ARMOUR

Handpicked elite military and intelligence cybersecurity veterans

ARMOUR

NOT FOR (their) PROFIT

How to prepare for an inevitable cyber-attack

Today:

- get your order in
- evolving threat landscape
- cyberattacks explained
- defences & tools to defend your practice
- how to elevate your cybersecurity

Rx:

military | intelligence | consulting

offices in:

USA | Canada | Mexico | Israel

cyberADVISORY

cyberPROFESSIONAL

services

cyberBREACH

cyberMANAGED

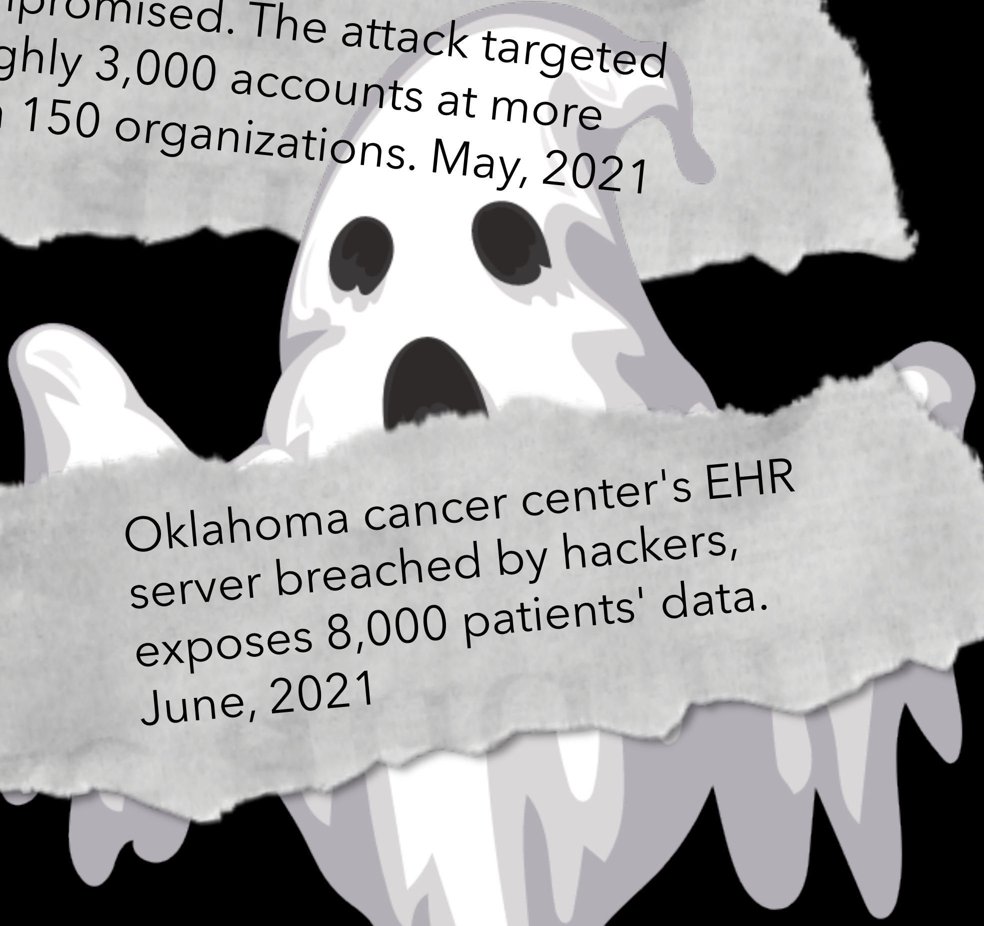
Horror Stories…

Colonial Pipeline Ransomware. East Cost was days away from major interruptions. May, 2021

Constant Contact USAID compromised. The attack targeted roughly 3,000 accounts at more than 150 organizations. May, 2021

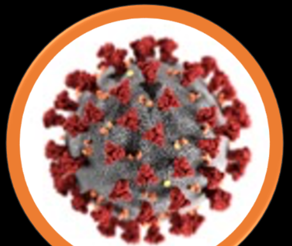
Blackbaud – major data breach. Affected many in the non-profit sector. July, 2020

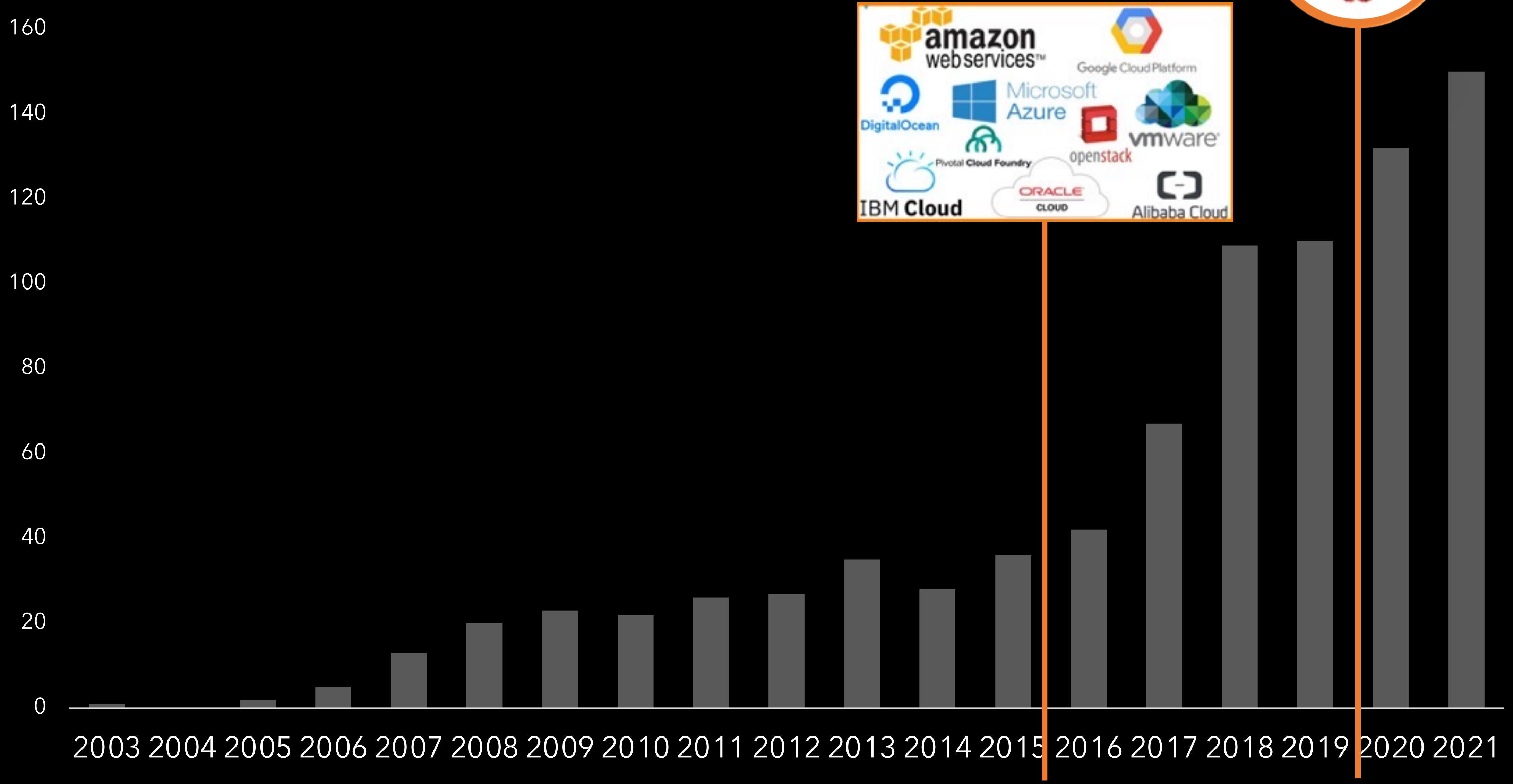
Oklahoma cancer center's EHR server breached by hackers, exposes 8,000 patients' data. June, 2021



Increased Criminal Activity

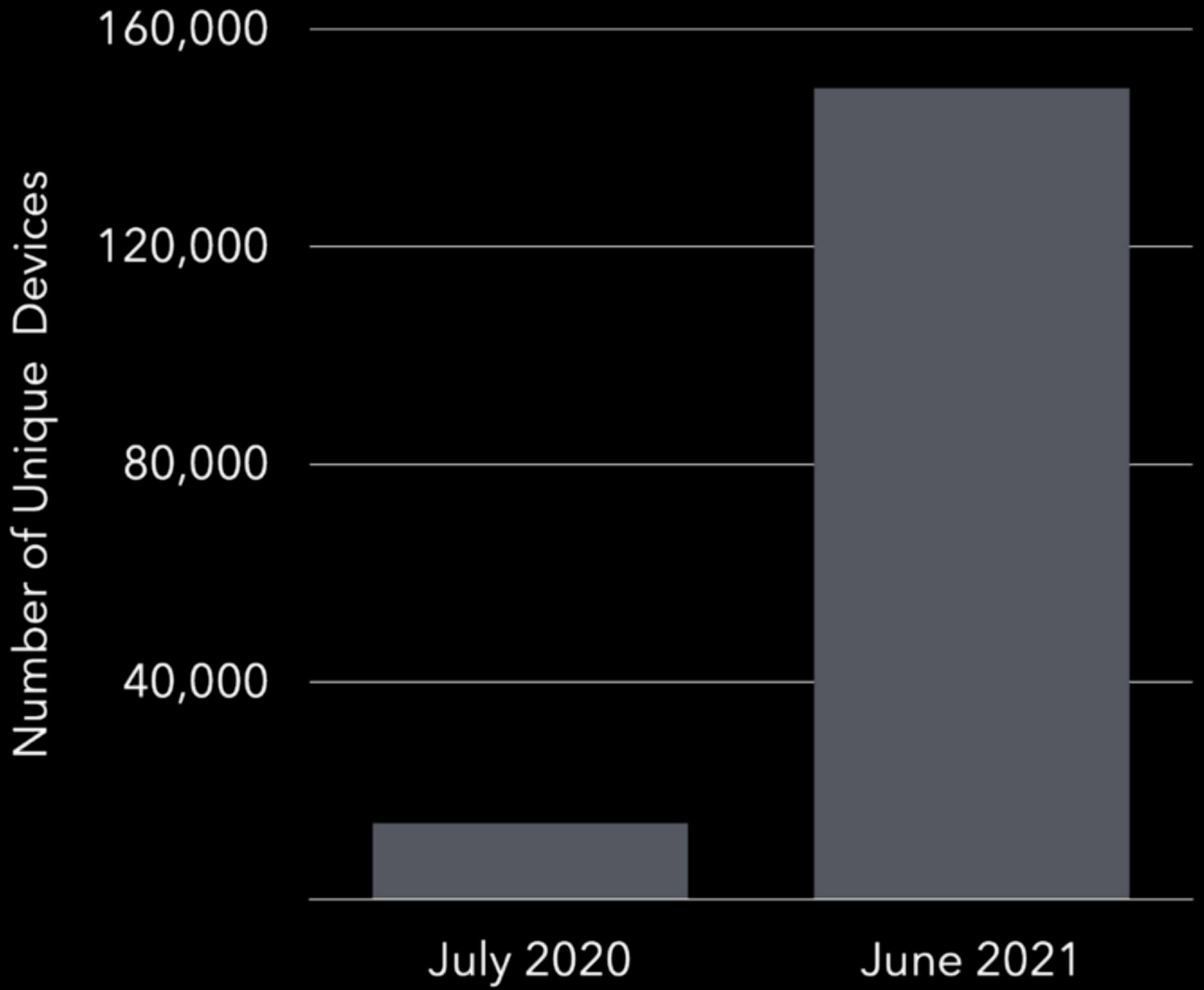
Number of significant cyber incidents since 2003





Zoom-in on Increased Activity

Cyber Attacks (weekly average)



The Main Drivers for the Increase

Accelerated Digital

Attack's ROI

Cybersecurity Experts Shortage

Work From Home

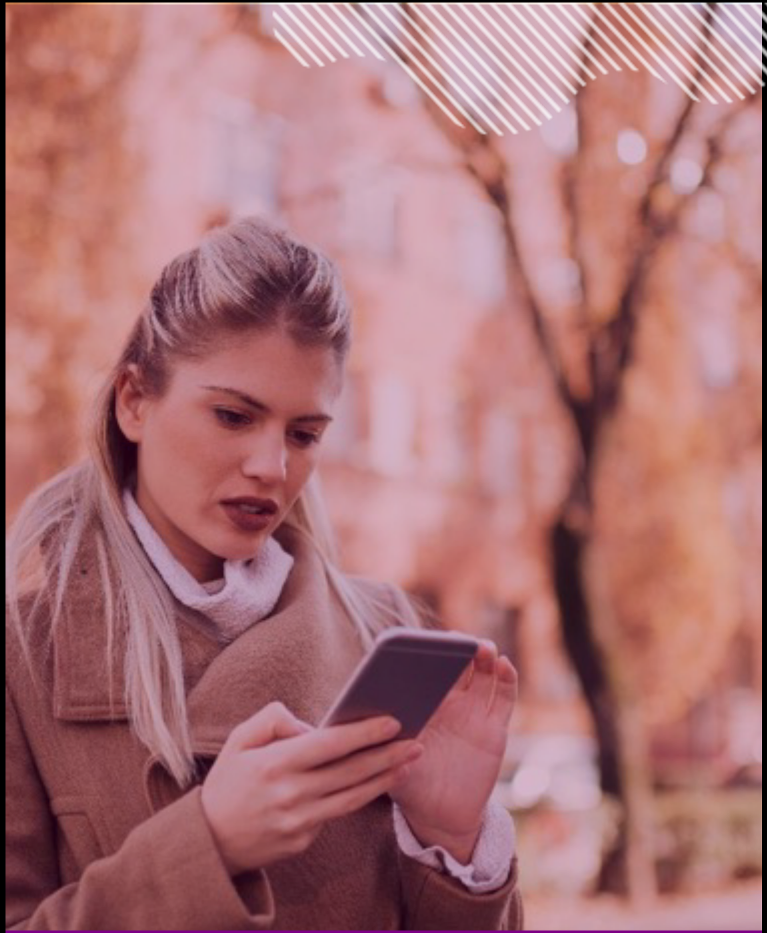
+ Nation-states

+ Volunteers

Source: Future Risk Report 2021, AXA

Your People Expect

Work anywhere

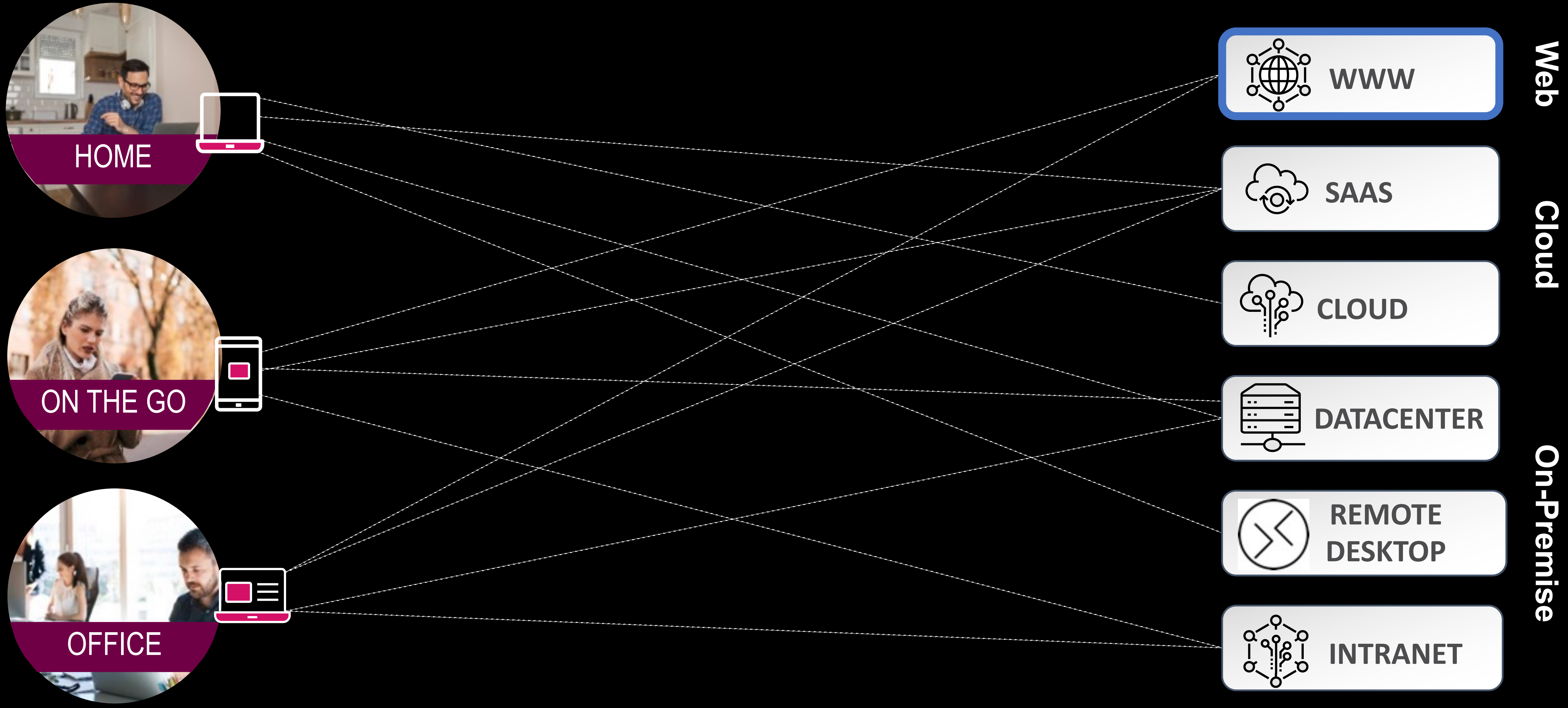


Use every device

Access any application

In The New World

We Want To Use Any Device To Access Any Application



1 of 5 businesses suffered an impactful breach

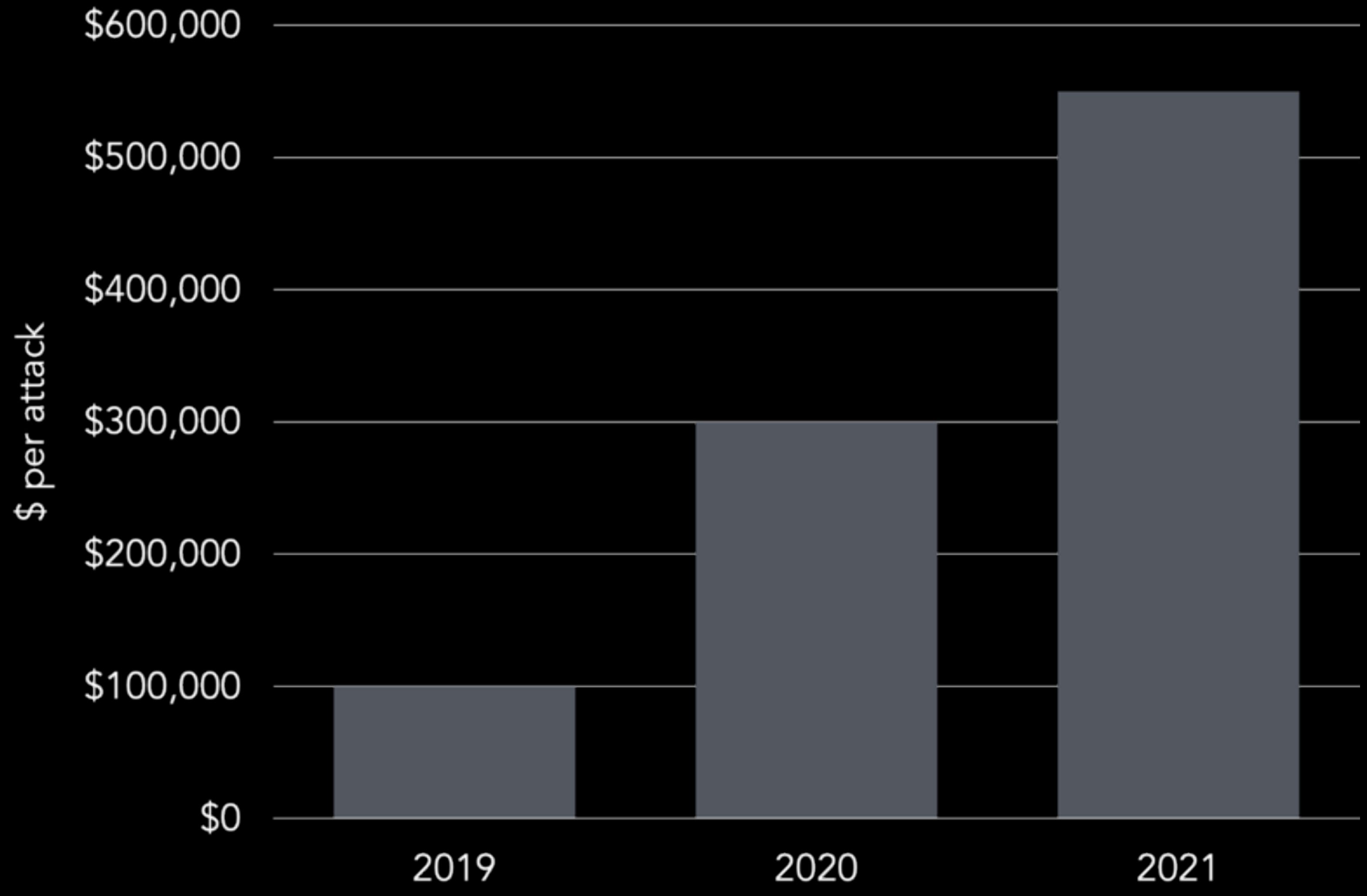
every **39** seconds a business is hacked

Weeks of downtime. Many SMBs do not recover

21% of North American foundations reported a security breach in the preceding two years.

31% of all nation-state notifications that we send out to organizations go to nonprofits. (MSFT)

Average Ransom Payments



Cybercrime Damages

2021

$2 Trillion | $11 Trillion

2025

** Cybersecurity Ventures*

What Are You Most Afraid of?

General Population

1. Pandemics and infectious diseases
2. Climate Change
3. Terrorism and New Security Threats
4. Cybersecurity Risk
5. Social Discontent and Local Conflicts

Risk Experts

1. Cybersecurity Risk
2. Climate Change
3. Pandemics and infectious diseases
4. Social Discontent and Local Conflicts
5. Geopolitical Instability

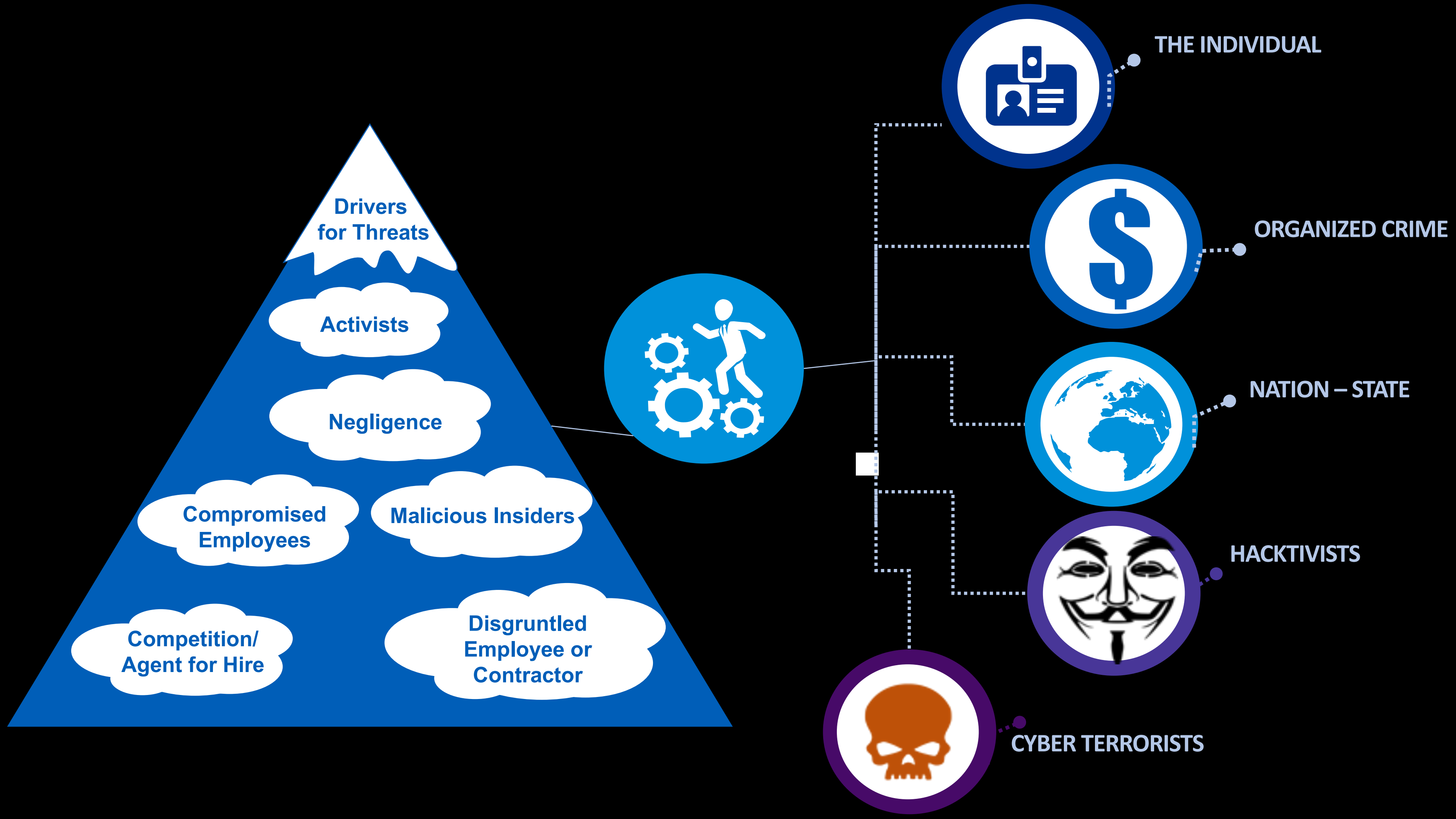
Source: Future Risk Report 2021, AXA

Breach Business Impact

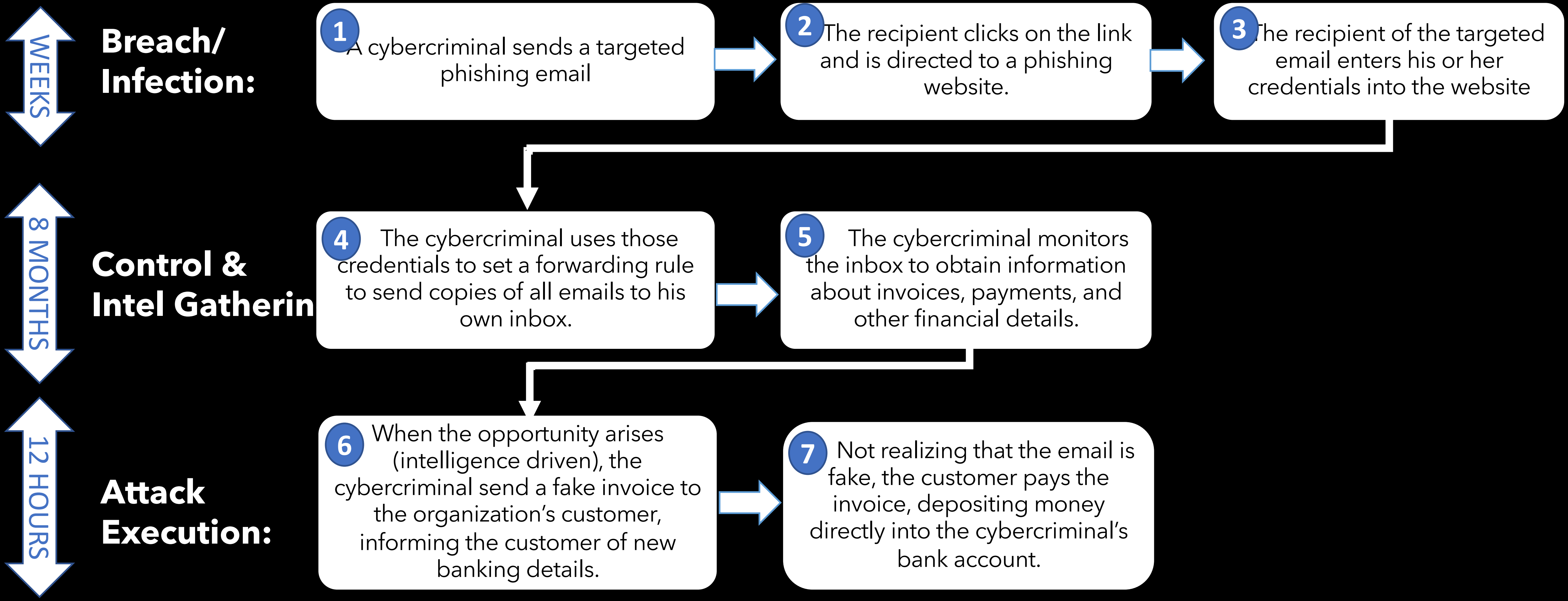
	short term	medium term	long term
Direct costs	Consultant fees Cyber ransom and extortion losses Financial theft Insurance excess Staff response (overtime) Staff response costs (contracting external staff)	Changes in cyber security practices Compensation/discounts Complaints (external) Fines Investigation (external) Legal PR/marketing activities (external) Recruitment costs Third party liability	Credit rating/insurance premiums Cyber security improvements Investment/donor/funding loss Staff costs (long term) Training costs Training costs (external resources) Share value
Indirect costs	Containment Data and software loss Intellectual property theft Interruption of staffs' business as usual activities (opportunity cost) T equipment damage Notification costs (authorities) Notification costs (customer) Physical equipment damage (not including it equipment damage) Interruption of service	Complaints (internal) Investigation (internal) Post-breach customer protection PR/marketing activities (internal) Customers departure	Customer attrition Cyber security improvements (opportunity cost) Long term productivity Supply chain attrition Training costs (internal resources) Training costs (opportunity cost)

Types of Attacks

Who's Attacking You?



Anatomy of Attack (example)



WEEKS

Breach/ Infection:

1 A cybercriminal sends a targeted phishing email

2 The recipient clicks on the link and is directed to a phishing website.

3 The recipient of the targeted email enters his or her credentials into the website

8 MONTHS

Control & Intel Gatherin

4 The cybercriminal uses those credentials to set a forwarding rule to send copies of all emails to his own inbox.

5 The cybercriminal monitors the inbox to obtain information about invoices, payments, and other financial details.

12 HOURS

Attack Execution:

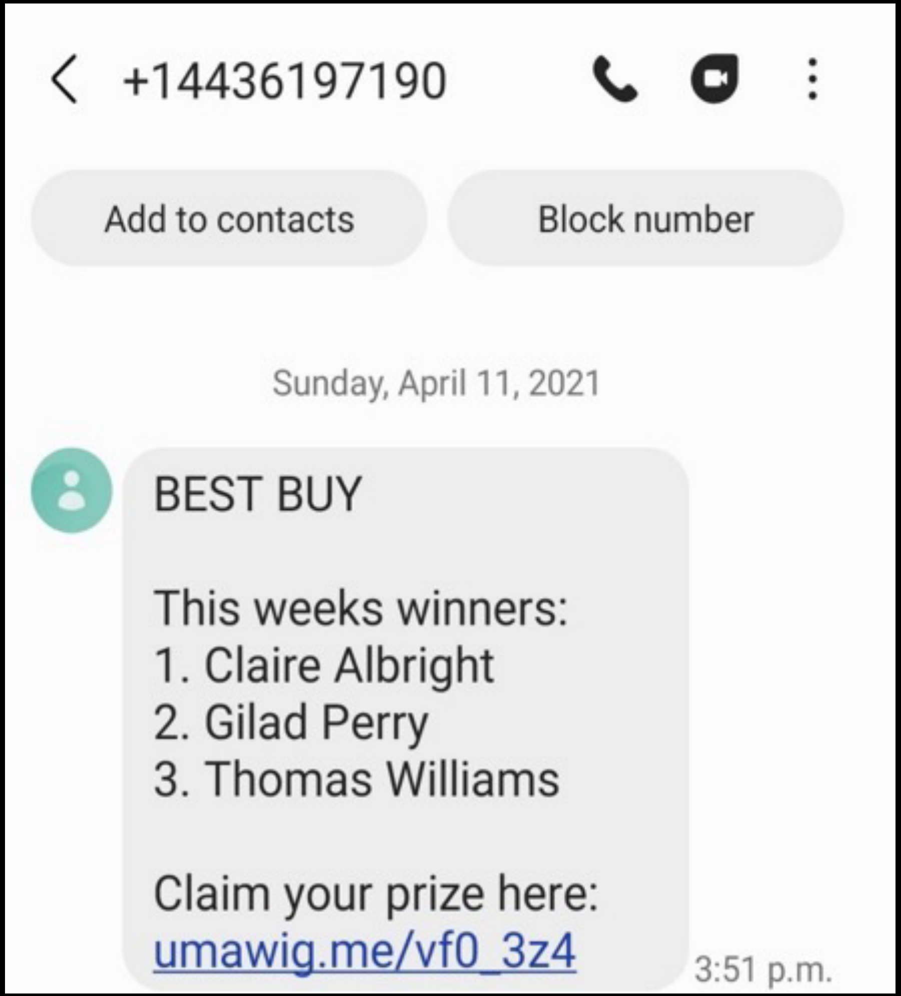
6 When the opportunity arises (intelligence driven), the cybercriminal send a fake invoice to the organization's customer, informing the customer of new banking details.

7 Not realizing that the email is fake, the customer pays the invoice, depositing money directly into the cybercriminal's bank account.

Social Engineering and Phishing

***65%** of attacker groups used spear phishing as the primary infection vector.*

Phishing



Sunday, April 11, 2021

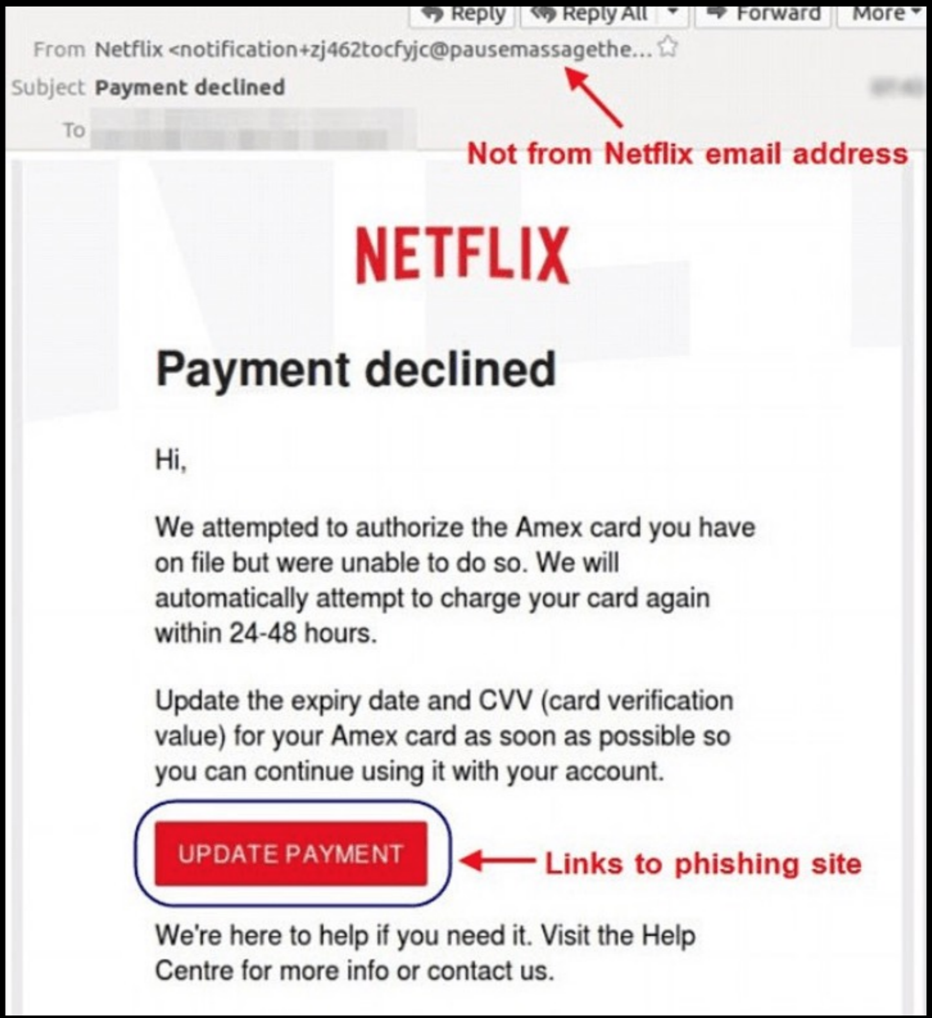
BEST BUY

This weeks winners:
1. Claire Albright
2. Gilad Perry
3. Thomas Williams

Claim your prize here:
umawig.me/vf0_3z4

3:51 p.m.

SMS



From Netflix <notification+zj462tocfyjc@pausemassagethe...

Subject **Payment declined**

To [redacted]

Not from Netflix email address

Payment declined

Hi,

We attempted to authorize the Amex card you have on file but were unable to do so. We will automatically attempt to charge your card again within 24-48 hours.

Update the expiry date and CVV (card verification value) for your Amex card as soon as possible so you can continue using it with your account.

Links to phishing site

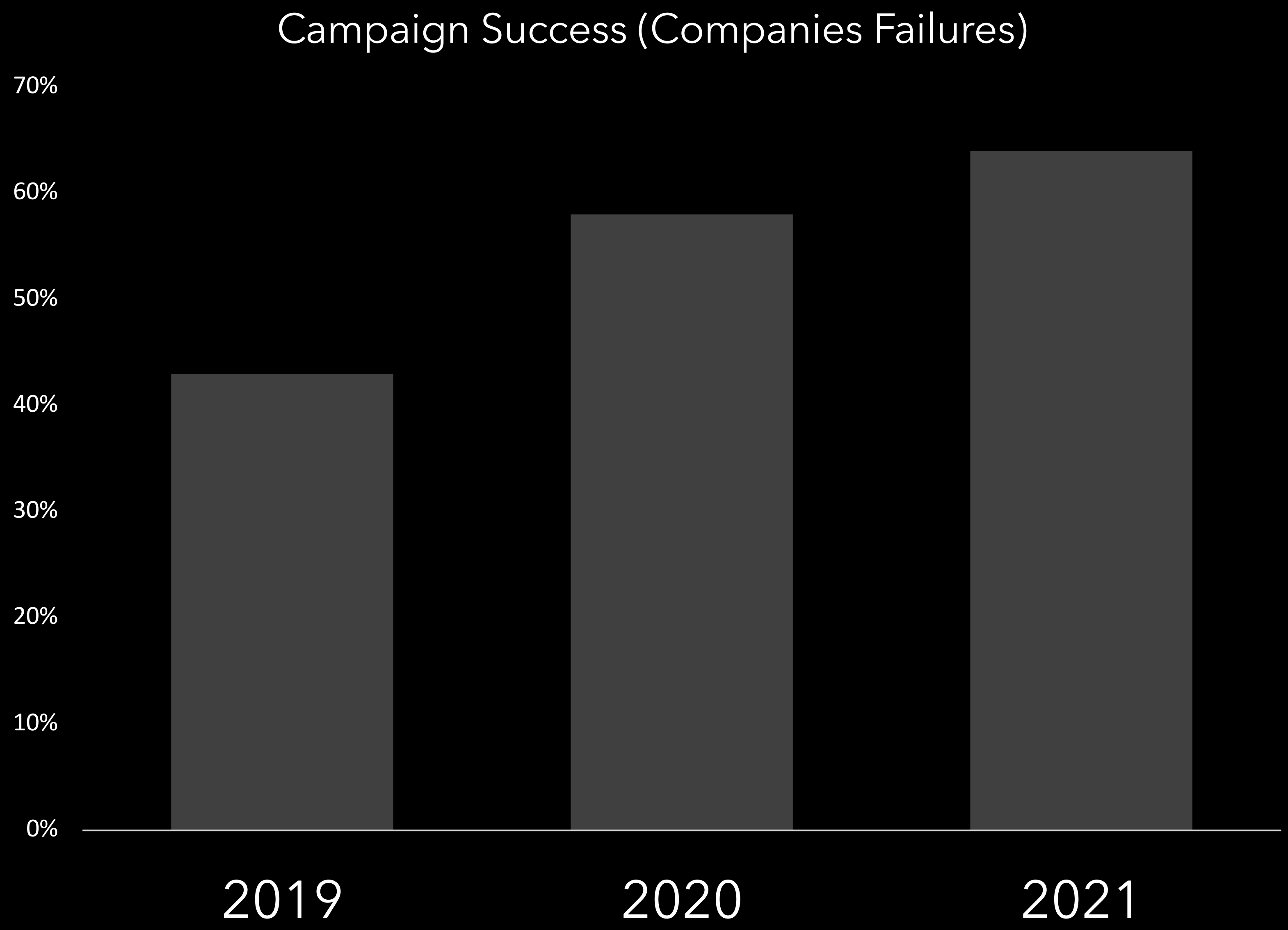
We're here to help if you need it. Visit the Help Centre for more info or contact us.

EMAIL

No food for you!
You’ve been phished!

- Establish trust
- The right context
- Sense of urgency
- Leveraging human nature
- Device of choice
- Disarming defenses

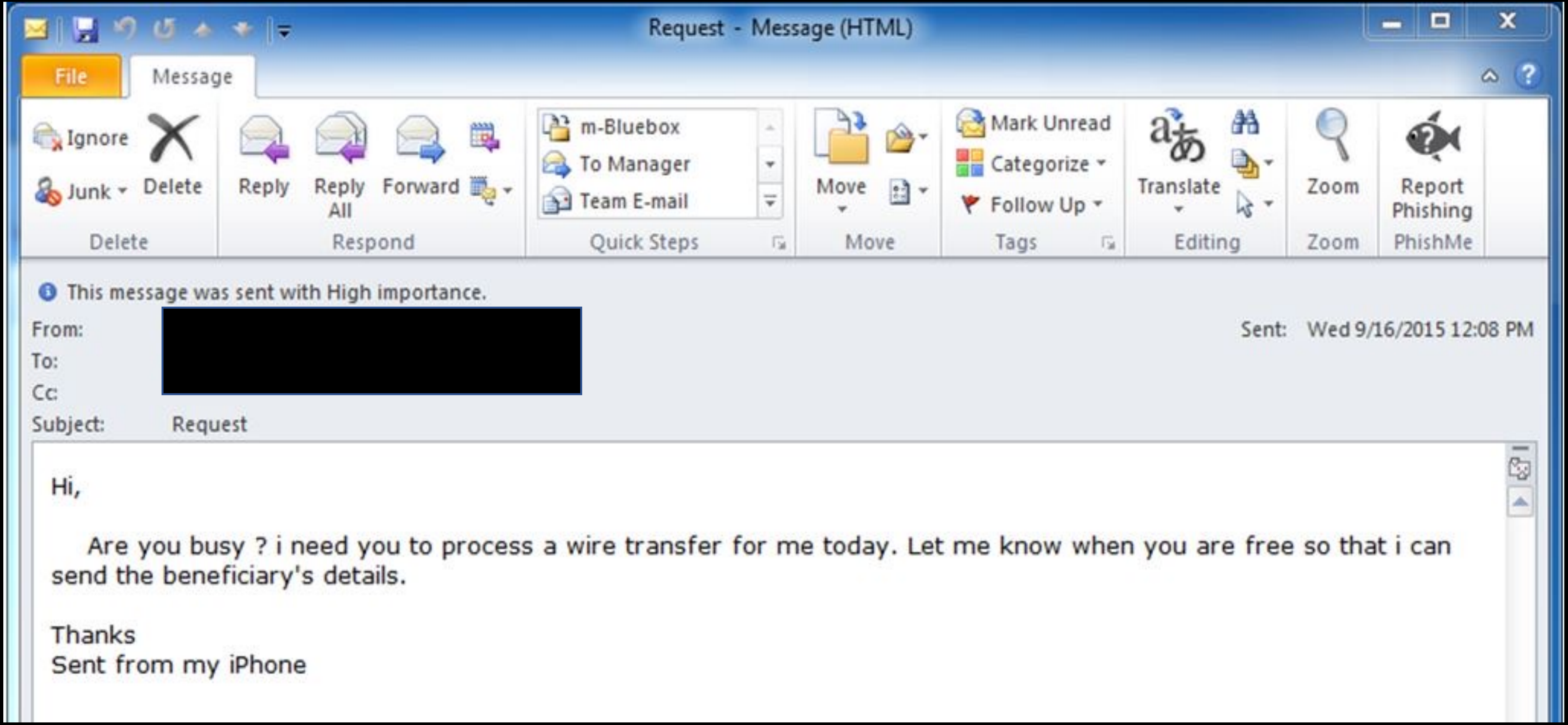
Phishing Is Smarter Now



BEC
Spoofing/CEO-CFO Fraud

94% *of malware was delivered via email.*

BEC/Spoofing/CEO-CFO Fraud



This message was sent with High importance.

From: [redacted]

To:

Cc:

Sent: Wed 9/16/2015 12:08 PM

Subject: Request

Hi,

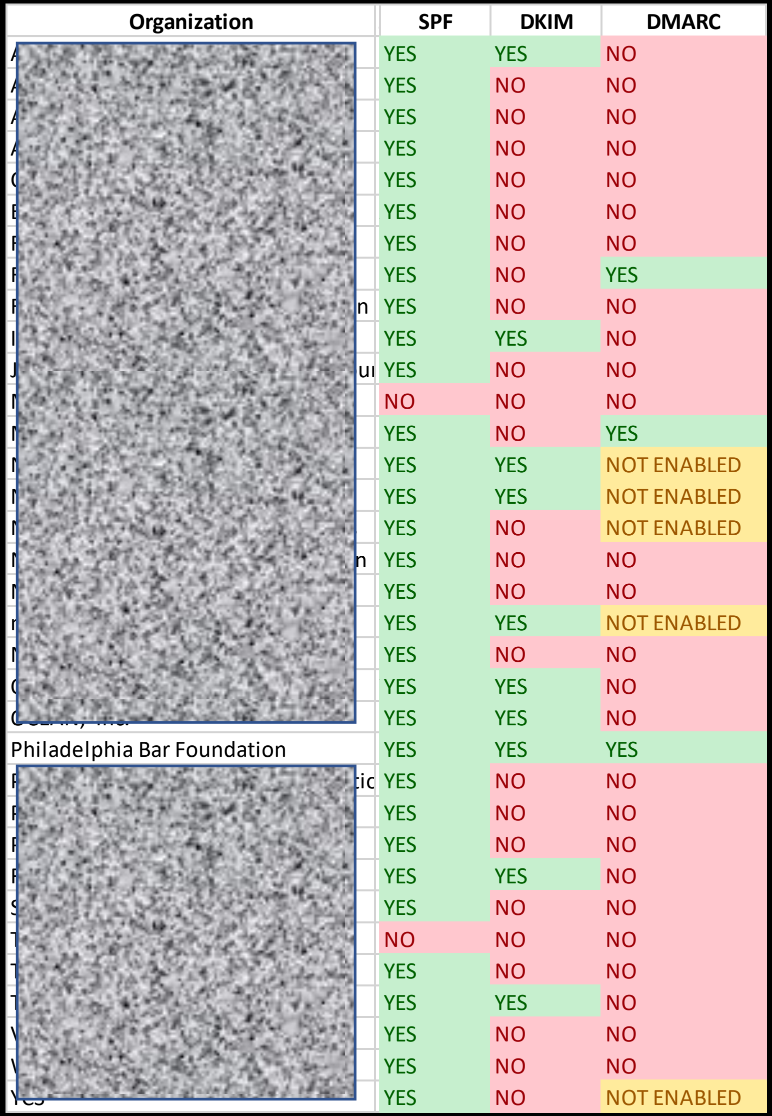
Are you busy ? i need you to process a wire transfer for me today. Let me know when you are free so that i can send the beneficiary's details.

Thanks
Sent from my iPhone

*FBI has estimated losses from such fraud to **4.1 Billion USD***

Email Protection Starts with the Basics

- **Sender Policy Framework (SPF)** - an email authentication method designed to detect forging sender addresses
- **DomainKeys Identified Mail (DKIM)** - allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain
- **DMARC** email authentication protocol that give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing

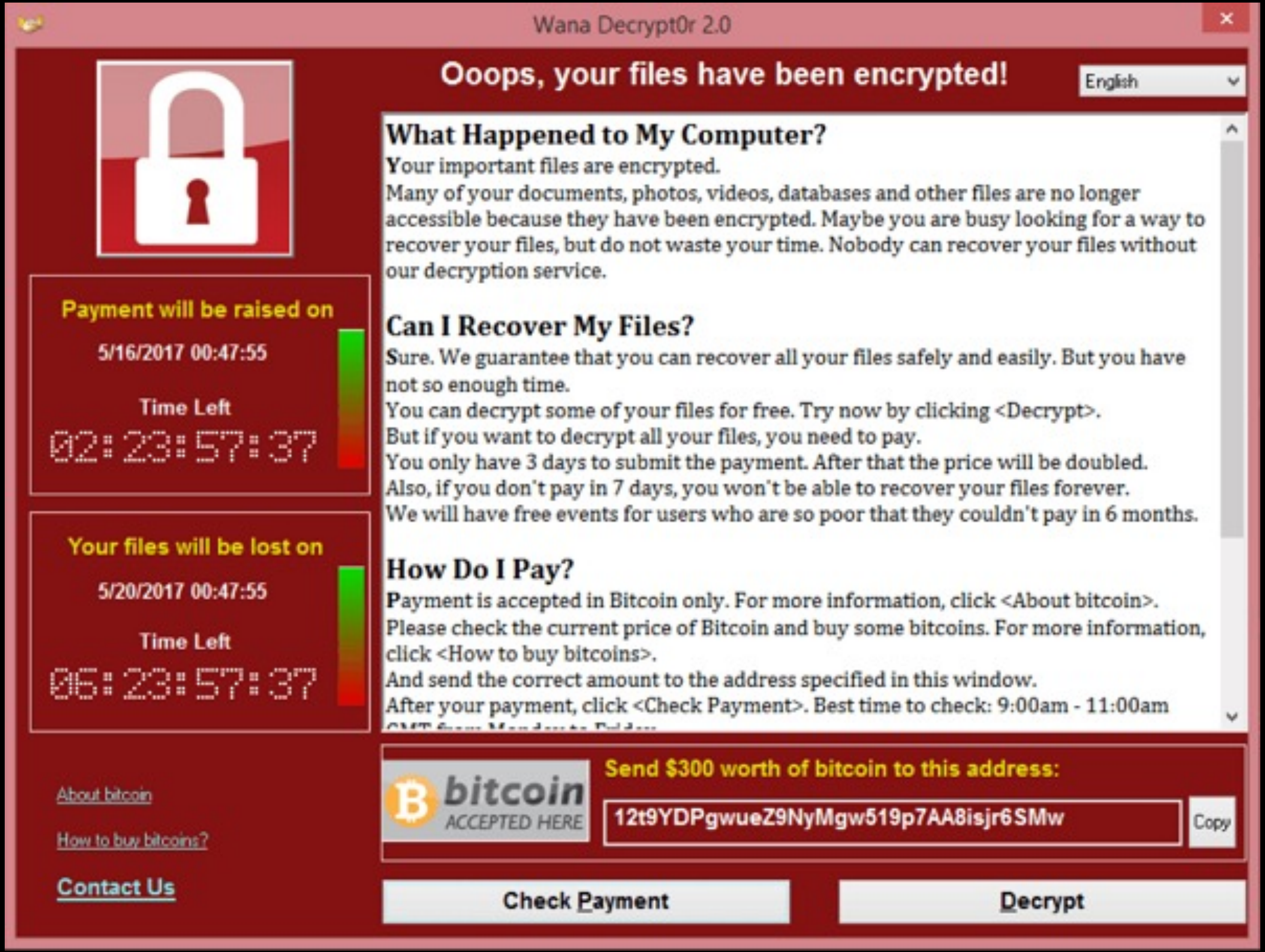


Organization	SPF	DKIM	DMARC
[redacted]	YES	YES	NO
[redacted]	YES	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	NO	YES
[redacted]	YES	NO	NO
[redacted]	YES	YES	NO
[redacted]	YES	NO	NO
[redacted]	NO	NO	NO
[redacted]	YES	NO	YES
[redacted]	YES	YES	NOT ENABLED
[redacted]	YES	YES	NOT ENABLED
[redacted]	YES	NO	NOT ENABLED
[redacted]	YES	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	YES	NOT ENABLED
[redacted]	YES	NO	NO
[redacted]	YES	YES	NO
[redacted]	YES	YES	NO
Philadelphia Bar Foundation	YES	YES	YES
[redacted]	YES	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	YES	NO
[redacted]	YES	NO	NO
[redacted]	NO	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	YES	NO
[redacted]	YES	NO	NO
[redacted]	YES	NO	NO
[redacted]	YES	NO	NOT ENABLED

Ransomware

40% of spam email contains ransomware (IBM)

Ransomware Attack



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

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.

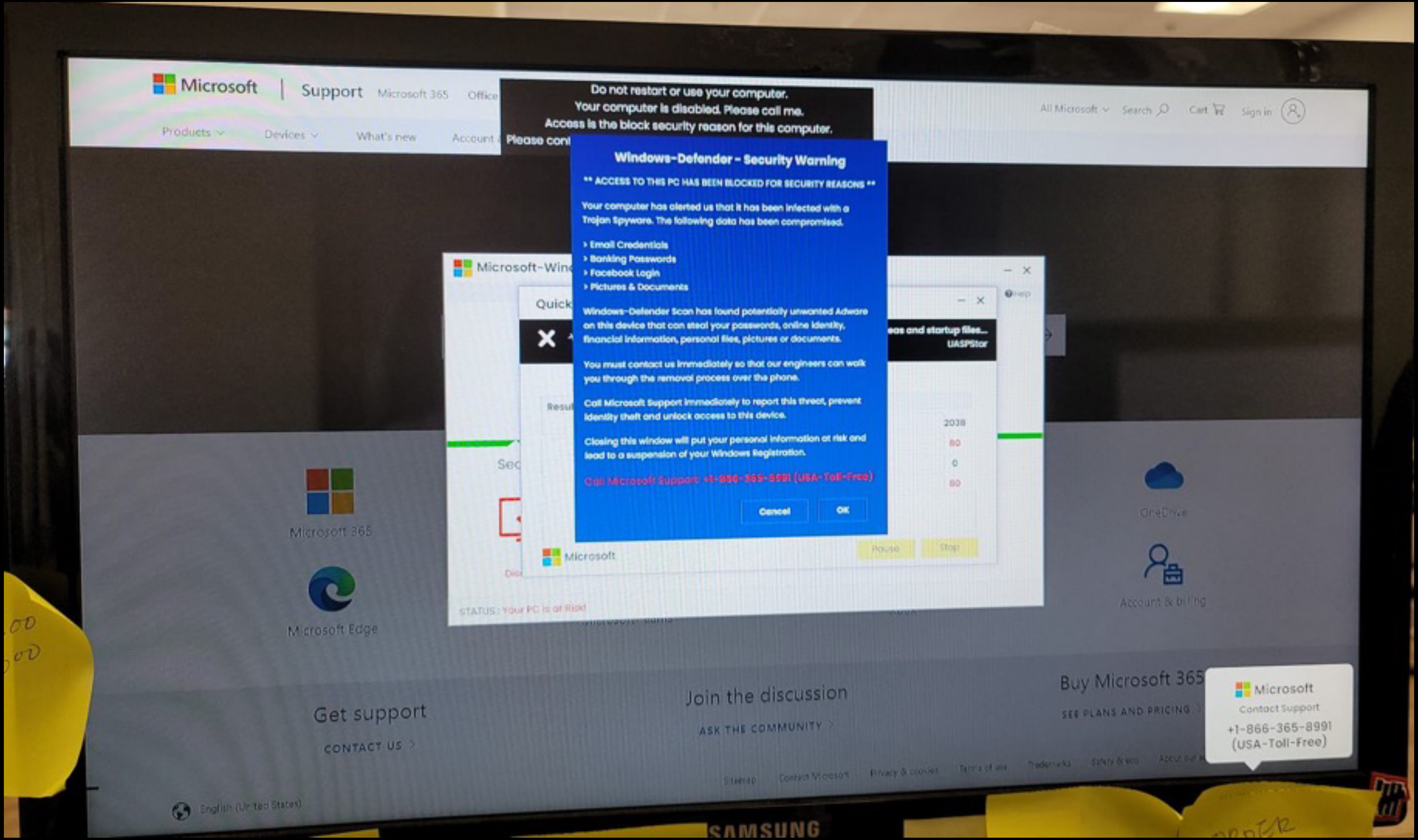
How Do I Pay?

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 GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Browser Highjack Fraud



Do not restart or use your computer.
Your computer is disabled. Please call me.
Access is the block security reason for this computer.
Please con

Windows-Defender - Security Warning

** ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS **

Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.

› Email Credentials
› Banking Passwords
› Facebook Login
› Pictures & Documents

Windows-Defender Scan has found potentially unwanted Adware on this device that can steal your passwords, online identity, financial information, personal files, pictures or documents.

You must contact us immediately so that our engineers can walk you through the removal process over the phone.

Call Microsoft Support immediately to report this threat, prevent identity theft and unlock access to this device.

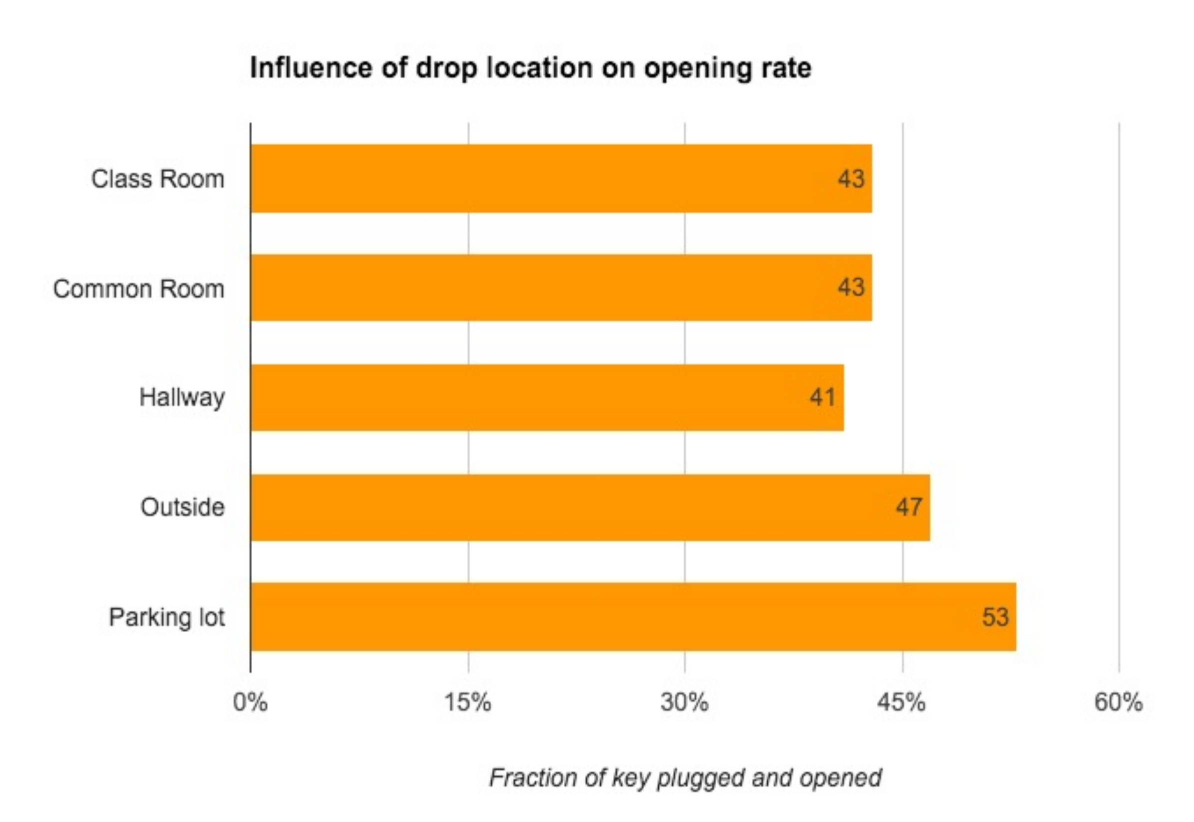
Closing this window will put your personal information at risk and lead to a suspension of your Windows Registration.

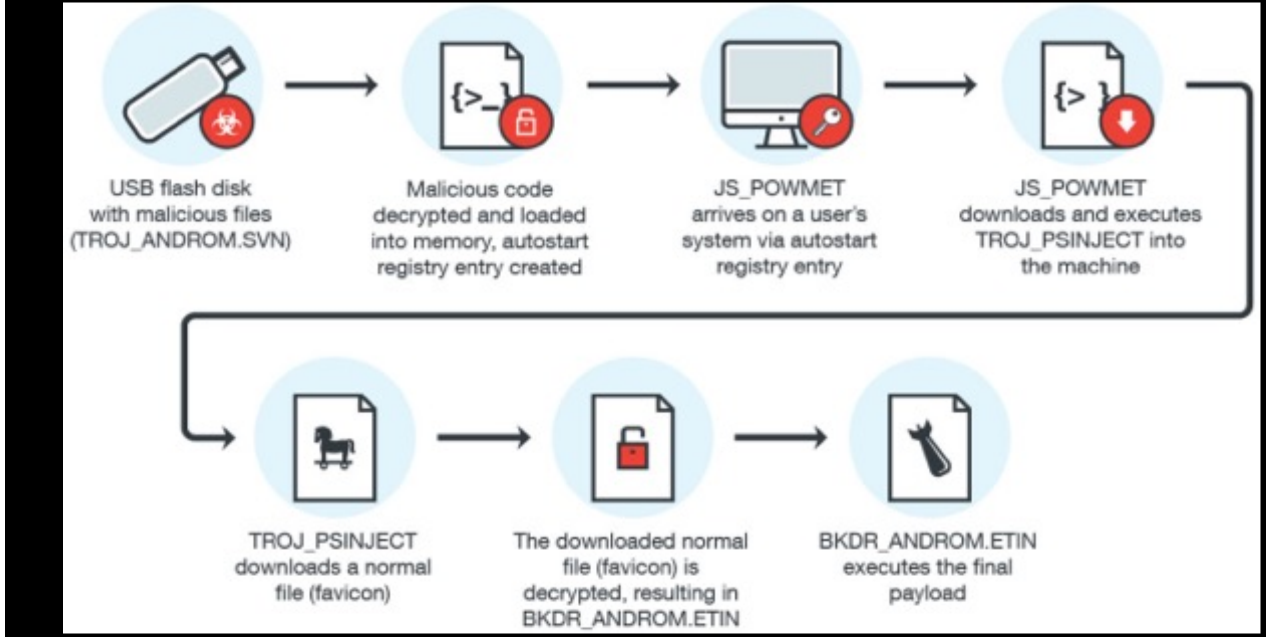
Call Microsoft Support: +1-866-365-8991 (USA-Toll-Free)

Cancel OK

Microsoft
Contact Support
+1-866-365-8991
(USA-Toll-Free)

USB Drop





USB flash disk with malicious files (TROJ_ANDROM.SVN)

Malicious code decrypted and loaded into memory, autostart registry entry created

JS_POWMET arrives on a user's system via autostart registry entry

JS_POWMET downloads and executes TROJ_PSINJECT into the machine

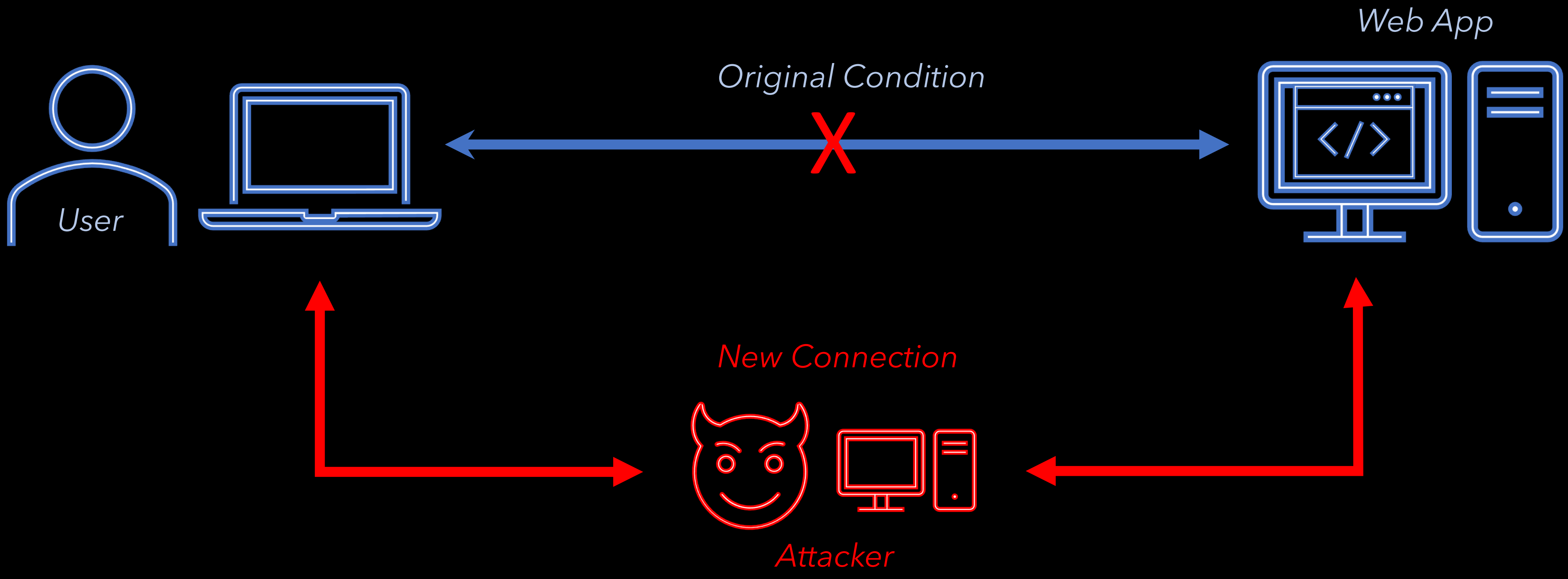
TROJ_PSINJECT downloads a normal file (favicon)

The downloaded normal file (favicon) is decrypted, resulting in BKDR_ANDROM.ETIN

BKDR_ANDROM.ETIN executes the final payload

Unattended USB Devices: *Another common avenue how hackers break into organizations*

Man in the Middle Attack



A very old attack technique that is still valid today – often seen in public places with "Free" Wifi access

Defending Against Cyber Attacks

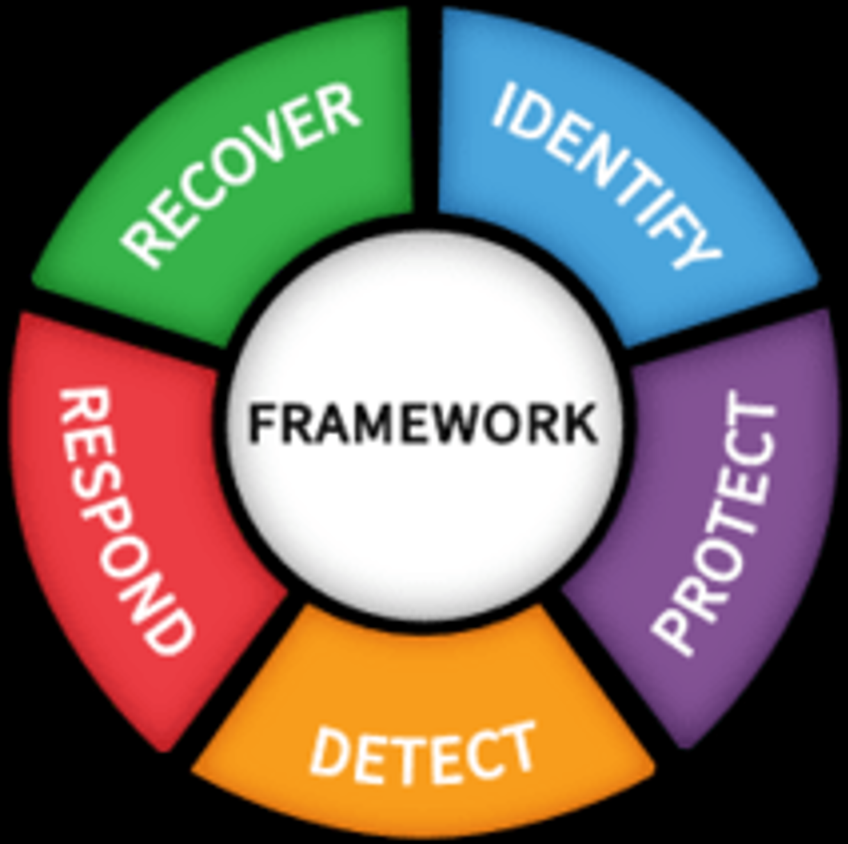
Cybersecurity Program Fundamentals

Recover

- Recover Planning
- Improvements
- Communications

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements



Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

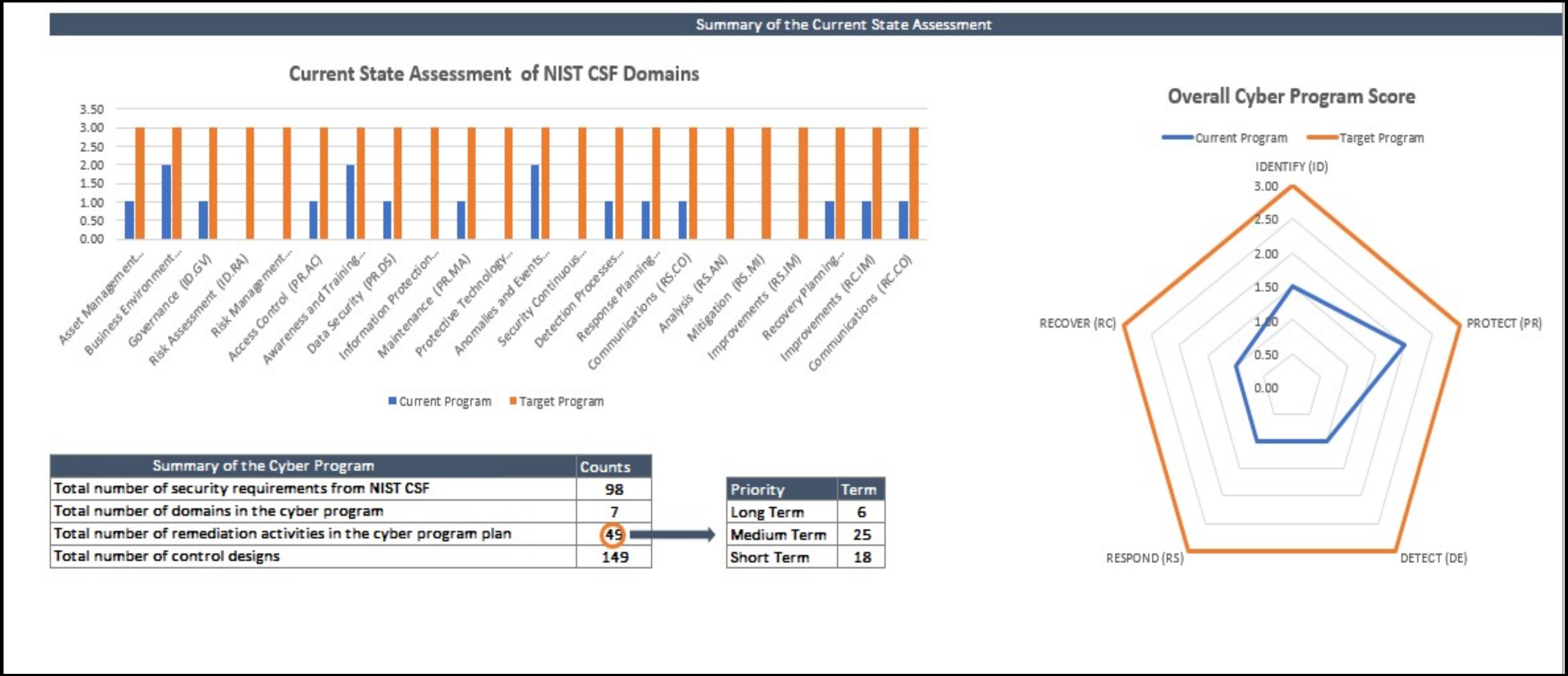
Protect

- Access Controls
- Awareness & training
- Data Security
- Information protection and procedures
- Maintenance
- Protective technology

Detect

- Anomalies and events
- Security Continuous Monitoring
- Detection process

Cybersecurity Program Fundamentals



Summary of the Current State Assessment

Summary of the Cyber Program	Counts
Total number of security requirements from NIST CSF	98
Total number of domains in the cyber program	7
Total number of remediation activities in the cyber program plan	49
Total number of control designs	149

Priority	Term
Long Term	6
Medium Term	25
Short Term	18

Control Your Destiny

1. Identify Crown Jewels
2. Gain Visibility
3. Introduce Resiliency (p/t)
4. Nurture Awareness Culture (p)
5. Proactively manage business-risk

Limited budget?

Use the **right tools** for the right job.

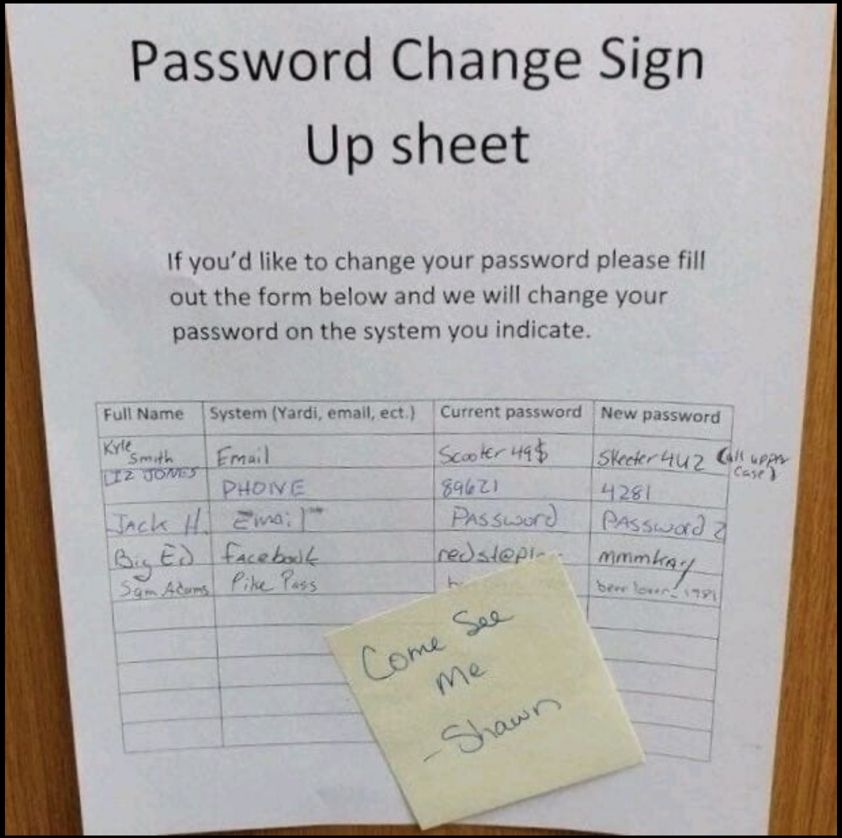
Control what's under your control.

Set **configurations** right. Not Easy.

Passwords are a big problem.

Password Management

- ✗ Cat and dog names
- ✗ Kids names
- ✗ Names and special dates
- ✗ Same password, different variations
- ✗ @ instead of “a”; ! Instead of 1
- ✗ Password under the keyboard
- ✓ Password Manager



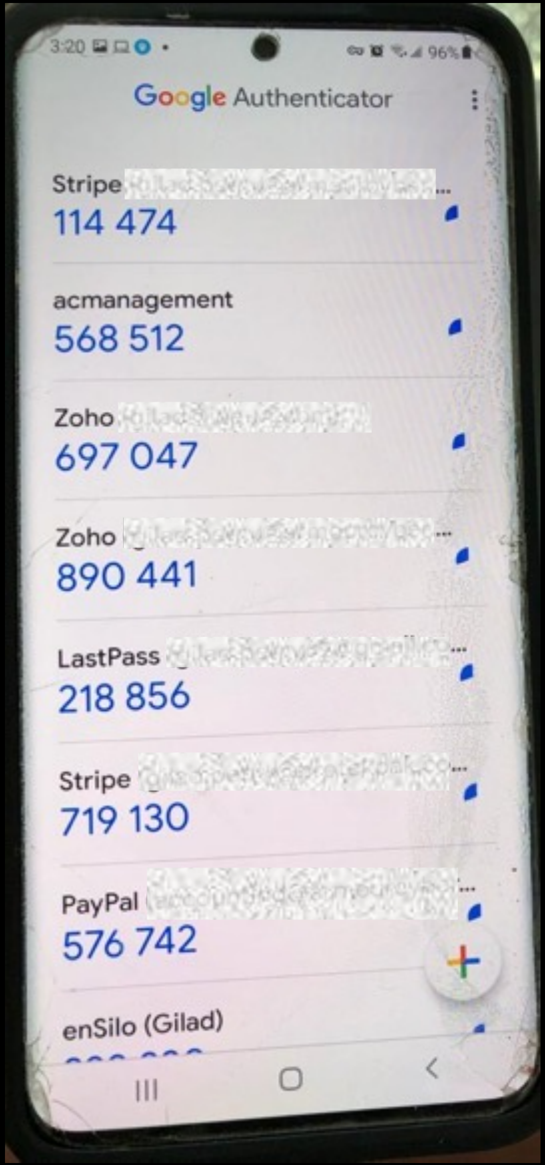
Password Change Sign Up sheet

If you’d like to change your password please fill out the form below and we will change your password on the system you indicate.

Full Name	System (Yardi, email, ect.)	Current password	New password
Kyle Smith	Email	Scooter 49$	Skeeter 4U2 (all upper case)
LIZ JONES	PHONE	89621	4281
Jack H.	Email	Password	Password 2
Big Ed	Facebook	redst@pl-	mmmkay
Sam Adams	Pike Pass	h	beer lover!1981

Come See Me -Shawn

Multi Factor Authentication



3:20 96%

Google Authenticator

Stripe [redacted]
114 474

acmanagement
568 512

Zoho [redacted]
697 047

Zoho [redacted]
890 441

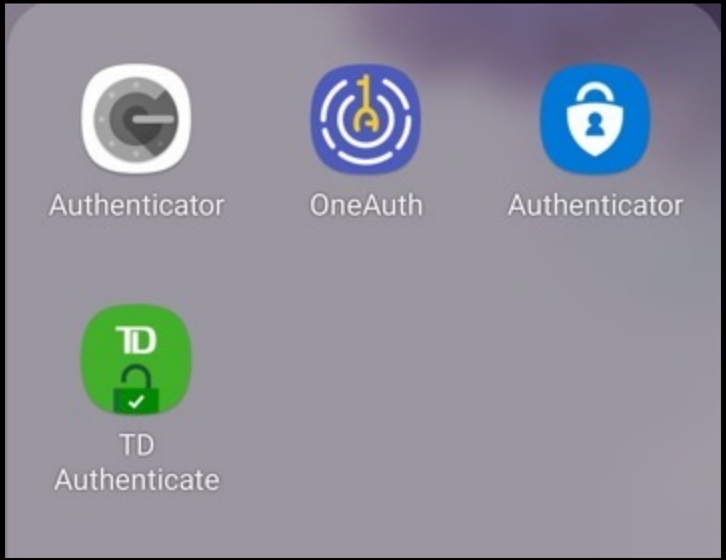
LastPass [redacted]
218 856

Stripe [redacted]
719 130

PayPal [redacted]
576 742

enSilo (Gilad)

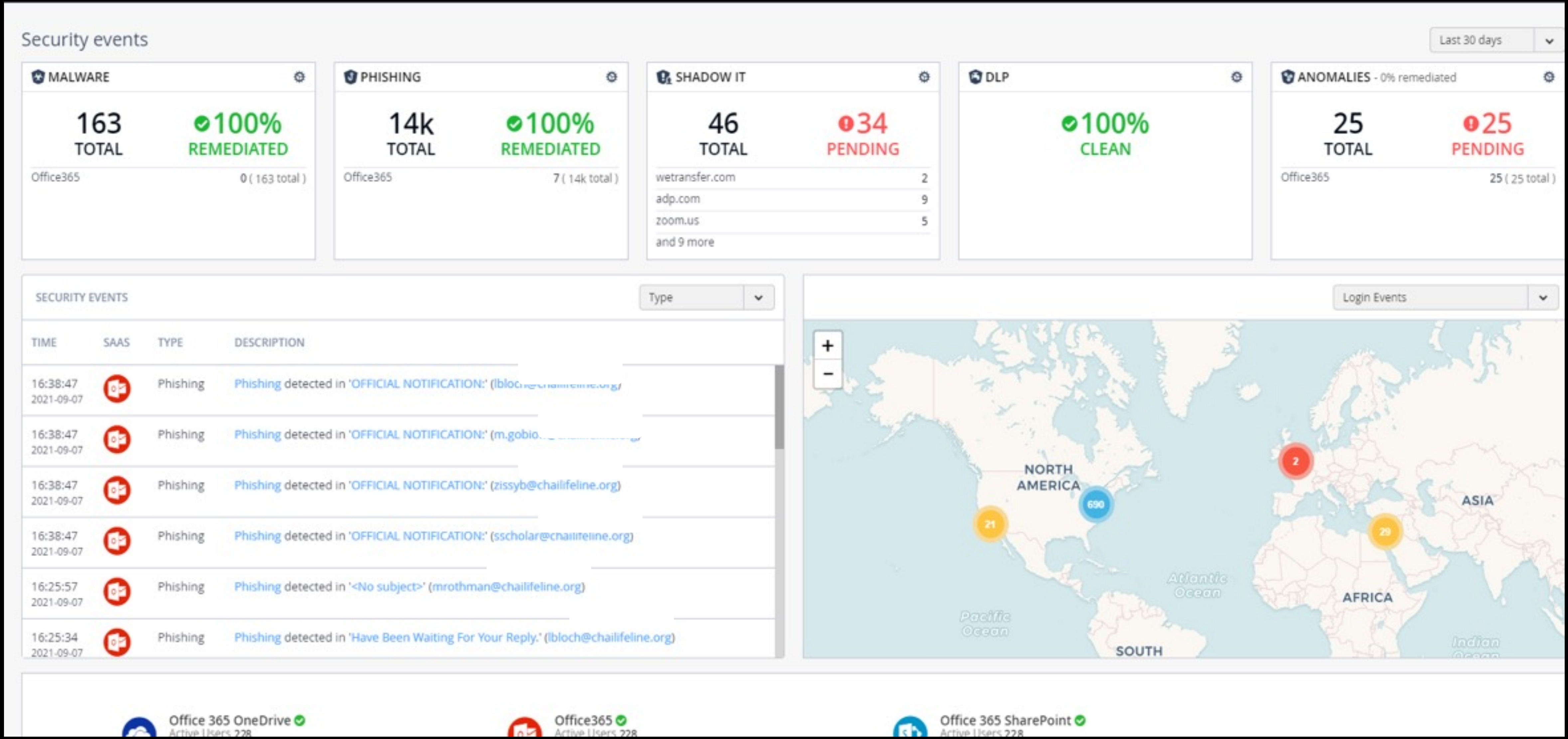
For critical accounts including email, financial, social media , health related accounts or any solution that supports it!



Email and productivity suites are wide open, and most commonly used.

Email and Productivity Suites

Keeping Up With The Adversaries



Security events

Last 30 days

MALWARE

163 TOTAL — 100% REMEDIATED

Office365 — 0 (163 total)

PHISHING

14k TOTAL — 100% REMEDIATED

Office365 — 7 (14k total)

SHADOW IT

46 TOTAL — 34 PENDING

wetransfer.com	2
adp.com	9
zoom.us	5
and 9 more	

DLP

100% CLEAN

ANOMALIES - 0% remediated

25 TOTAL — 25 PENDING

Office365 — 25 (25 total)

SECURITY EVENTS

Type

TIME	SAAS	TYPE	DESCRIPTION
16:38:47 2021-09-07		Phishing	Phishing detected in 'OFFICIAL NOTIFICATION:' (lbloc[redacted])
16:38:47 2021-09-07		Phishing	Phishing detected in 'OFFICIAL NOTIFICATION:' (m.gobio[redacted])
16:38:47 2021-09-07		Phishing	Phishing detected in 'OFFICIAL NOTIFICATION:' (zissyb@chailifeline.org)
16:38:47 2021-09-07		Phishing	Phishing detected in 'OFFICIAL NOTIFICATION:' (sscholar@chailifeline.org)
16:25:57 2021-09-07		Phishing	Phishing detected in '<No subject>' (mrothman@chailifeline.org)
16:25:34 2021-09-07		Phishing	Phishing detected in 'Have Been Waiting For Your Reply.' (lbloch@chailifeline.org)

Login Events

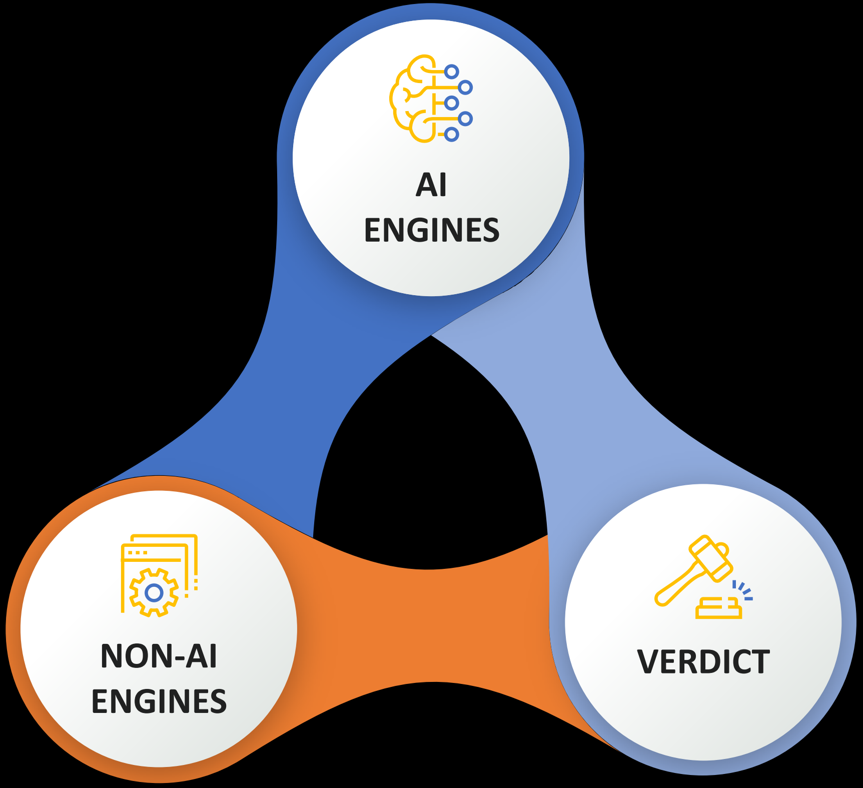
Office 365 OneDrive ✓ Active Users 228

Office365 ✓ Active Users 228

Office 365 SharePoint ✓ Active Users 228

Email and Productivity Suites

Keeping Up With The Adversaries

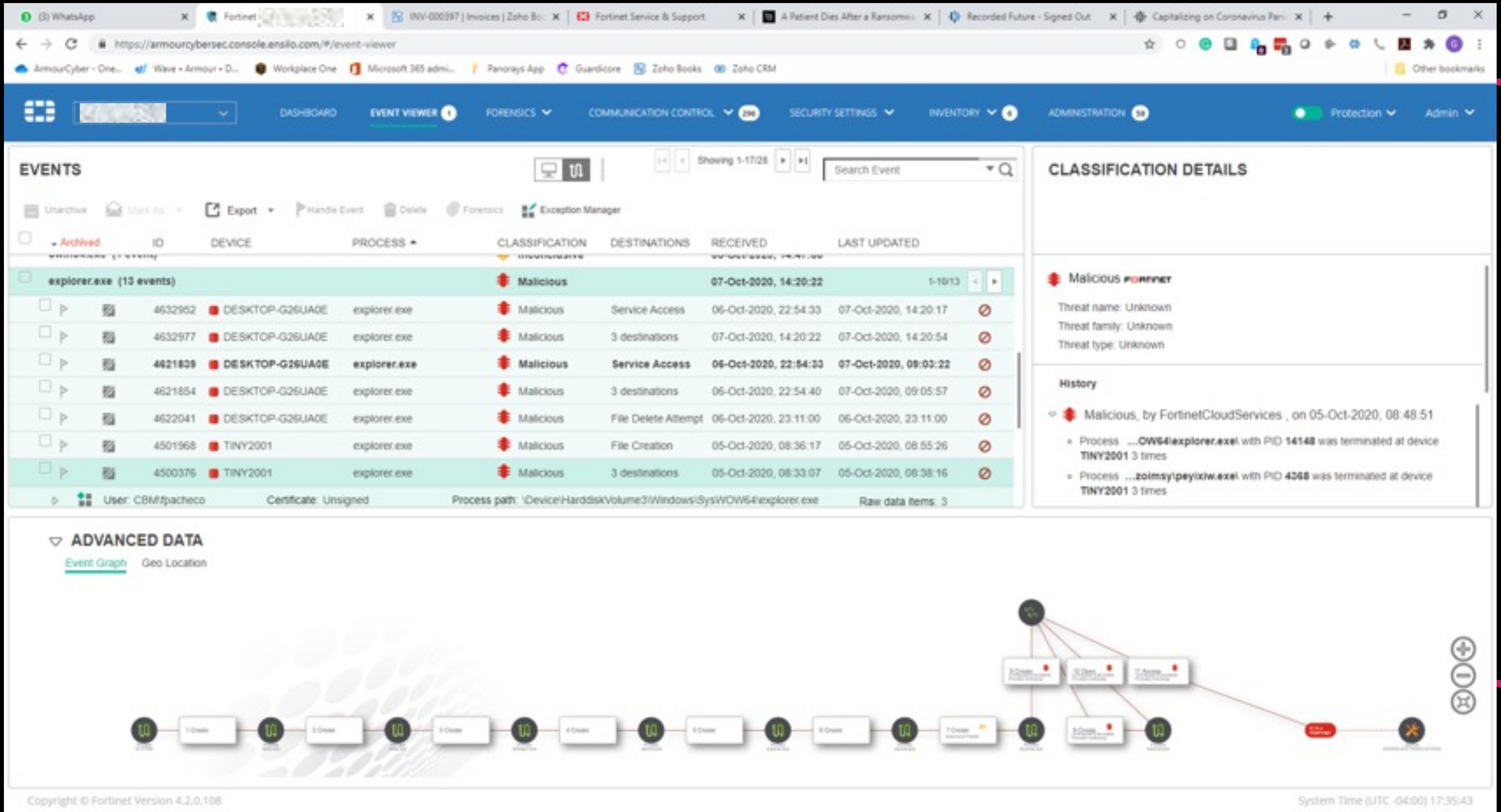


- Human Interaction Simulator
- Neural Network Model
- CPU-level Detection
- AI-based Behavioral Patterns
- Evasion Detection
- Documents macro analyzer
- DeepScan
- AI-based Aggregator Model
- Macro Analysis
- Virtual Network Service
- Malware DNA
- Click-time URL Protection
- Malware Universe Model
- Network Activity Monitor
- Reputation Analysis

Traditional Anti-virus Protects Against Yesterday’s Threats

End Point Detection and Response (EDR)

Block Malware Before It Infiltrates Your Organization



EVENTS

	Archived	ID	DEVICE	PROCESS ▴	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	
□	explorer.exe (13 events)				Malicious		07-Oct-2020, 14:20:22		
□ ▷		4632952	DESKTOP-G26UA0E	explorer.exe	Malicious	Service Access	06-Oct-2020, 22:54:33	07-Oct-2020, 14:20:17	⊘
□ ▷		4632977	DESKTOP-G26UA0E	explorer.exe	Malicious	3 destinations	07-Oct-2020, 14:20:22	07-Oct-2020, 14:20:54	⊘
□ ▷		**4621839**	**DESKTOP-G26UA0E**	**explorer.exe**	**Malicious**	**Service Access**	**06-Oct-2020, 22:54:33**	**07-Oct-2020, 09:03:22**	⊘
□ ▷		4621854	DESKTOP-G26UA0E	explorer.exe	Malicious	3 destinations	06-Oct-2020, 22:54:40	07-Oct-2020, 09:05:57	⊘
□ ▷		4622041	DESKTOP-G26UA0E	explorer.exe	Malicious	File Delete Attempt	06-Oct-2020, 23:11:00	06-Oct-2020, 23:11:00	⊘
□ ▷		4501968	TINY2001	explorer.exe	Malicious	File Creation	05-Oct-2020, 08:36:17	05-Oct-2020, 08:55:26	⊘
□ ▷		4500376	TINY2001	explorer.exe	Malicious	3 destinations	05-Oct-2020, 08:33:07	05-Oct-2020, 08:38:16	⊘

User: CBM\fpacheco   Certificate: Unsigned   Process path: \Device\HarddiskVolume3\Windows\SysWOW64\explorer.exe   Raw data items: 3

CLASSIFICATION DETAILS

Malicious FORTINET

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Malicious, by FortinetCloudServices , on 05-Oct-2020, 08:48:51

- Process **...OW64\explorer.exe\** with PID **14148** was terminated at device **TINY2001** 3 times
- Process **...zoimsy\peyixiw.exe\** with PID **4368** was terminated at device **TINY2001** 3 times

ADVANCED DATA

Copyright © Fortinet Version 4.2.0.108

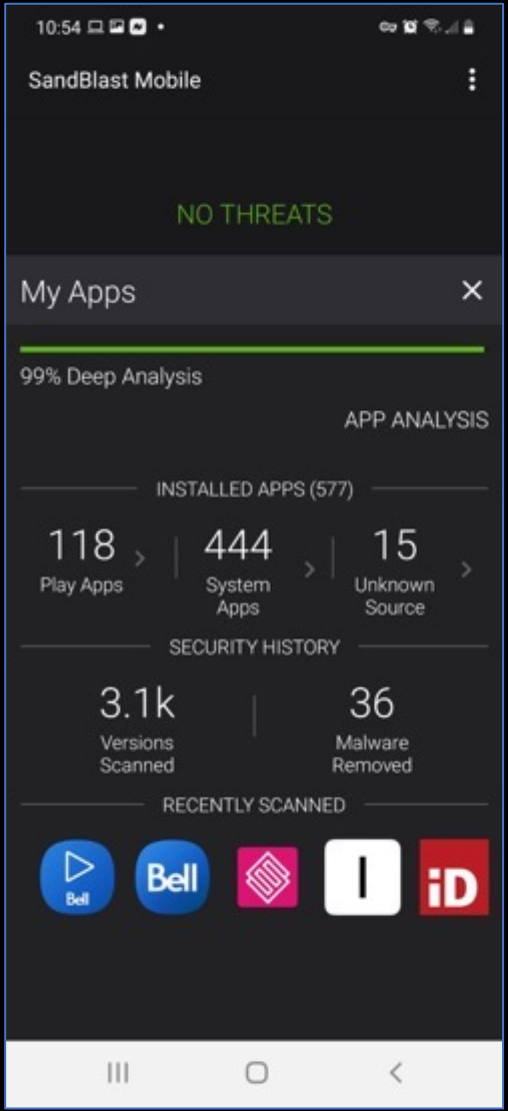
System Time (UTC -04:00) 17:35:43

FORENSICS

EVENT GRAPH

Mobile is the new soft underbelly.

Mobile Security



10:54

SandBlast Mobile

NO THREATS

My Apps ×

99% Deep Analysis

APP ANALYSIS

INSTALLED APPS (577)

118 Play Apps

444 System Apps

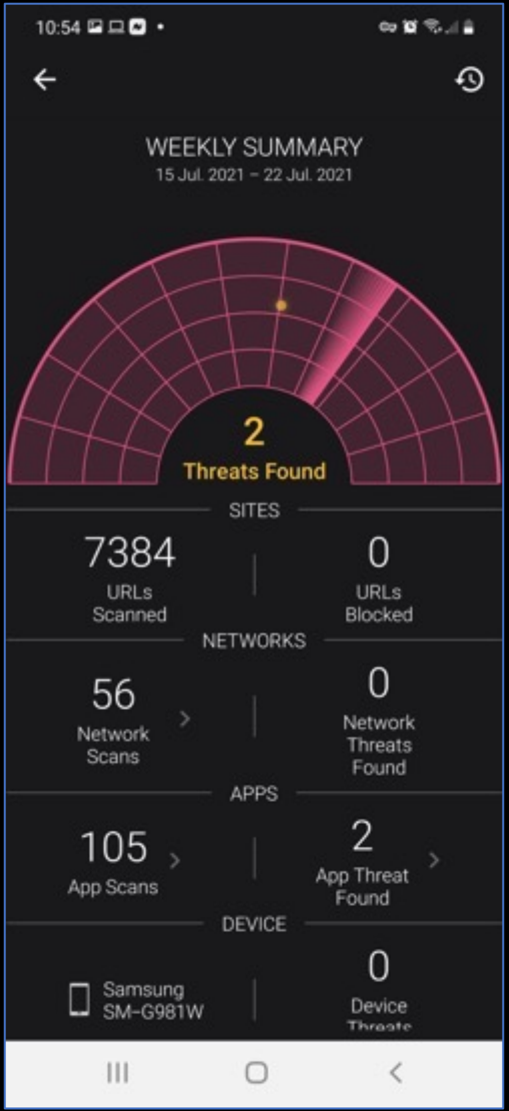
15 Unknown Source

SECURITY HISTORY

3.1k Versions Scanned

36 Malware Removed

RECENTLY SCANNED



10:54

WEEKLY SUMMARY

15 Jul. 2021 – 22 Jul. 2021

2 Threats Found

SITES

7384 URLs Scanned

0 URLs Blocked

NETWORKS

56 Network Scans

0 Network Threats Found

APPS

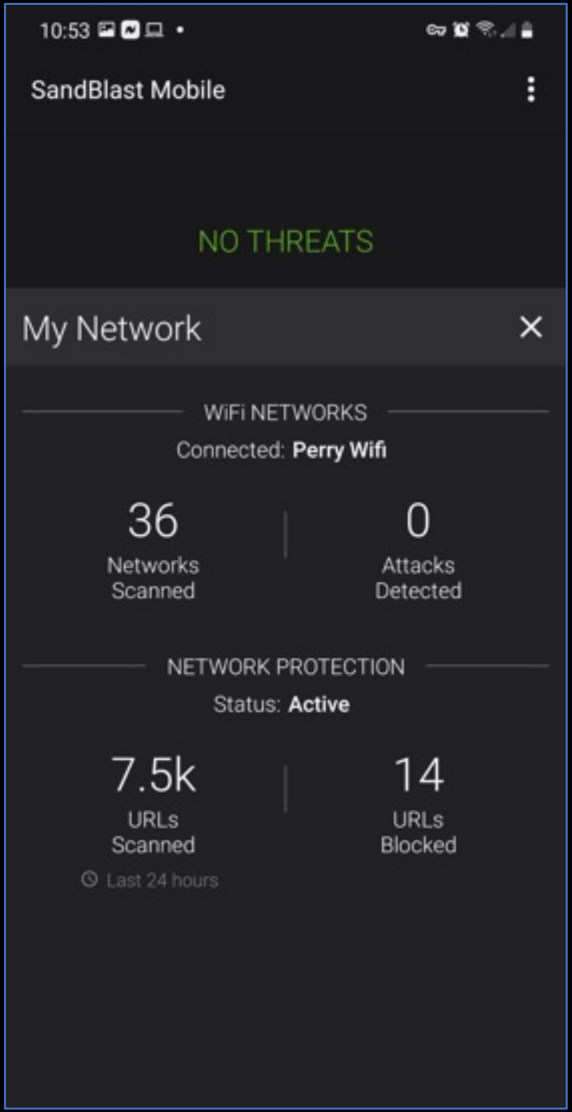
105 App Scans

2 App Threat Found

DEVICE

Samsung SM-G981W

0 Device Threats



10:53

SandBlast Mobile

NO THREATS

My Network ×

WiFi NETWORKS

Connected: **Perry Wifi**

36 Networks Scanned

0 Attacks Detected

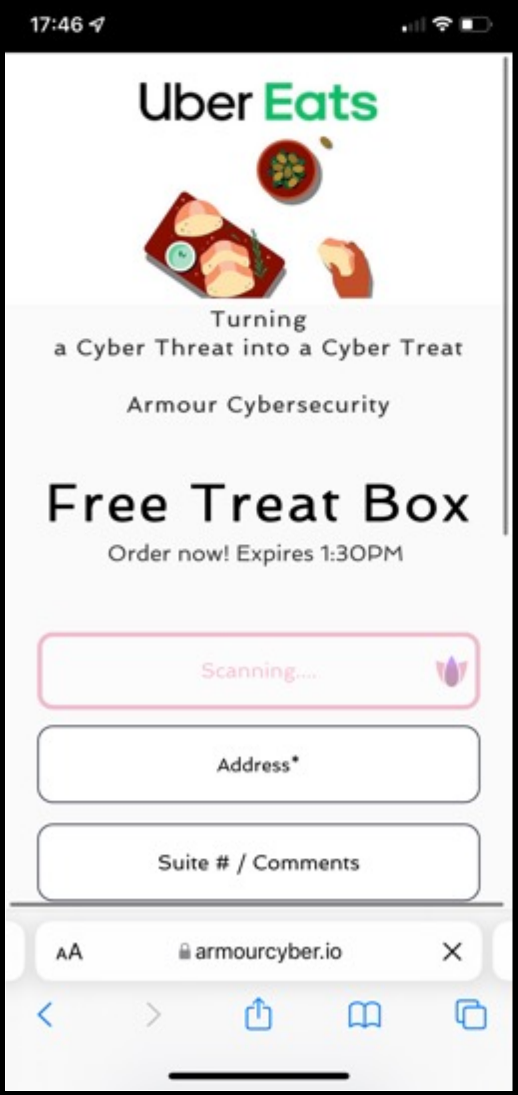
NETWORK PROTECTION

Status: **Active**

7.5k URLs Scanned

Last 24 hours

14 URLs Blocked



17:46

Uber Eats

Turning
a Cyber Threat into a Cyber Treat

Armour Cybersecurity

Free Treat Box

Order now! Expires 1:30PM

Scanning....

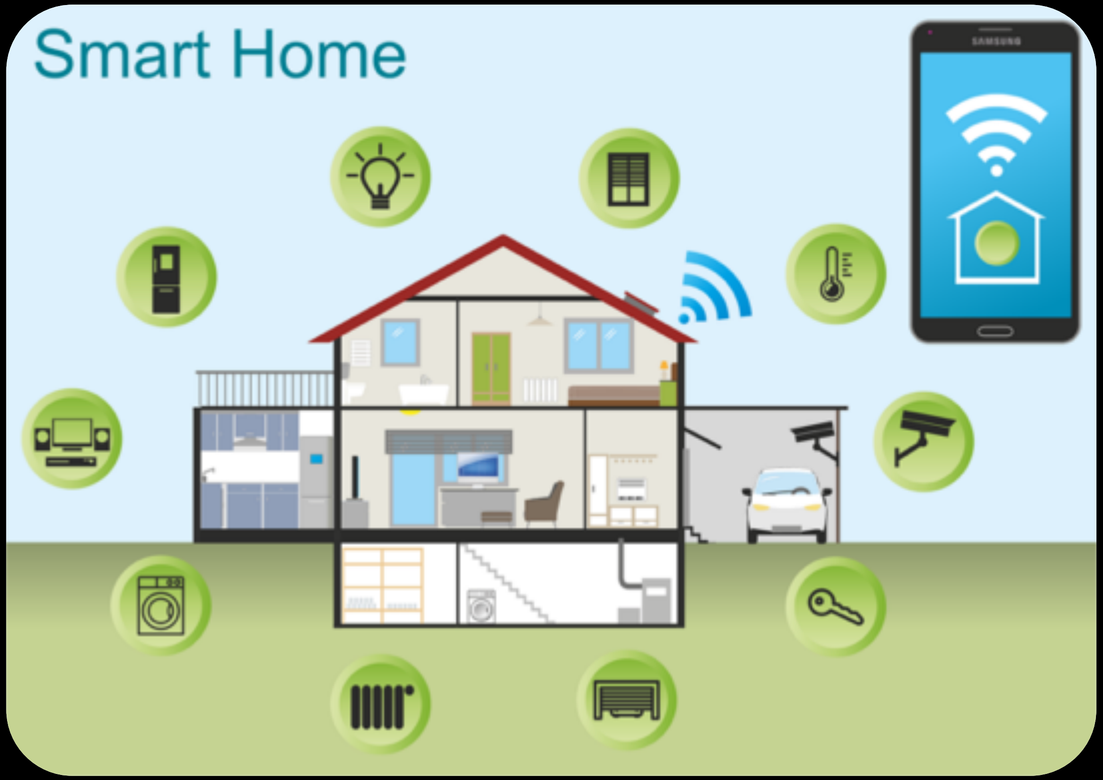
Address*

Suite # / Comments

AA armourcyber.io ×

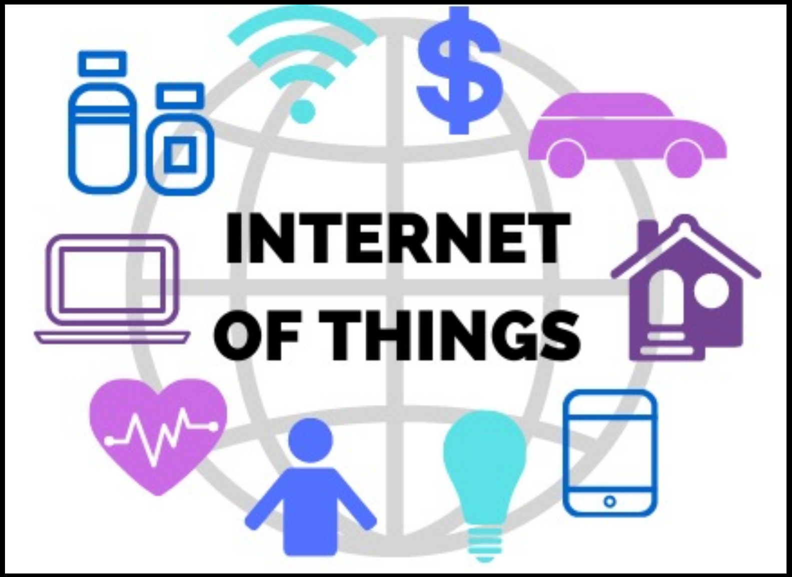
Cyber Attacks @WFH

- **Everyone** is working from home
- **Home environments** are typically insecure
- **Home automation** like Alexa and Google Home listen to all our conversations
- **Smart Devices** at more risk of being compromised
- If personal devices are compromised, it may be possible to get access to corporate data and resources



Secure Smart Devices

- Change default Passwords
- Update all software
- Do not connect the device to the internet, unless necessary
- Review privacy settings
- Choose Minimal Viable Privacy
- Turn off data and analytics sharing



Control The Under-controls

Easy To Do & Cost (almost) Nothing:

❑ **Think before you click** – don't click links or reply to suspicious emails. Check the address of the sender.

❑ Chose **passwords that are unique** and complicated. Always change **IoT default passwords**. Make it easy use a Password Generator.

❑ Set **multi factor authentication** on all key accounts.

❑ Apply all **software updates**.

❑ Have a ransomware proof **backup**. Follow 3-2-1. **Test** backup.

❑ Use the **right tools** to protect systems, communication and users.

Easy To Do & Cost (almost) Nothing:

- ❑ Use private and **protected Wi-Fi** connections.

- ❑ Assume your device listens to you 100% of the time – If you want **100% confidential meeting shut it down**. To be more specific disconnect desktop from electricity, laptop from electricity and battery.

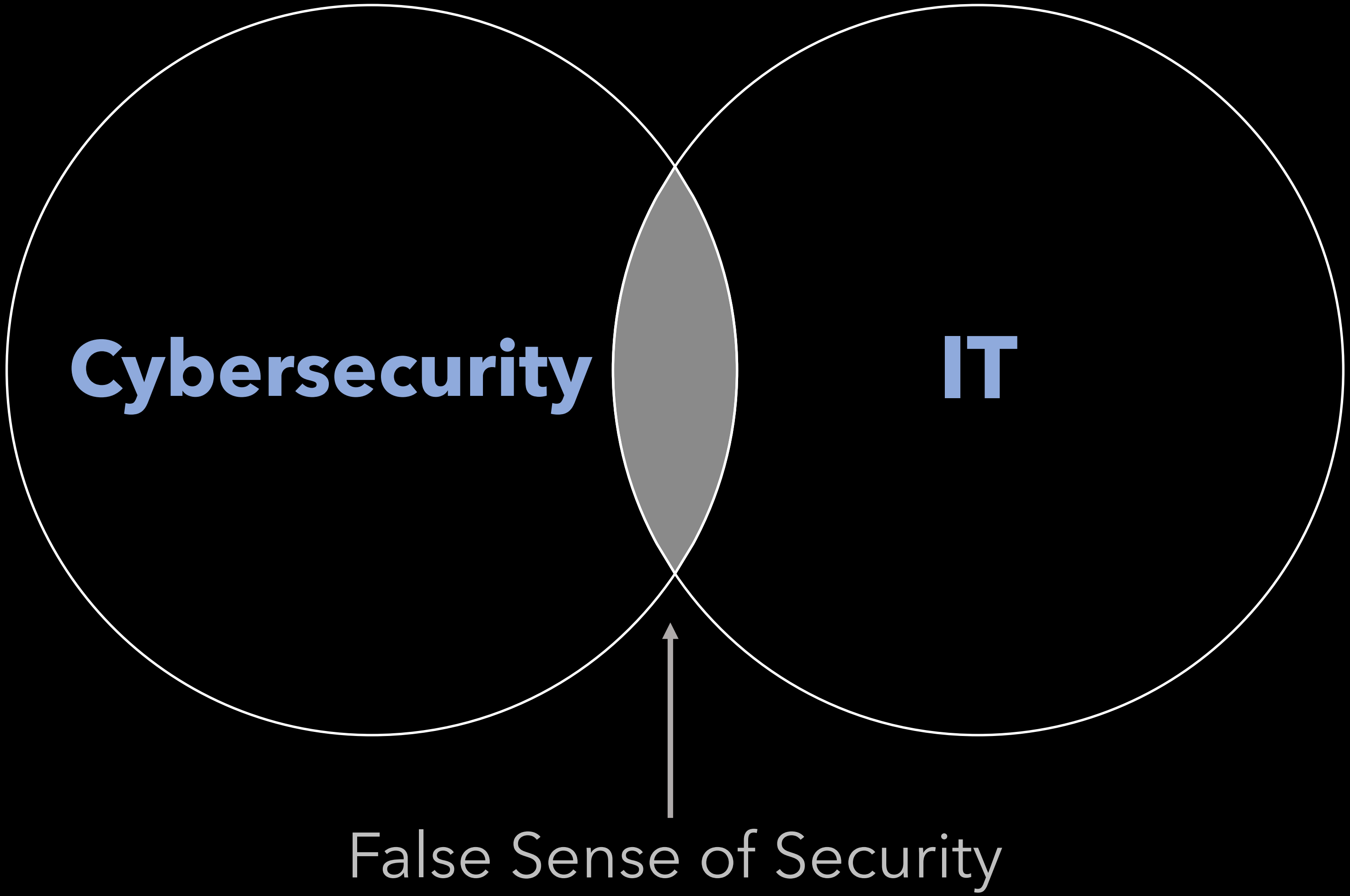
- ❑ Prevent physical access to endpoints, servers, printers, network components.

- ❑ Ensure your staff is **constantly** cyber trained. Everyone has a role to play!

- ❑ Plan for the worst – Prepare Incident Response Plan

- ❑ Take our 5 minute online self-directed assessment for actionable recommendations

Work With Experts



Q & A

For You

Was your email breached?

www.armourcyber.io/email-check

For Your Business

5 minute organization security assessment

www.armourcyber.io/self-assess

Thank You

For further details contact:

David Chernitzky
Co-Founder &CEO
Mobile: +1-(416)-702-8867
david.chernitzky@armourcyber.io

Jeffrey M. Zeiger
General Manager USA
Mobile: +1-856-308-8698
jeffrey.zeiger@armourcyber.io

ARMOUR
www.armourcyber.io