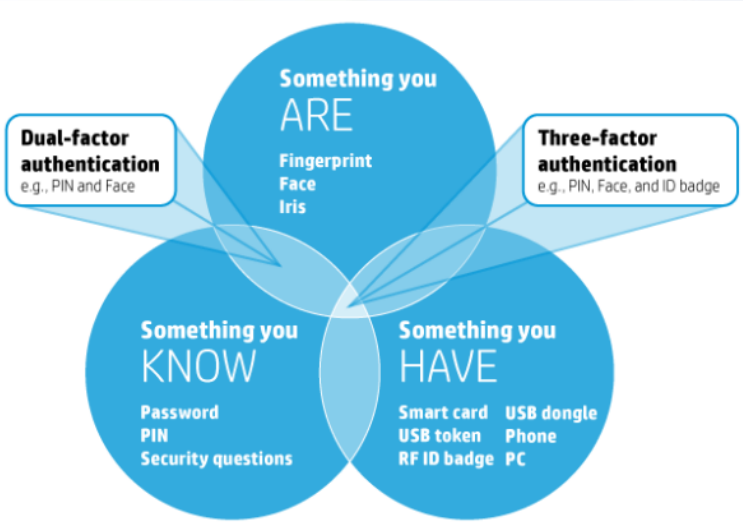
Phishing

- Two-Factor Authentication (2FA)
  - Usually Password & Text/SMS Codes



Phishing

- Multi-Factor Authentication (MFA)
  - Multiple verification methods required



Phishing

- Strong & Unique Password for EACH & EVERY LOGIN
  - https://howsecureismypassword.net
  - https://lastpass.com/howsecure.php
  - https://password.kaspersky.com/
  - https://passwordsgenerator.net/
  - https://www.lastpass.com/password-generator/
  - https://www.roboform.com/password-generator

Phishing

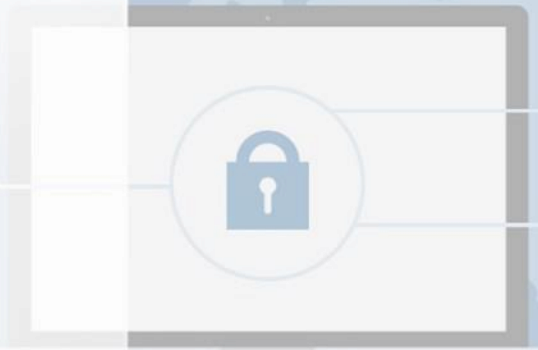
- Check/Monitor for Account Breaches
  - https://haveibeenpwned.com
  - https://www.dehashed.com/
  - https://monitor.firefox.com
  - https://www.creditkarma.com/id-monitoring
  - https://wallethub.com/free-credit-monitoring/

Phishing

Fact: The fastest special purpose password cracking machine can generate and check 100 billion hashes per second.

The data represent how long a password at that level can resist being cracked.

Number of Characters	123	abc	abc123	ABCabc	ABab123	AllASCII!
6	*0.00001 s*	*0.00309 s*	*0.02177 s*	*0.19771 s*	*0.568 s*	*7.4 s*
7	*0.0001 s*	*0.08032 s*	*0.78364 s*	*10.3 s*	*35.2 s*	*11.6 m*
8	*0.001 s*	*2.1 s*	*28.2 s*	*8.9 m*	*36.4 m*	*18.4 h*
9	*0.01 s*	*54.3 s*	*16.9 m*	*7.7 h*	*1.6 d*	*72.9 d*
10	*0.1 s*	*23.5 m*	*10.2 h*	*16.7 d*	*97.1 d*	19. y
11	*1. s*	*10.2 h*	*15.2 d*	2.4 y	16.5 y	**1.8 ky**
12	*10. s*	*11. d*	1.5 y	123.9 y	**1. ky**	**171.2 ky**
13	*1.7 m*	*287.2 d*	54.1 y	**6.4 ky**	**63.4 ky**	**.gt. 1 my**
14	*16.7 m*	20.4 y	**1.9 ky**	**334.9 ky**	**.gt. 1 my**	**.gt. 1 my**
15	*2.8 h*	531.5 y	**70.1 ky**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**
16	*1.2 d*	**13.8 ky**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**
17	*11.6 d*	**359.3 ky**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**
18	*115.7 d*	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**
19	3.2 y	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**
20	31.7 y	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**	**.gt. 1 my**



Phishing

PASSWORD CRACKING DURATIONS

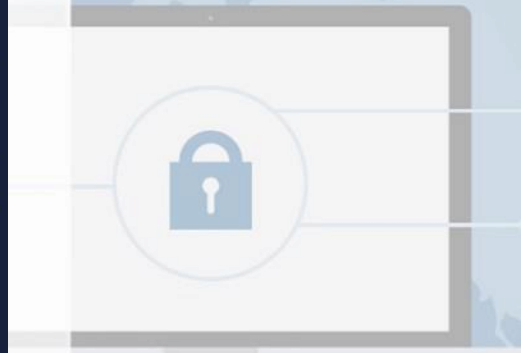
PASSWORD	CHARACTER SET SIZE	PASSWORD LENGTH	TIME TO CRACK (100 TRILLION GUESS/SECOND)
94351184	10	9	0.00000111 second
0833185837	10	10	0.000111 second
362924565493467	10	15	11.11 second
o3G1qHFe	52	8	2.22 second
W4ZflLEm1o	52	10	2.37 hour
inKm0p7UPVMFx87	52	15	2.48 thousand centurie
2ILqzp_#	62	8	1.12 minute
*n>z_K1GVQ	62	10	1 wee
#Eu{5'p5[<-\QLz	62	15	1.49 million centurie
D0g.....	95	24	9.38 hundred billion trillion centurie

MEDIA LABS

PASSWORD SEARCH SPACE

COMPLEXITY	CHARACTER SET SIZE	PASSWORD LENGTH	NUMBER OF POSSIBLE PASSWORDS
Numeric 1234567890	10	9	100,000,000
Numeric 1234567890	10	10	11,111,111,110
Numeric 1234567890	10	15	1,111,111,111,111,110
Alphabetic AaBbCcDdEe	52	8	54,507,958,502,660
Alphabetic AaBbCcDdEe	52	10	147,389,519,791,195,396
Alphabetic AaBbCcDdEe	52	15	56,038,089,699,156,288,046,695,684
Alphanumeric AaBbCc 12390	62	8	221,919,451,578,090
Alphanumeric AaBbCc 12390	62	10	853,058,371,866,181,866
Alphanumeric AaBbCc 12390	62	15	781,514,782,079,074,318,856,775,914
Alphanumeric + symbols AaBbCc 12390 &%@!	95	8	6,704,780,954,517,120
Alphanumeric + symbols AaBbCc 12390 &%@!	95	10	60,510,648,114,517,017,120
Alphanumeric + symbols AaBbCc 12390 &%@!	95	15	468,219,860,267,835,848,675,991,626,495

MEDIA LABS



Phishing

- Password Managers
  - Roboform
  - Dashlane
  - Lastpass
  - Keepass
  - 1Password

1Password

Phishing

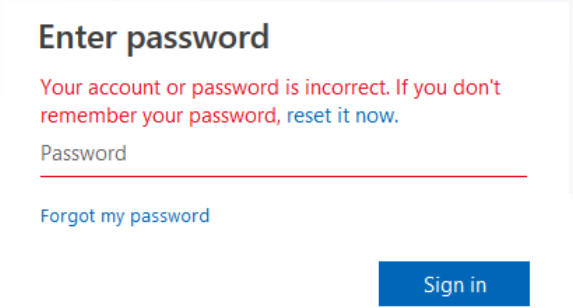
- Different / Shared / Aliased Email Accounts / Profiles
  - Generic / Shared Mailboxes
    - info@mydomain.org, admin@mydomain.org, media@mydomain.org, accounts@mydomain.org
  - Aliased Email Accounts
    - Primary email: garyhires@mydomain.org
    - Alias email: it@mydomain.org, network@mydomain.org

Phishing

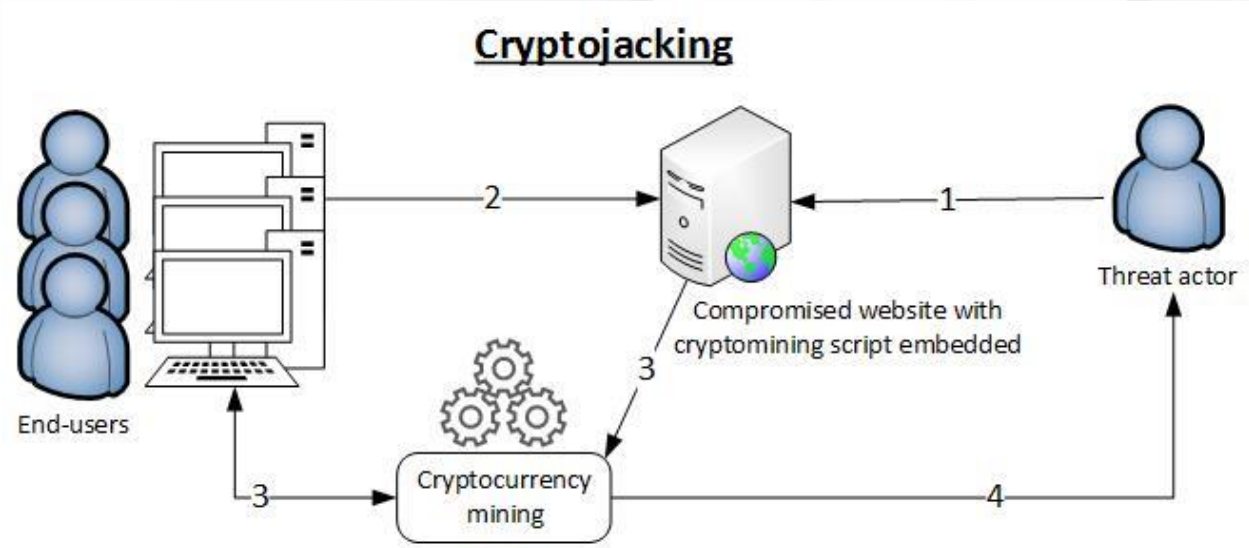
- Different/Browsers Profiles
  - Setup and utilize “browser profiles” for specific “internet tasks” within single “browser”
    - Firefox, Chrome, Edge, Opera, Ghost Browser
  - Install and utilize different “browsers” for specific “internet tasks”

Phishing

- Wrong Passwords
  - Simply enter an intentionally INCORRECT/BAD password
  - The “real” website should return with an “invalid account, username or password” type response.



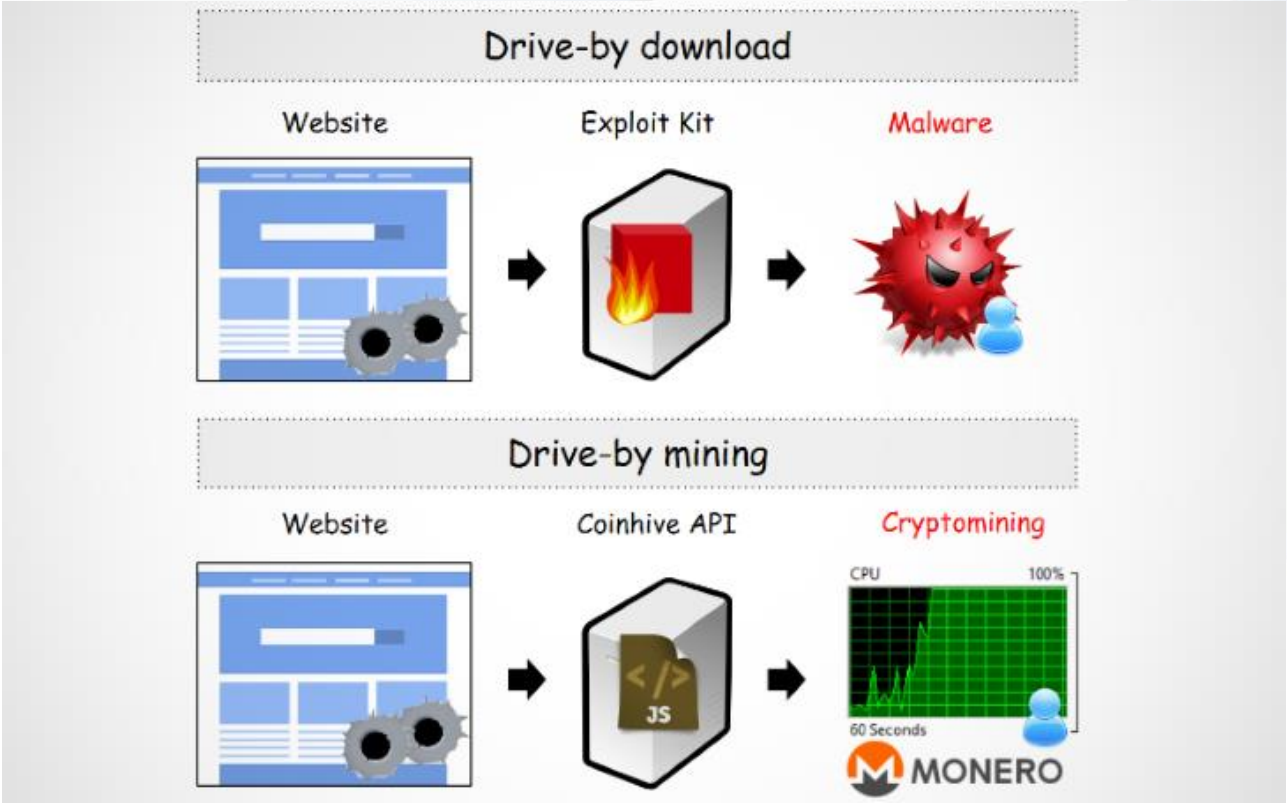
Cryptojacking



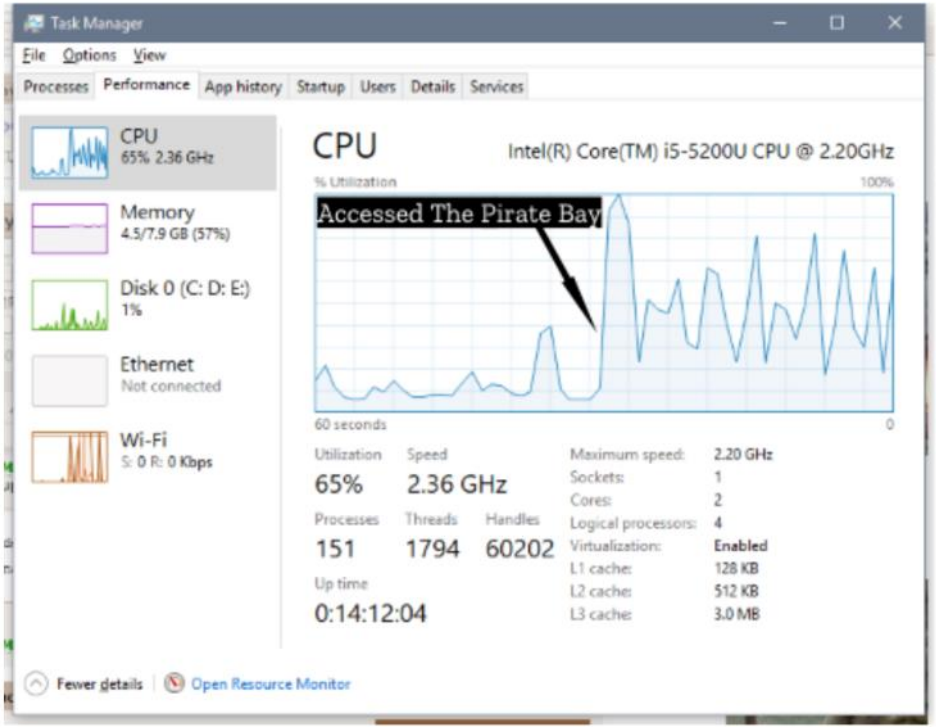
Steps

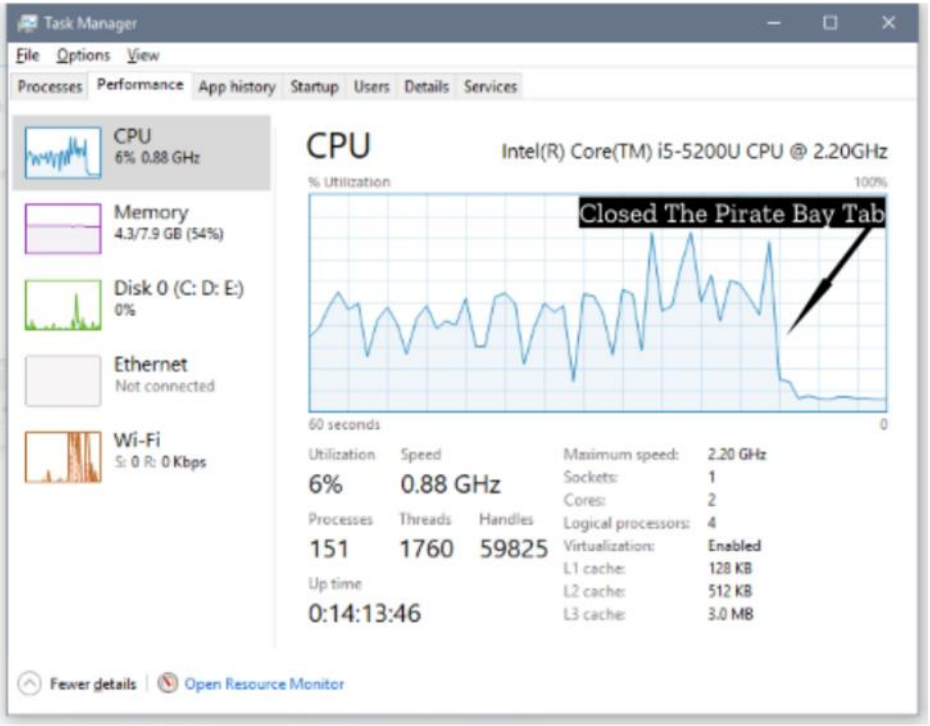
1. The threat actor compromises a website
2. Users connect to the compromised website and the cryptomining script executes
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

Cryptojacking

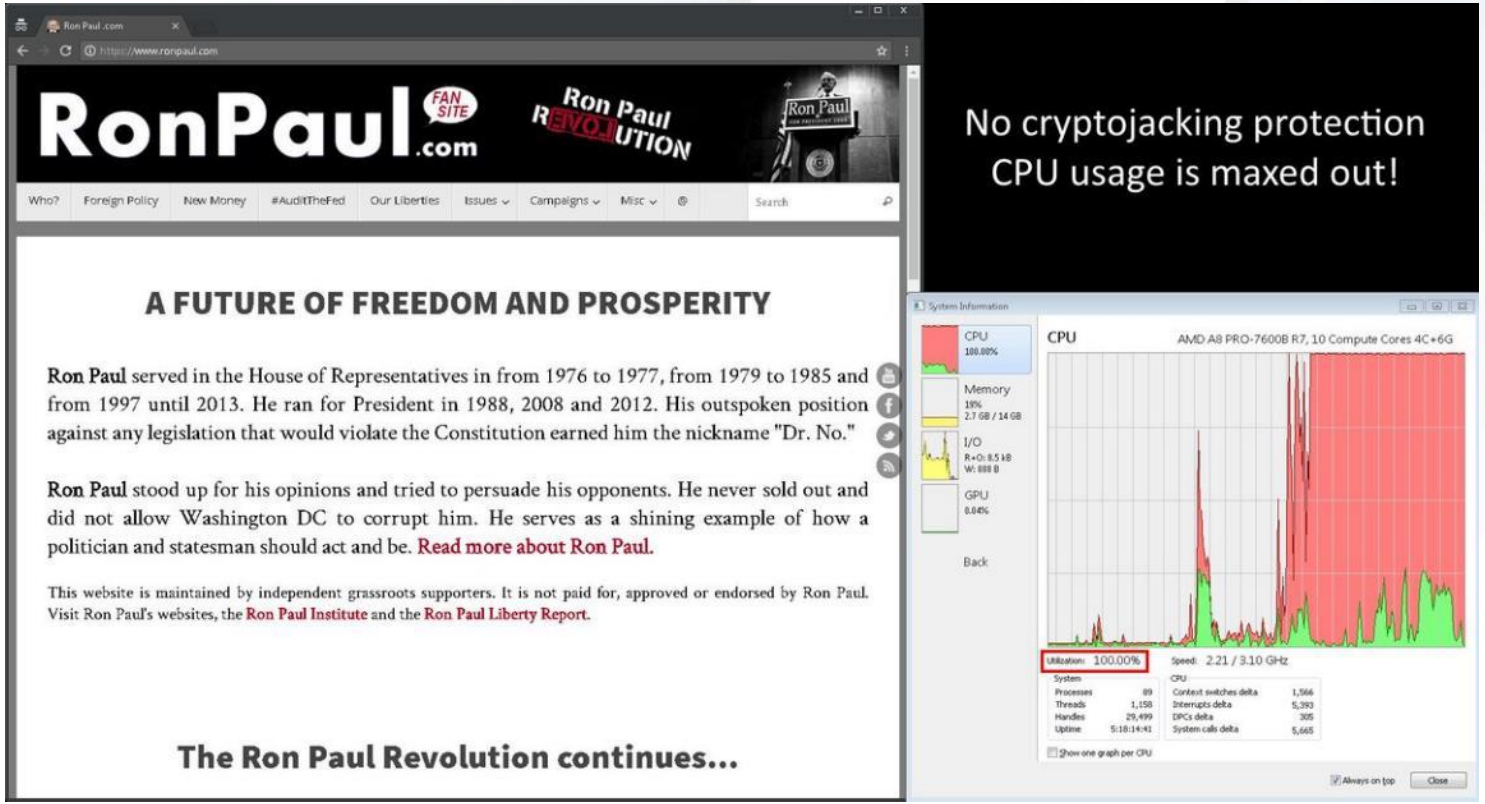


Cryptojacking

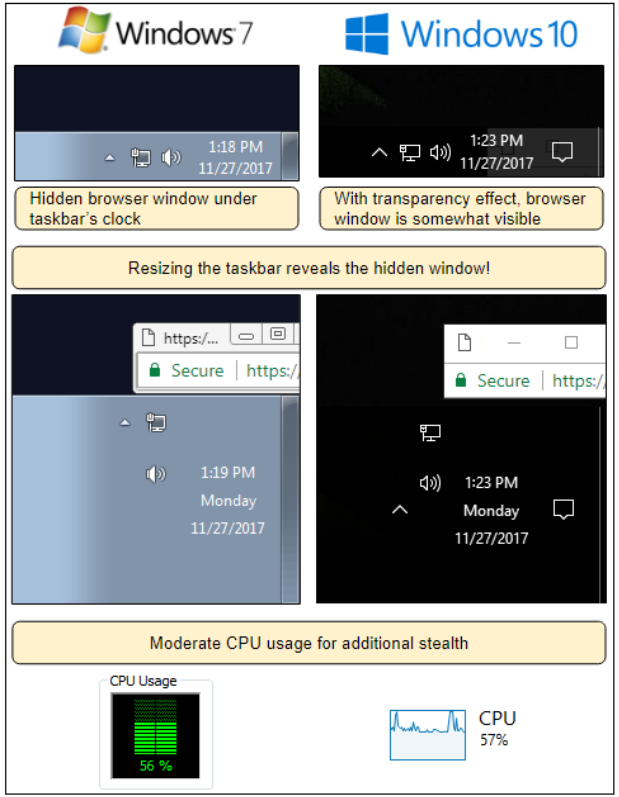


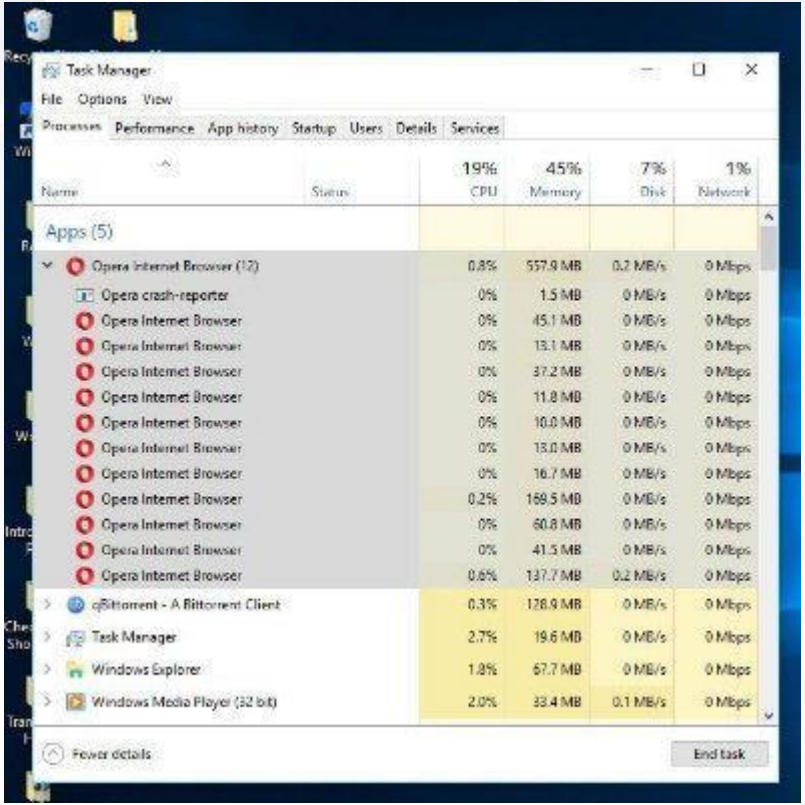


Cryptojacking



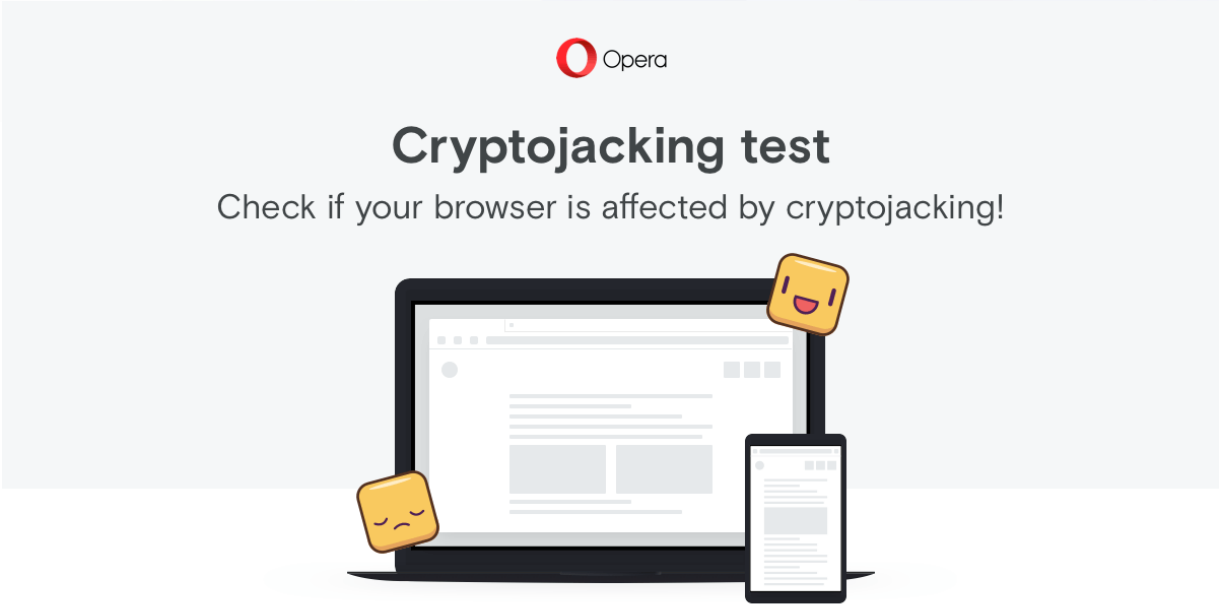
Cryptojacking





Cryptojacking

- https://cryptojackingtest.com



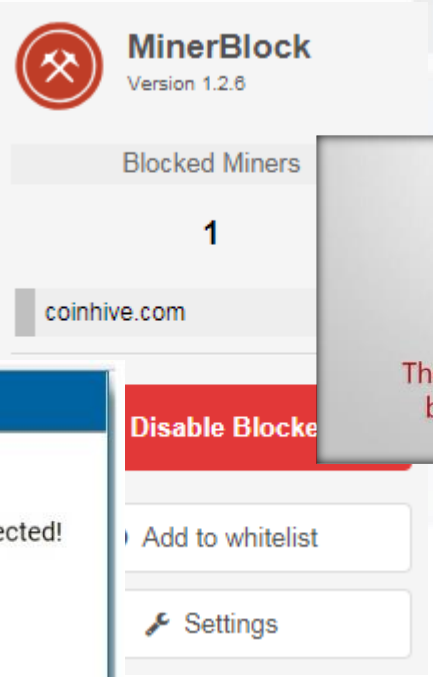
Cryptojacking

- Use the Task Manager (Windows) or Activity Monitor (Mac OS X)
- Disable JavaScript in the browser
- Browser extensions like “No Coin”, “Miner Blocker”, “CoinBlocker” are available for most browsers.
  Opera has it enabled already.
- Install third-party malware detection and anti-virus software
- Update and patch software

Cryptojacking

Chrome Task Manager

- Open the Chrome Task Manager by using the Shift+ESC keyboard combination
- Or from the Chrome menu, then More Tools, and then Chrome Task Manager.



Cryptojacking

- Anti-Malware, Anti-Spyware, Anti-Spamware
  - https://www.malwarebytes.com/
  - http://www.safer-networking.org/private/
  - https://superantispyware.com/
  - https://www.malwarebytes.com/adwcleaner/

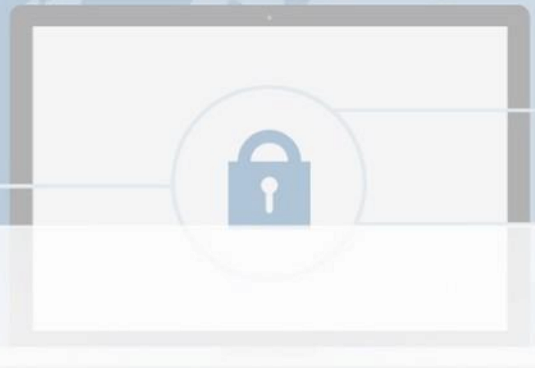
Ransomware


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
1/4/1970 01:00:00
Time Left
00:00:00:00
Your files will be lost on
1/8/1970 01:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
Check Payment
Decrypt

Ransomware


1
INSTALLATION
After a victim's computer is infected, the crypto-ransomware installs itself, and sets keys in the Windows Registry to start automatically every time your computer boots up.
CONTACTING HEADQUARTERS
2
Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.
3
HANDSHAKE AND KEYS
The ransomware client and server identify each other through a carefully arranged "handshake," and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals' server.
ENCRYPTION
4
With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.
5
EXTORTION
The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, $300 to $500, must be paid in untraceable bitcoins or other electronic payments.

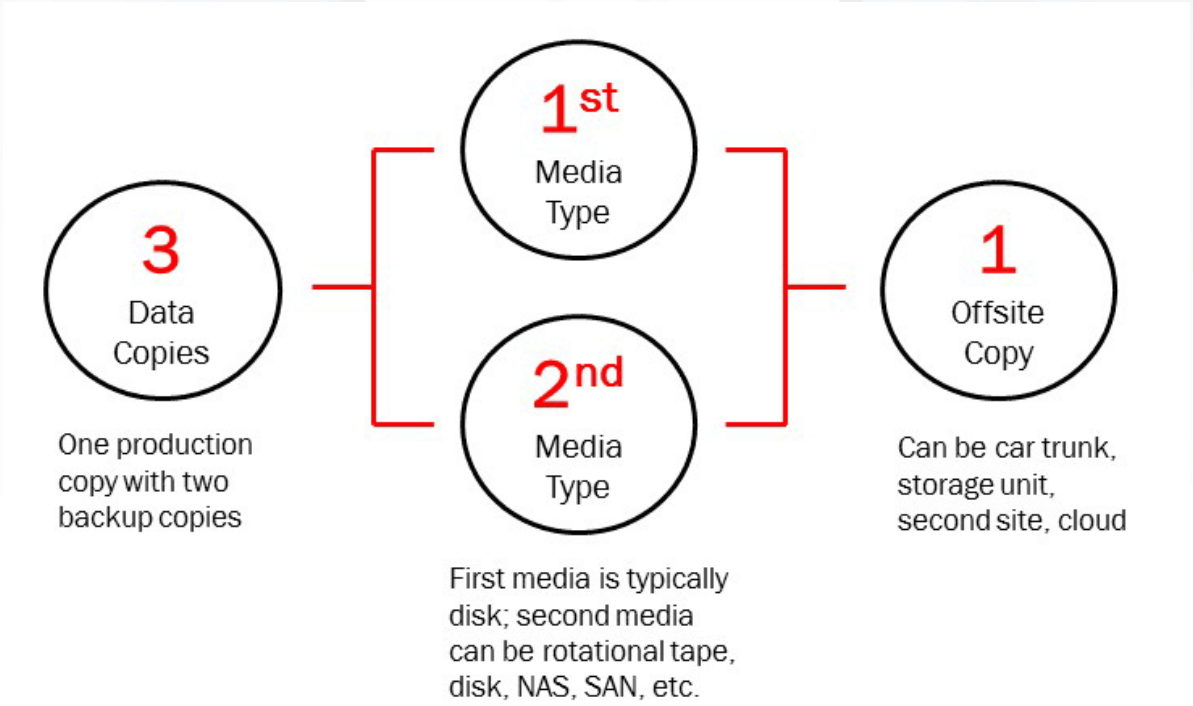
Ransomware



- Education
- Backups
- Remove local administrative rights from daily use account
- Be wary of any email attachments

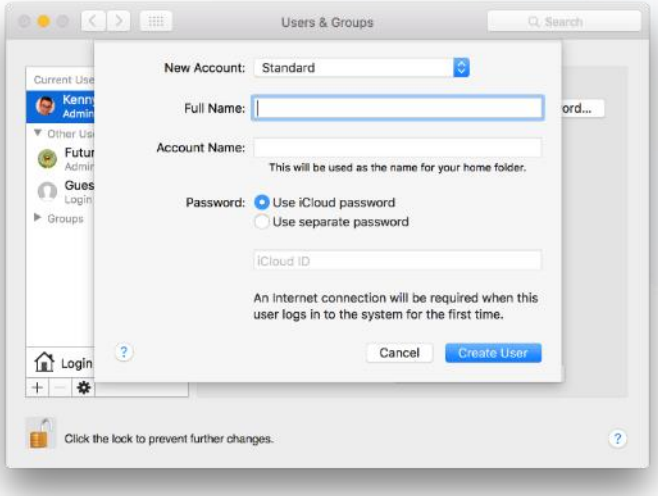
Ransomware

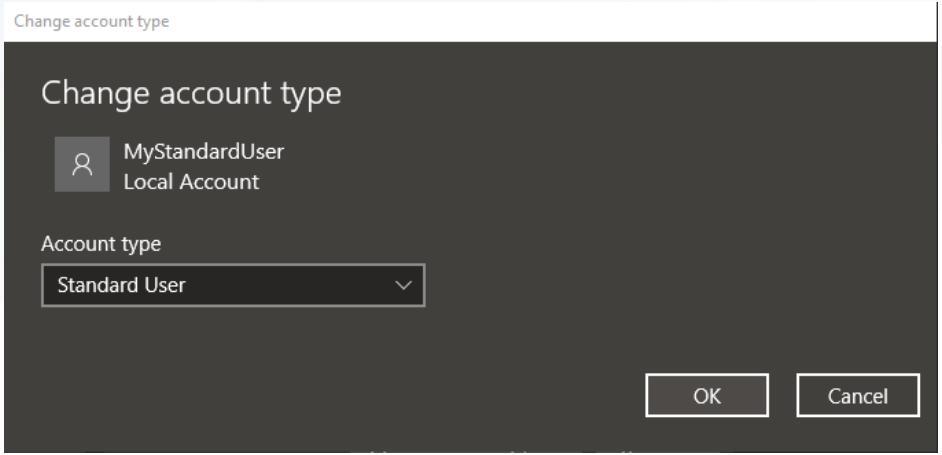
- Backups



Ransomware

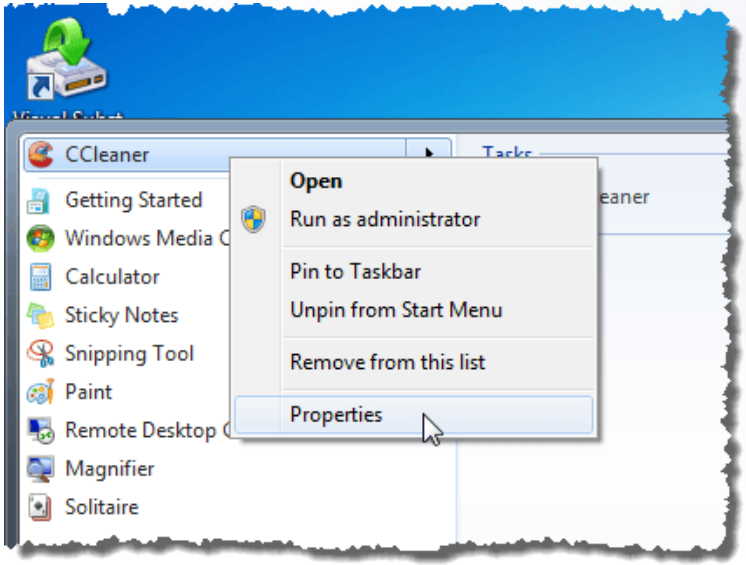
- Remove local administrative rights
  - Use Standard User rather than Administrator



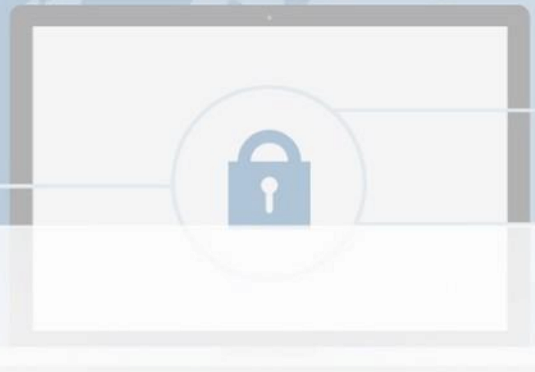


Ransomware

- Elevate permissions to Administrator only when necessary

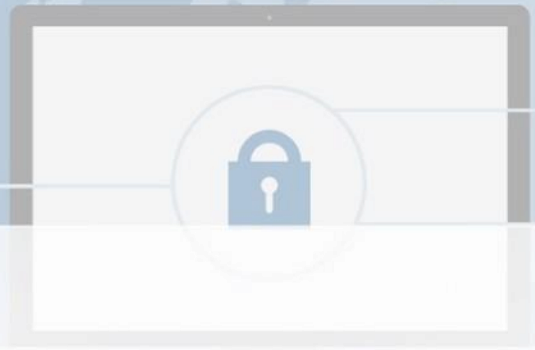


Internal Threats



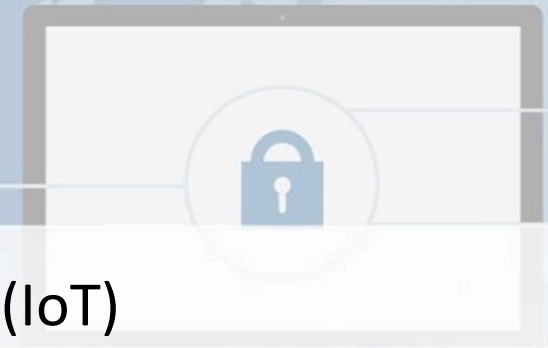
- Employees
  - Insider malice
  - Poor Password Practices
  - Weak Access Policies
  - Unsafe Downloads
  - Unprotected Data and Email

Internal Threats



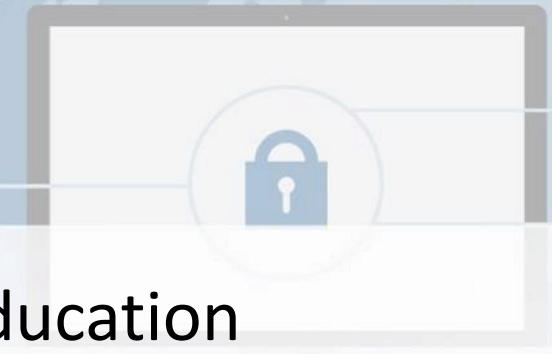
- Software / Systems
  - Unsecured Software
  - Unsecured Devices
  - Unsecured Network / Wi-Fi
  - Bad Access Practices

Internal Threats



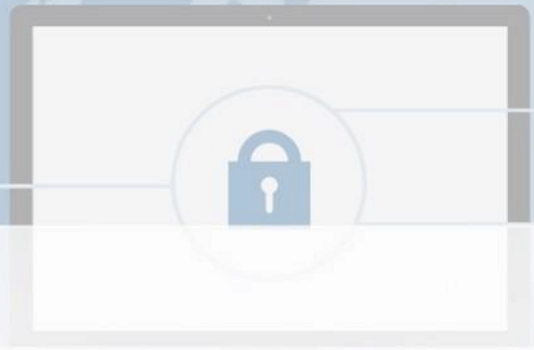
- Devices / Internet-of-Things (IoT)
  - Employee's BYOD – Bring your own device
  - Employee Online Access, VPN, Remote Access/Connectivity
- Automation/"Connected" Devices
  - Software/Firmware Outdated/Unpatched
- Websites, Remote Access Gateways, VPN, Servers
  - Outdated/Unpatched
  - Unmanaged and Unmonitored

Internal Threats



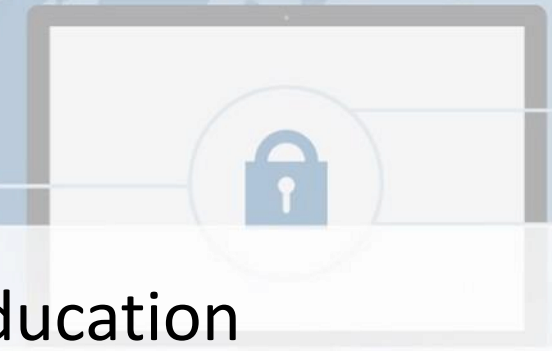
- Education, Education, Education
- IT Service/Support/Consultants
- Conditional Access
- Privileged Access
- Updated/Patched Software/Firmware
- Managed/Monitored Servers, Software and Devices
- Intentional Increased Security Measures

External Threats



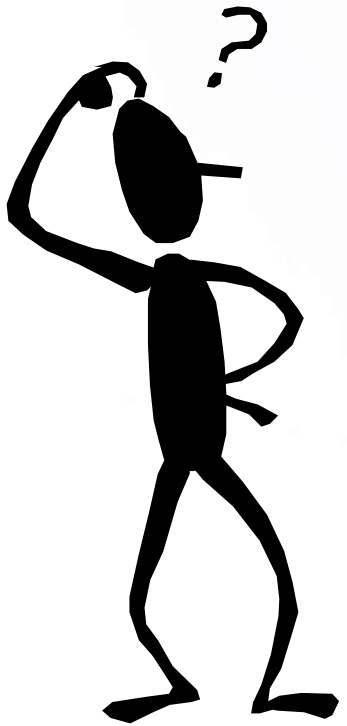
- Employees
  - BYOD – Bring your own device
  - Online Access, VPN, Remote Access/Connectivity
  - Severed, Malicious Intentions
- Websites, Remote Access Gateways, VPN, Servers
  - Outdated/Unpatched
  - Unmanaged and Unmonitored

External Threats



- Education, Education, Education
- IT Service/Support/Consultants
- Conditional Access (Filtering, Blocking)
- Privileged Access
- Updated/Patched Software
- Managed/Monitored Servers, Software and Devices
- Intentional Increased Security Measures

Questions & Answers



Contact Information

- Midland Shared Spaces (MSS)
  3500 N A St, Ste 1100
  Midland, TX 79705
  (432) 685-0400 main
  ghires@midlandss.org
  https://midlandss.org

- Hires Consulting (website for this presentation)
  http://hiresconsulting.com