

“ABC” OF CLOUD SECURITY

Harry Pun

Deputy Chairman (Hong Kong)
Cloud Security Alliance
Hong Kong & Macau Chapter



Why do you care about
Cybersecurity?

Data breaches need to be taken seriously

Largest U.S. pipeline shuts down operations after ransomware attack

May 8, 2021



"The decision to shut down its infrastructure as a precaution after the ransomware attack was followed by the U.S. Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA) declaring a [state of emergency in 17 states and the District of Columbia](#)"

McDonald's discloses data breach after theft of customer, employee info

Jun 11, 2021



"While we were able to close off access quickly after identification, our investigation has determined that a small number of files were accessed, some of which [contained personal data including Korea and Taiwan customer data](#)"

Audi, Volkswagen data breach affects 3.3 million customers

Jun 12, 2021



"The data also included more sensitive information relating to eligibility for a purchase, loan, or lease. [More than 95% of the sensitive data](#) included was driver's license numbers. "

Source: Bleepingcomputer.com

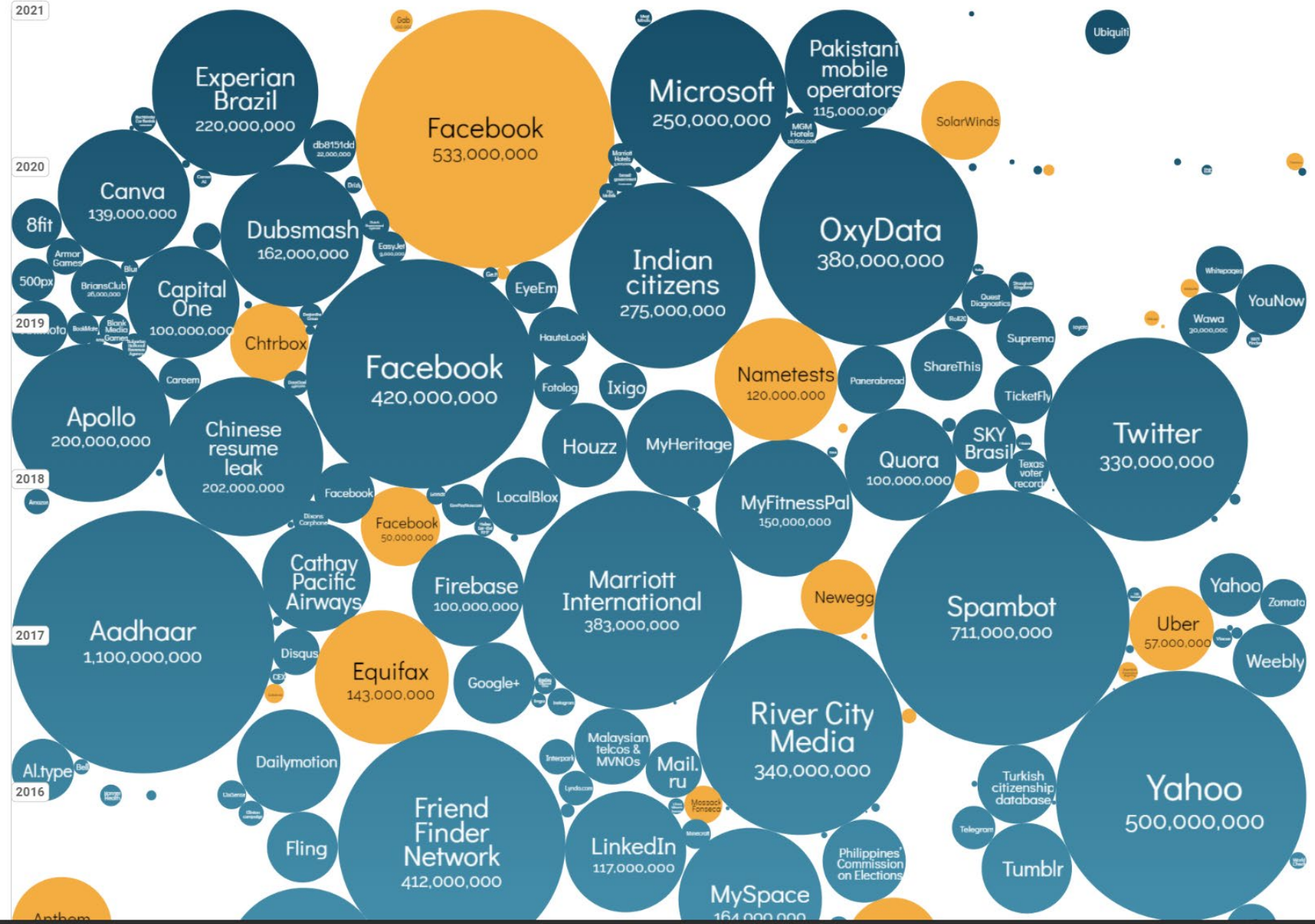
© 2016 Cloud Security Alliance, APAC. All rights reserved.

CSA APAC cloud security
ASIA PACIFIC REGION alliance*

interesting story

UPDATED: Apr 2021

2021



HACKING SERVICES & ATTACKS

IDENTITY SERVICES

SER	DESCRIPTION OF ITEM(S)	USD	NUMBER OF CARDS
PASSPORT		\$120 - \$135	1
ID CARD	COUNTRY-SPECIFIC CREDIT / DEBIT CARDS – BALANCES RANGE FROM \$2,500-\$3,500	\$200 - \$210	2
		\$350	5
DRIVERS LICENSE		\$700	10
		\$1,250	20
PERMANENT RESIDENCE		\$250	1
START A NEW LIFE IN A NEW COUNTRY		\$450	2
ID, PASSPORT, DRIVERS LICENSE	HIGH BALANCE AMEX CARDS – BALANCES RANGE FROM \$6,000 - \$9,000	\$1,950	10
REGISTRATION		\$3,700	20
		\$112	1
	PRELOADED CREDIT / DEBIT CARDS (MAGNETIC STRIP ONLY) – BALANCES RANGE FROM \$2,000 - \$2,400	\$438	5
		\$782	10
		\$2,198	40
		\$145	1
	PRELOADED CREDIT / DEBIT CARDS (EMV / CHIP) – BALANCES RANGE FROM \$2,000 - \$2,400	\$569	5
		\$1,025	10
		\$3,125	40

Ref: <https://www.>

Threat Landscape

Growing number of **cyberattacks**

- **90 %** begin with a phishing email
- **74%** of the world's businesses expect to be hacked this year
- **\$400B** annual cost of cybercrime to global economy
- **4% of annual revenue** max fine for failure to comply with GDPR
- Entry of more **Nation-State attacks**



Phishing and business email compromise



Detections in
the past year:

6T

Messages
scanned

~13B

Malicious emails
blocked

~1.6B

URL-based email
phishing threats
blocked

~1.7-2B

URL payloads being created
each month, orchestrated
through thousands of
phishing campaigns

We're seeing 3 main types of phishing:

Credential phishing

Business email compromise

Combination

Top 5 spoofed brands:

Microsoft
UPS
Amazon
Apple
Zoom

Phishing campaigns: Top 10 targeted industries:

Accounting & Consulting	Healthcare
Wholesale Distribution	Chemicals
IT Services	High Tech & Electronics
Real Estate	Legal Services
Education	Outsourced Services

Up until a few years ago, cybercriminals focused their efforts on malware attacks for greatest ROI.

More recently, they've shifted their focus to phishing attacks with the goal of harvesting user credentials.

COVID- Related Phishing Campaigns

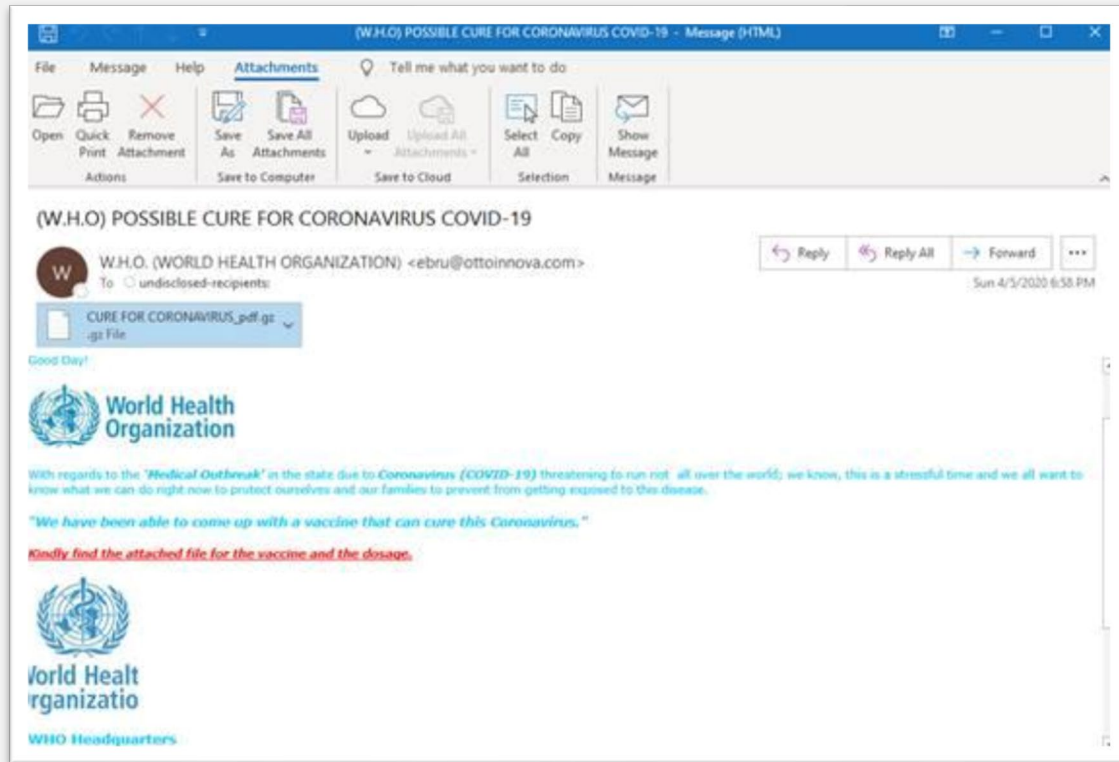


Figure 1: Spoofing WHO branding with “cure” and “vaccine” messaging

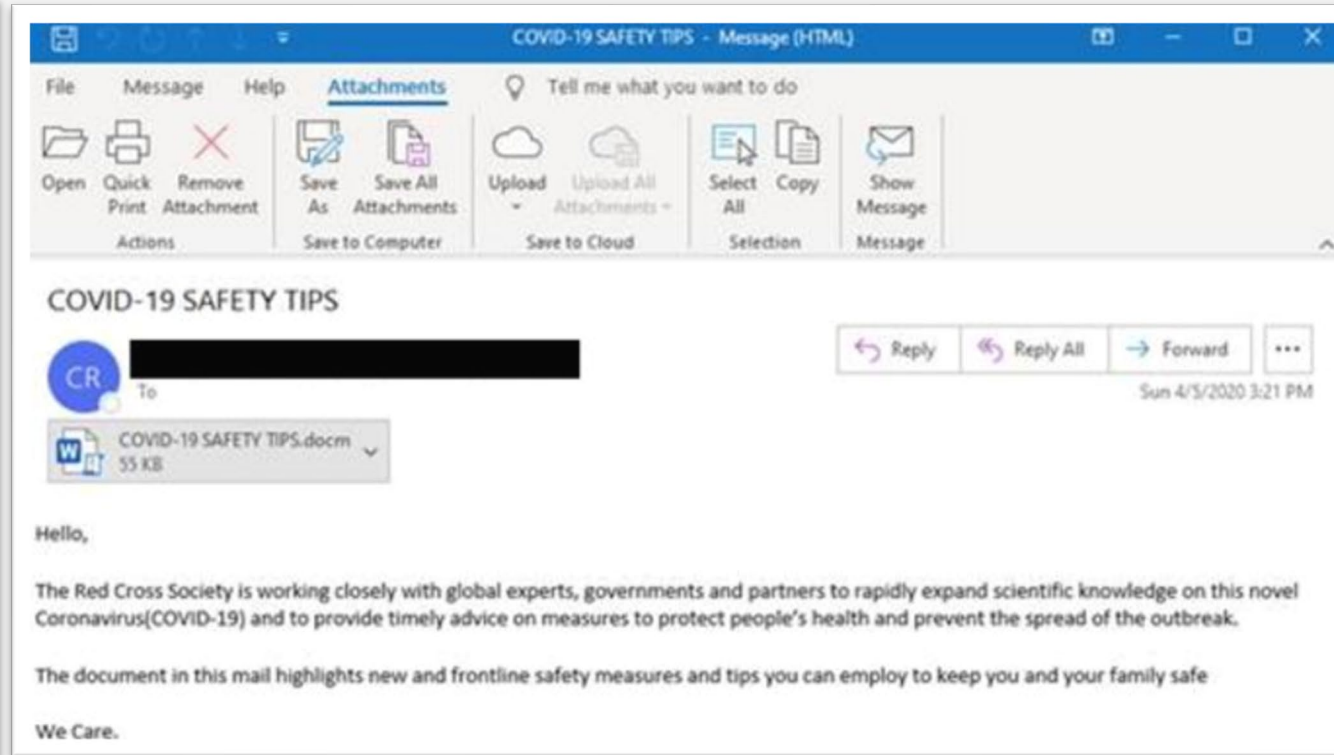


Figure 2: Spoofing Red Cross Safety Tips with malicious .docm file

COVID- Related Phishing Campaigns

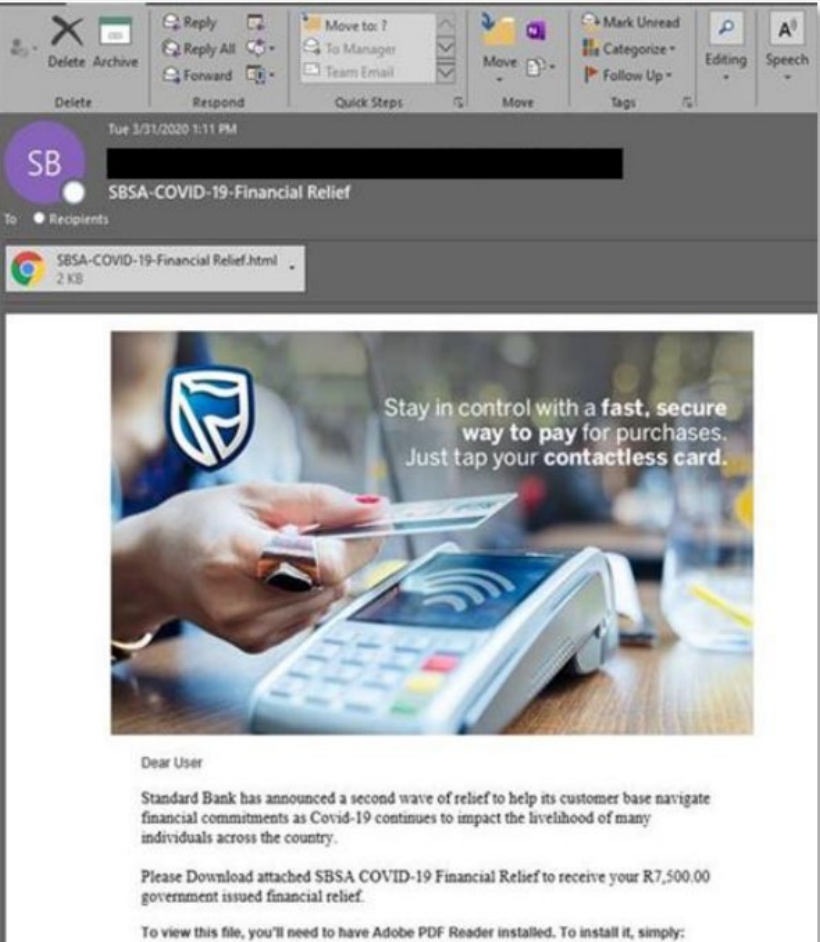


Figure 3: South African banking lure promoting COVID-19 financial relief with malicious .html files

Source: Microsoft Special Report on COVID-19 Threat Intelligence

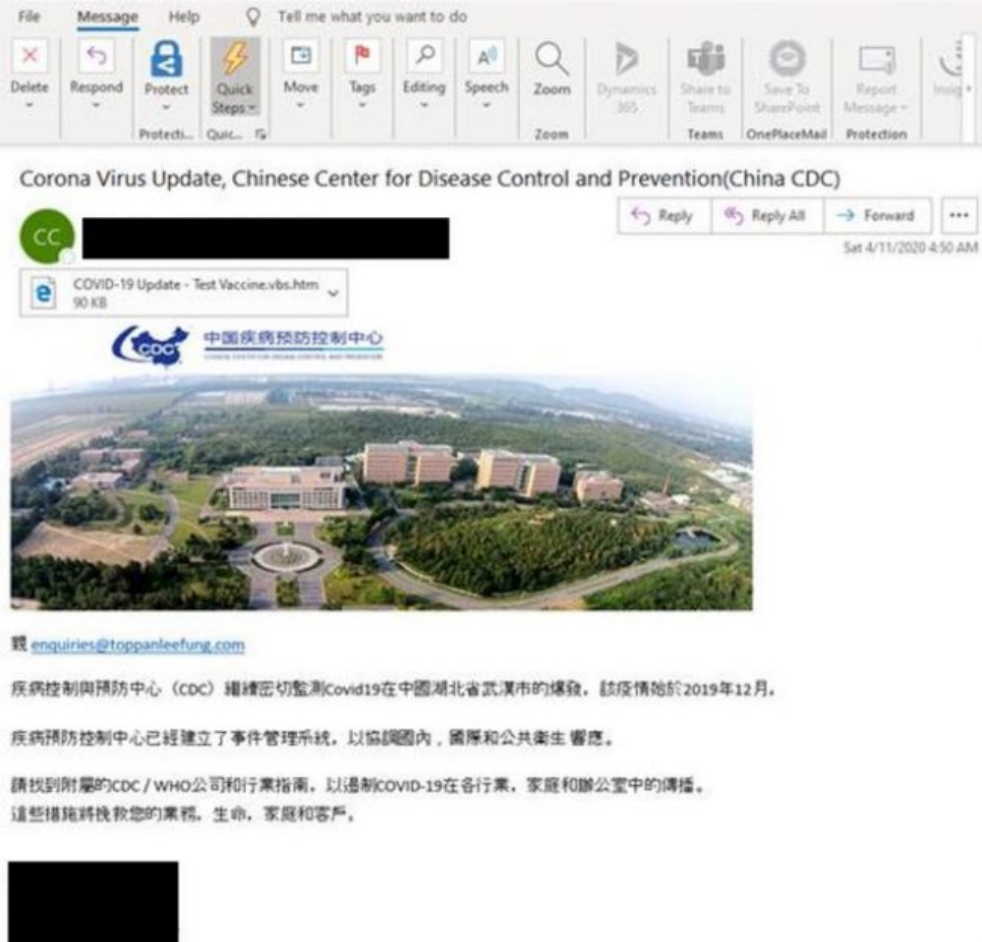


Figure 5: Spoofing China CDC and virus updates with malicious .htm file

Beyond Phishing

Top Observations



Vulnerable
Internet-facing
network devices



Brute forcing RDP
servers

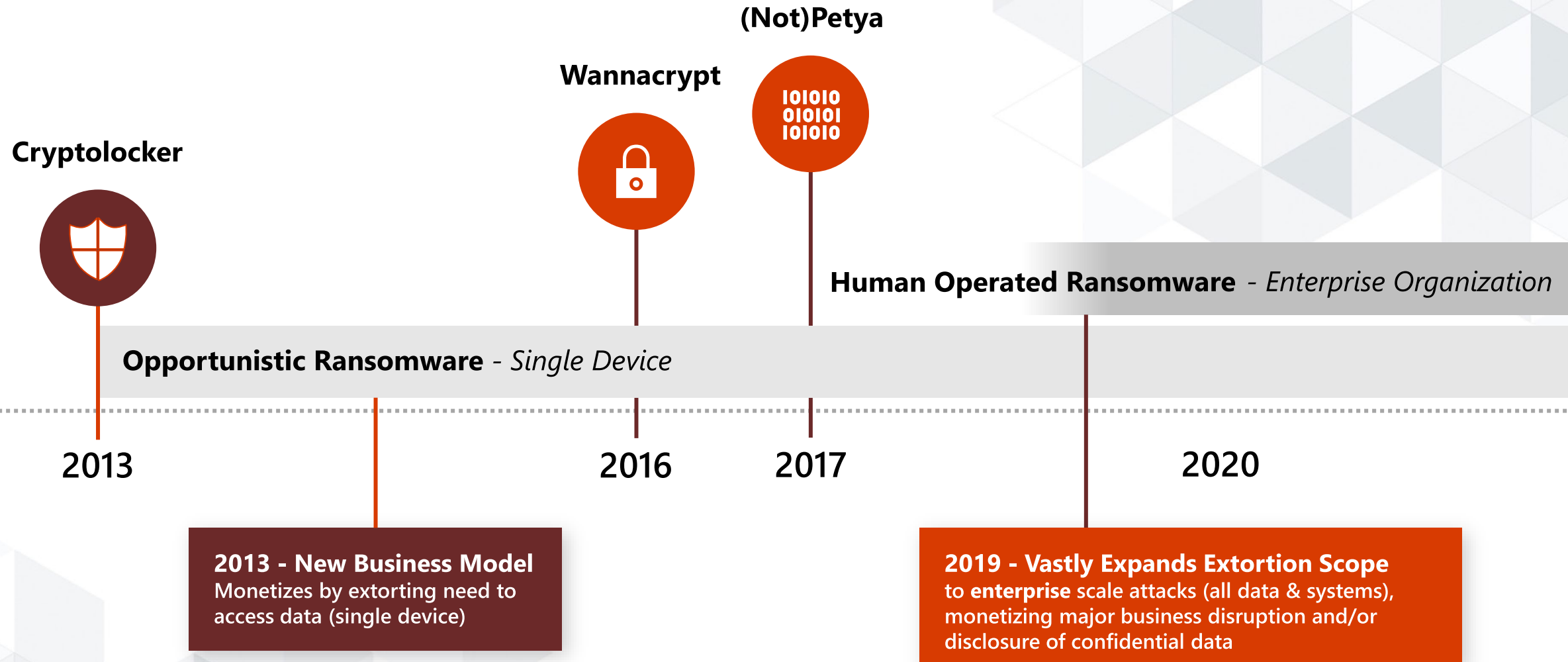


Credential theft
and lateral
movement
(Mimikatz, Cobalt
Strike)

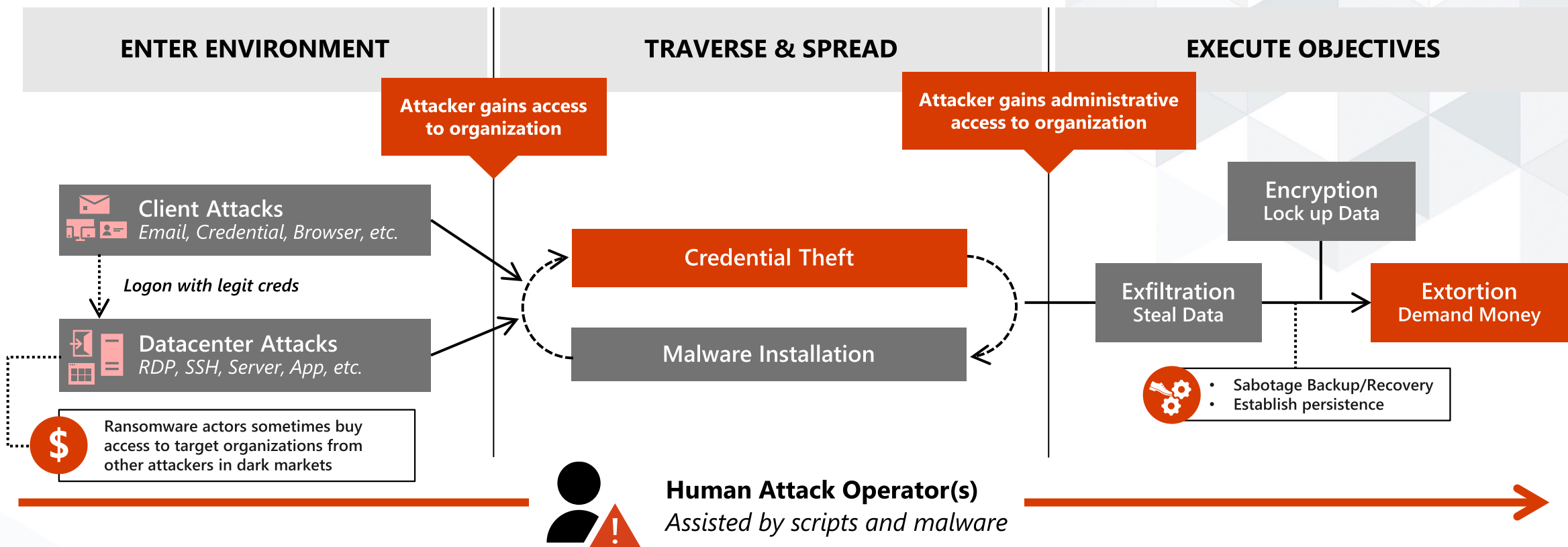


Wide range of
ransomware
payloads

Evolution of ransomware models



Pattern – Human Operated Ransomware



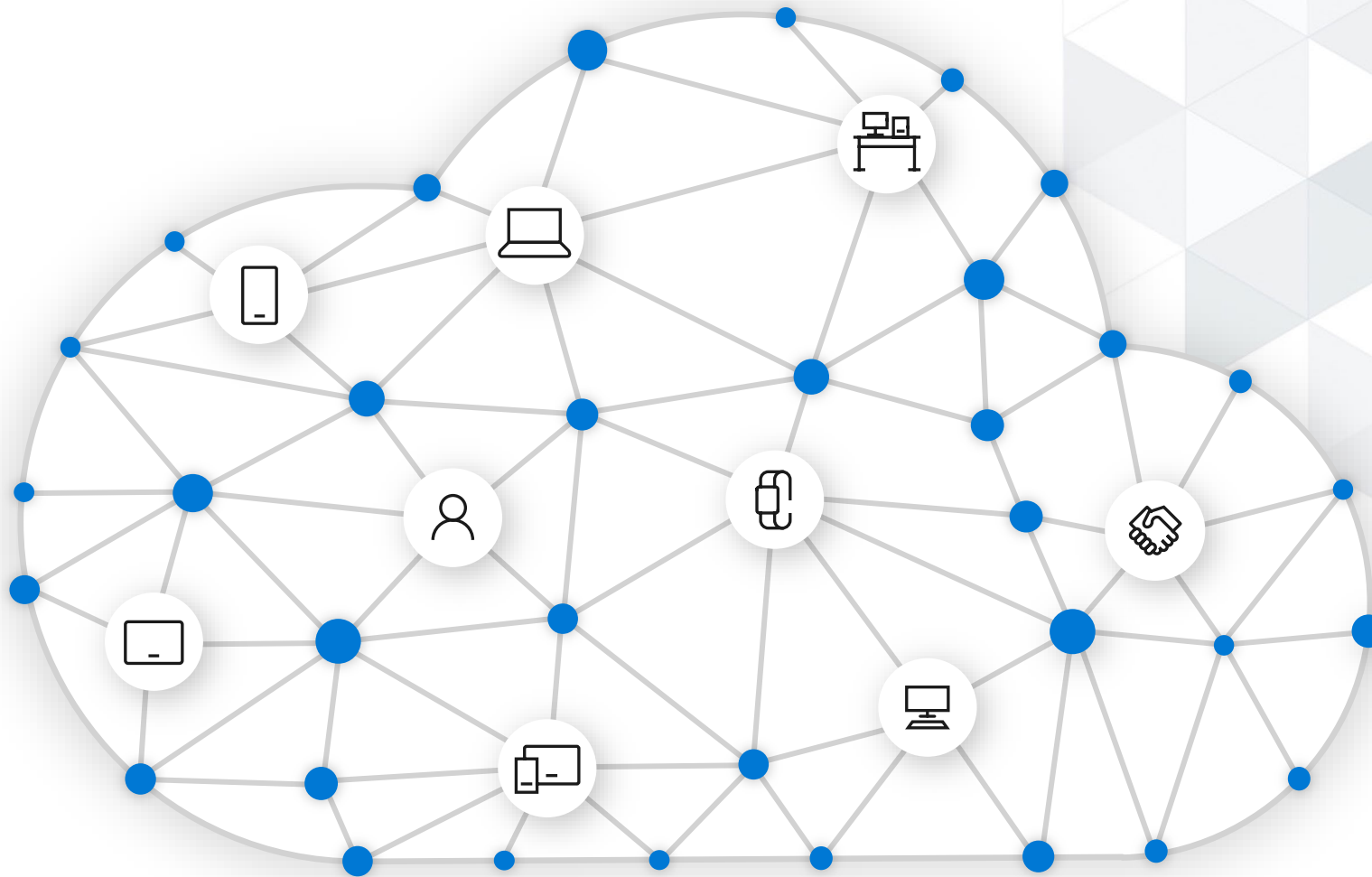
Ryuk example (Email)



Wadhrama example (RDP)



Comparison to traditional ransomware

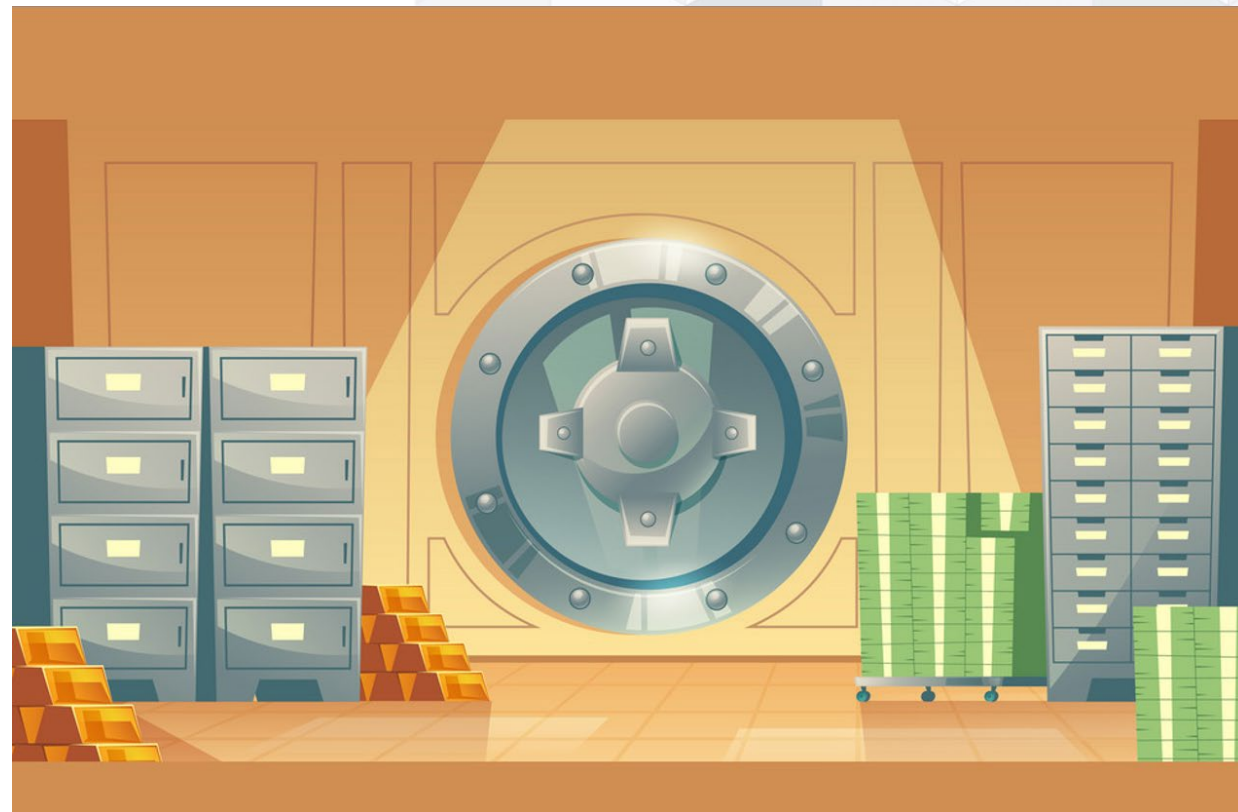


“The future of cybersecurity...is in the cloud.”¹

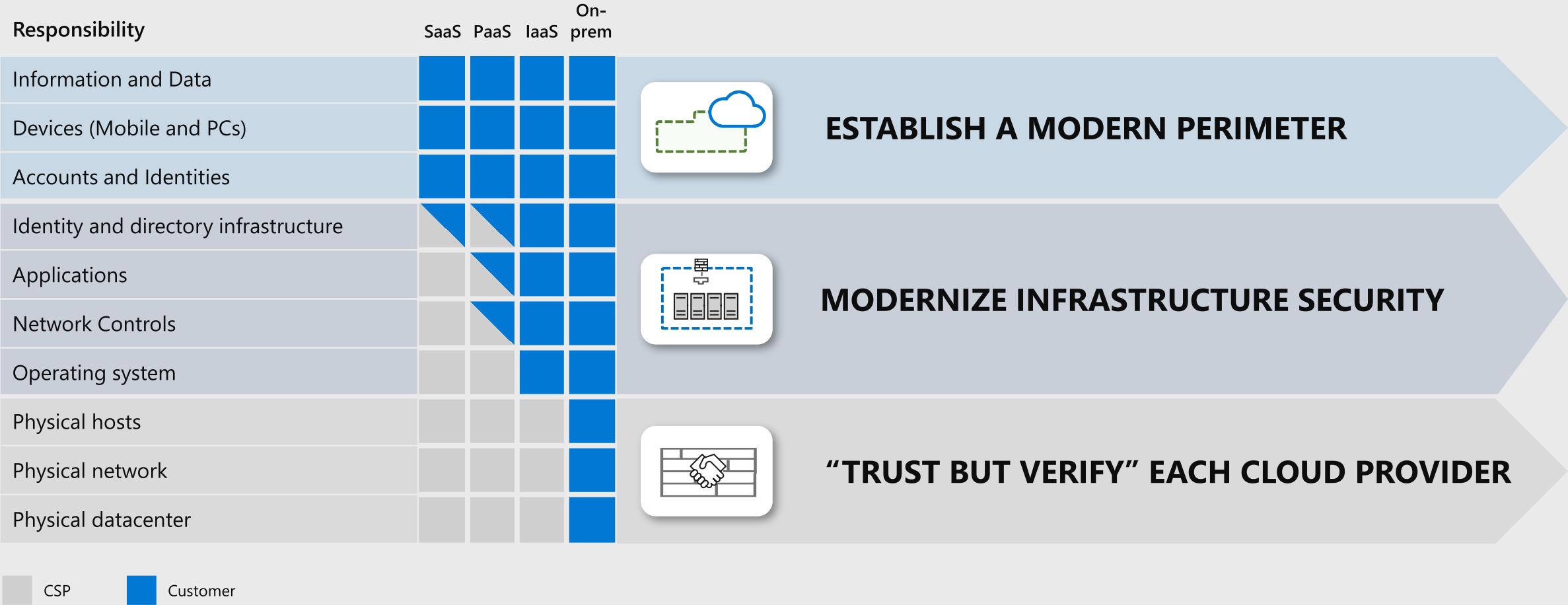
¹ <https://go.forrester.com/blogs/tech-titans-google-and-microsoft-are-transforming-cybersecurity/>



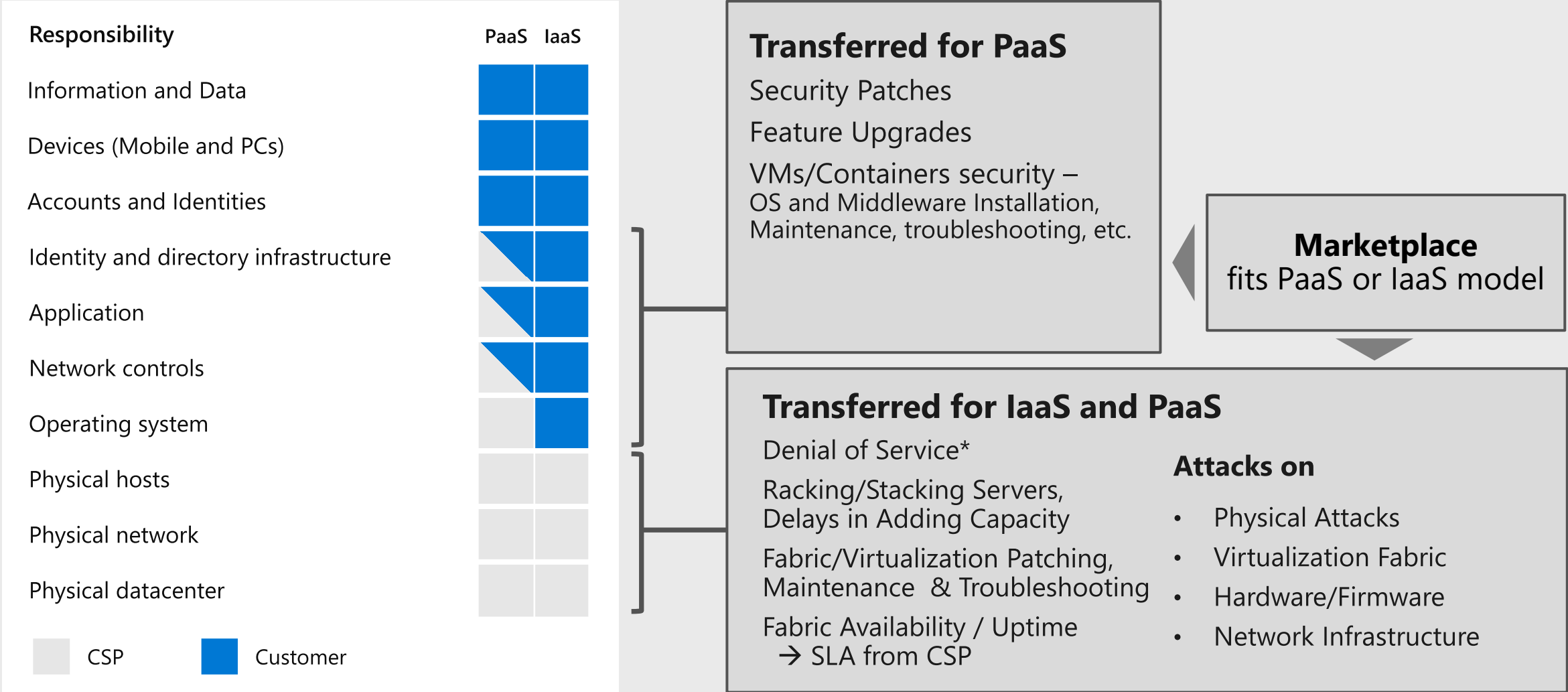
VS



Shared Responsibility Model and Key Strategies



Security Responsibilities Transfer to Cloud



What Is CCM?

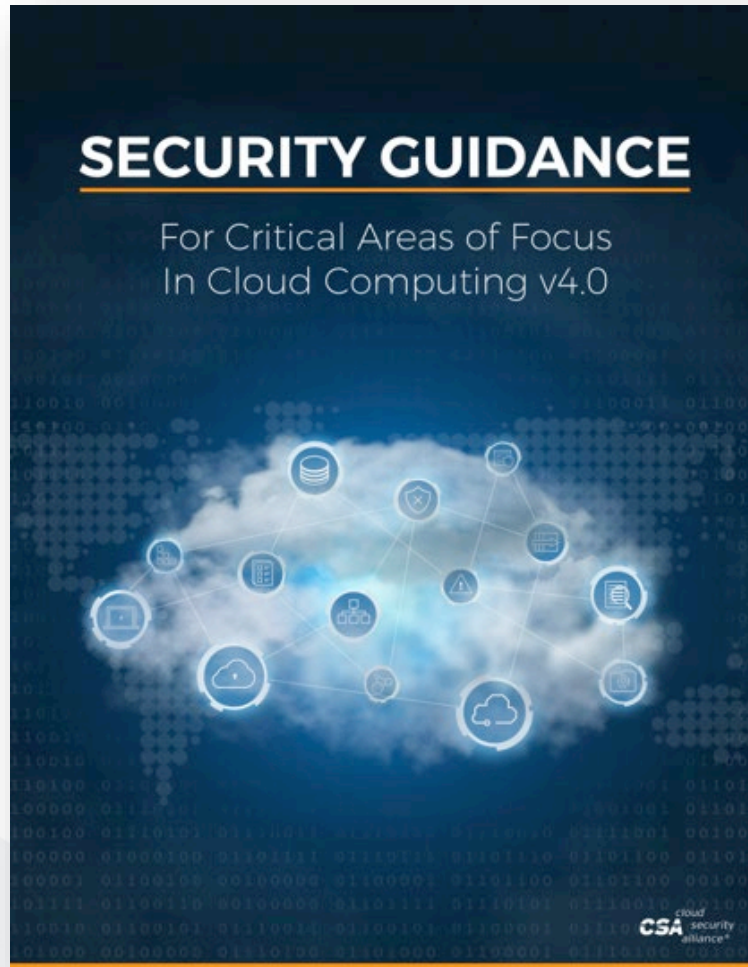
- **First ever baseline control framework specifically designed for cloud supply chain risk management**
- Delineates control ownership (provider, customer)
- An anchor for security & compliance posture measurement
- Provides a framework of 17 control domains
- Controls map to global regulations & security standards
- **Industry driven effort: 120+ peer review participants**
- **Participants: AICPA, Microsoft, McKesson, ISACA, oracle**
- **Backbone of open certification framework & STAR**



A&A	Audit and Assurance	IAM	Identity & Access Management
AIS	Application & Interface Security	IPY	Interoperability & Portability
BCR	Business Continuity Mgmt & Op Resilience	IVS	Infrastructure & Virtualization Security
CCC	Change Control and Configuration Management	LOG	Logging and Monitoring
CEK	Cryptography, Encryption and Key Management	SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
DCS	Datacenter Security	STA	Supply Chain Mgmt, Transparency & Accountability
DSP	Data Security and Privacy	TVM	Threat & Vulnerability Management
GRC	Governance, Risk Management and Compliance	UEM	Universal EndPoint Management
HRS	Human Resources Security		

17 Control Domains Over 130+ Controls

CSA Security Guidance v4.0



- Fundamental cloud security research that started CSA
- Foundation for certificate of cloud security knowledge (CCSK)
- 4th version, released July 2017
- Architecture
- Governing in the cloud
 - Governance and enterprise risk management
 - Legal
 - Compliance & audit management
 - Information governance
- Operating in the cloud
 - Management plane & business continuity
 - Infrastructure security
 - Virtualization & containers
 - Incident response
 - Application security
 - Data security & encryption
 - Identity management
 - Security as a service
 - Related technologies

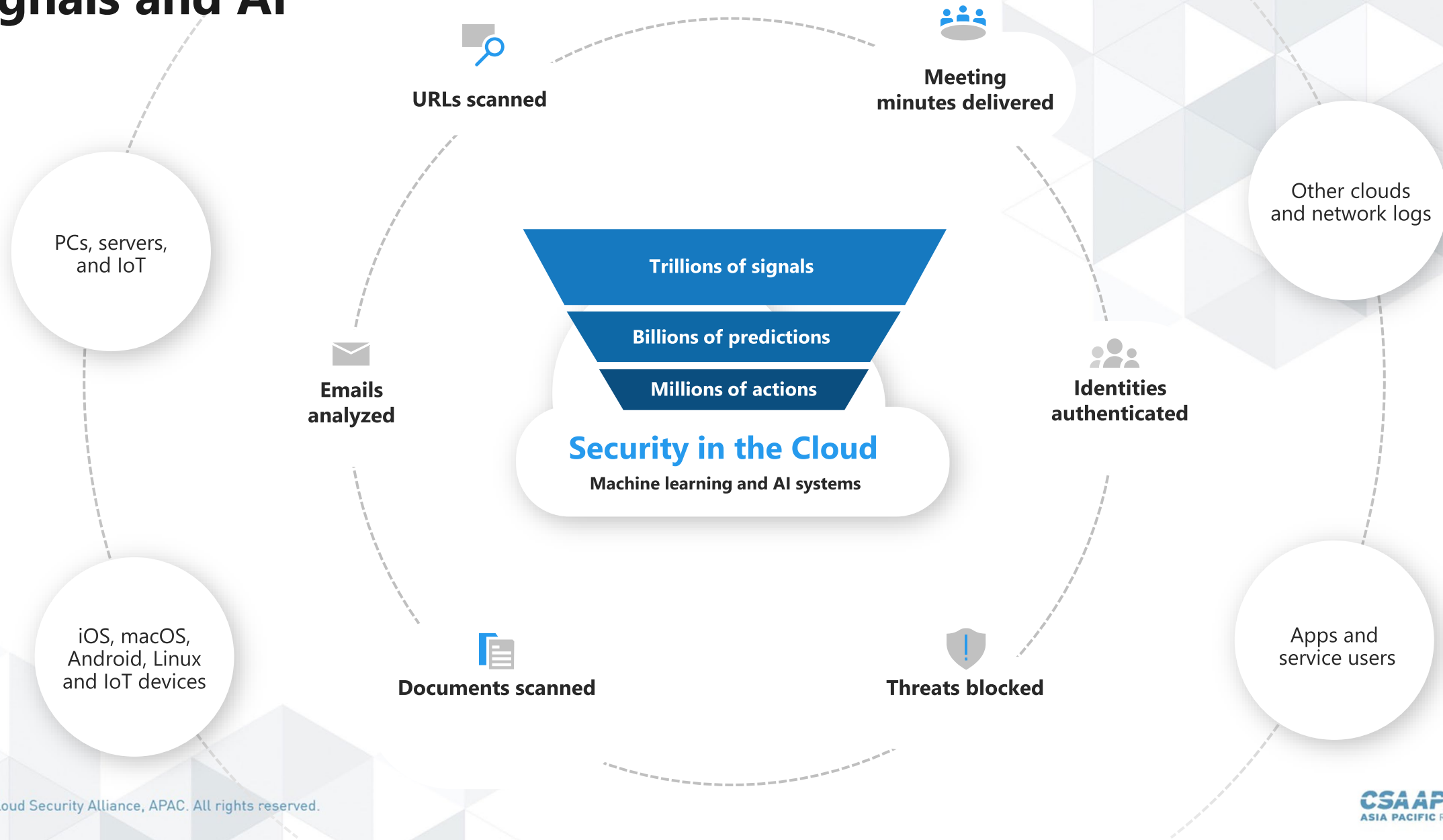
CSA STAR: Security, Trust & Assurance Registry



Launched in 2011, the CSA STAR is the first step improving transparency and assurance in the cloud.

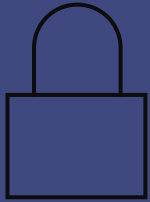
- Searchable registry to allow cloud customers to review the security practices of providers, accelerating their due diligence and leading to **higher quality procurement experiences**
- STAR is a **publicly accessible** registry that documents the security controls provided by cloud computing offerings
- Helps users to assess the security of cloud providers
- It is based on a multi-layered structure defined by **Open Certification Framework working group**

Signals and AI



Always verify
Believe nobody
Check everything

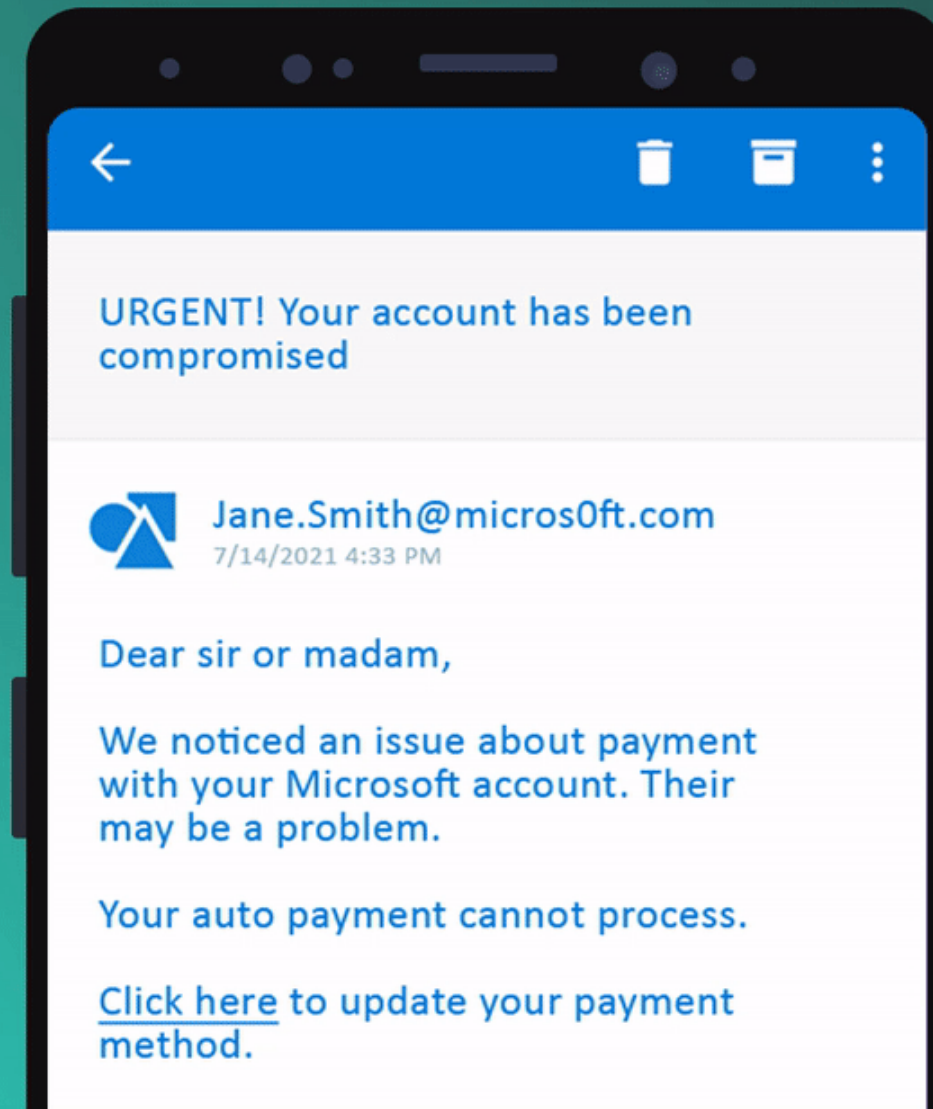




Some phishing stories



Can you spot the phishy email clues?



Pause, Think ...

Account Notification !

Inbox

Team Support Service@account.com via [redacted] hostgator.com
to me

7:45 AM (15 hours ago)



Your Account PayPal is Limited, You Have To Solve The Problem In 24 Hours.

Hello PayPal Customer,

We are sorry to inform you that you can't access all your paypal advantages like sending money and purchasing, due to account limitation.

Why my account PayPal™ is limited?

Because we think that your account is in danger from stealing and unauthorized uses.

What can I do to resolve the problem?

You have to confirm all your account details on our secure server by clicking the link below and following all the steps.

[Confirm Your Information](#)



Apple Help <noreply-apple-notifcation@dramamission.com>

Vanessa Huang

Re : [Confirmation] Thanks For Your Purchase Rock Apps Case Id [892317698]



Subscription Confirmation

Dear User,

This email confirms your order of the following subscription with a free trial of 7 days. You are not charged for the free trial period, but when your 1 month subscription automatically renews on 11 November 2018 you will be charged USD 194\$ for the period.

Name of Subscription: **Premium Membership**

Running for Weight Loss: interval training plan, GPS, how-to-

lose-weight tips by Red Rock Apps

Name of Application: **Grinasys Corp.**

Content Provider: **Grinasys Corp.**

Date of purchase: **11/11/2018**

Subscription Period: **1 month**

Length of Trial: **7 days**

Price: **USD 194\$**

Payment Method: **iTunes account**

<="">

[Cancel My Subscription](#)

The subscription period will automatically renew unless you turn it off no later than 24 hours before the end of the current period. To cancel automatic renewal or manage your subscriptions, click below and sign in.

Developer's Support Page or Terms of Use:

[MZSubscriptionEmail.Welcome.PublisherSupportOrTerms.supportUrl]<http://www.apple.com/uk/support>

[View Account Information](#)

Sincerely,
Apple

(Source: [CSO Online](#))

...and Verify

Account Notification !

Inbox

Team Support Service@account.com via [redacted] hostgator.com
to me

7:45 AM (15 hours ago)



Your Account PayPal is Limited, You Have To Solve The Problem In 24 Hours.

Hello PayPal Customer,

We are sorry to inform you that you can't access all your paypal advantages like sending money and purchasing, due to account limitation.

Why my account PayPal™ is limited?

Because we think that your account is in danger from stealing and unauthorized uses

What can I do to resolve the problem?

You have to confirm all your account details on our secure server by clicking the link below and following the steps

Confirm Your Information

Hover first!
Don't click it!

<https://www.woodgrovebank.com/loginscript/user2.jsp>

<http://192.0.2.1/wood/index.htm>



Apple Help <noreply-apple-notifcation@dramamission.com>

Vanessa Huang

Re : [Confirmation] Thanks For Your Purchase Rock Apps Case Id [892317698]



Subscription Confirmation

Dear User,

This email confirms your order of the following subscription with a free trial of 7 days. You are not charged for the free trial period, but when your 1 month subscription automatically renews on 11 November 2018 you will be charged USD 194\$ for the period.

Name of Subscription: **Premium Membership**

Running for Weight Loss: interval training plan, GPS, how-to-

lose-weight tips by Red Rock Apps

Name of Application: **Grinasys Corp.**

Content Provider: **Grinasys Corp.**

Date of purchase: **11/11/2018**

Subscription Period: **1 month**

Length of Trial: **7 days**

Price: **USD 194\$**

Payment Method: **iTunes account**

<="">

[Cancel My Subscription](#)

The subscription period will automatically renew unless you turn it off no later than 24 hours before the end of the current period. To cancel automatic renewal or manage your subscriptions, click below and sign in.

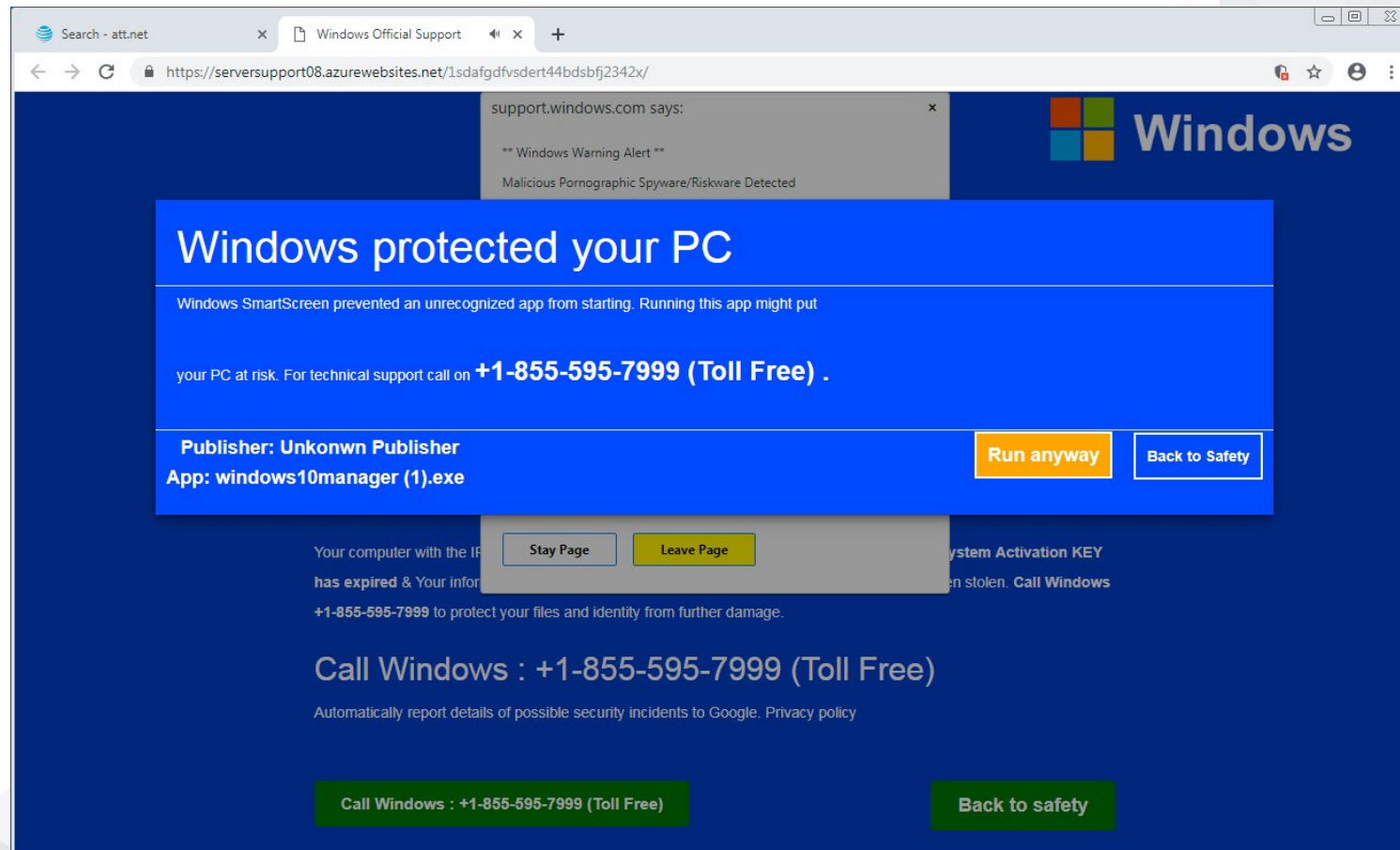
Developer's Support Page or Terms of Use:

[M2SubscriptionEmail.Welcome.PublisherSupportOrTerms.supportUrl]<http://www.apple.com/uk/support>

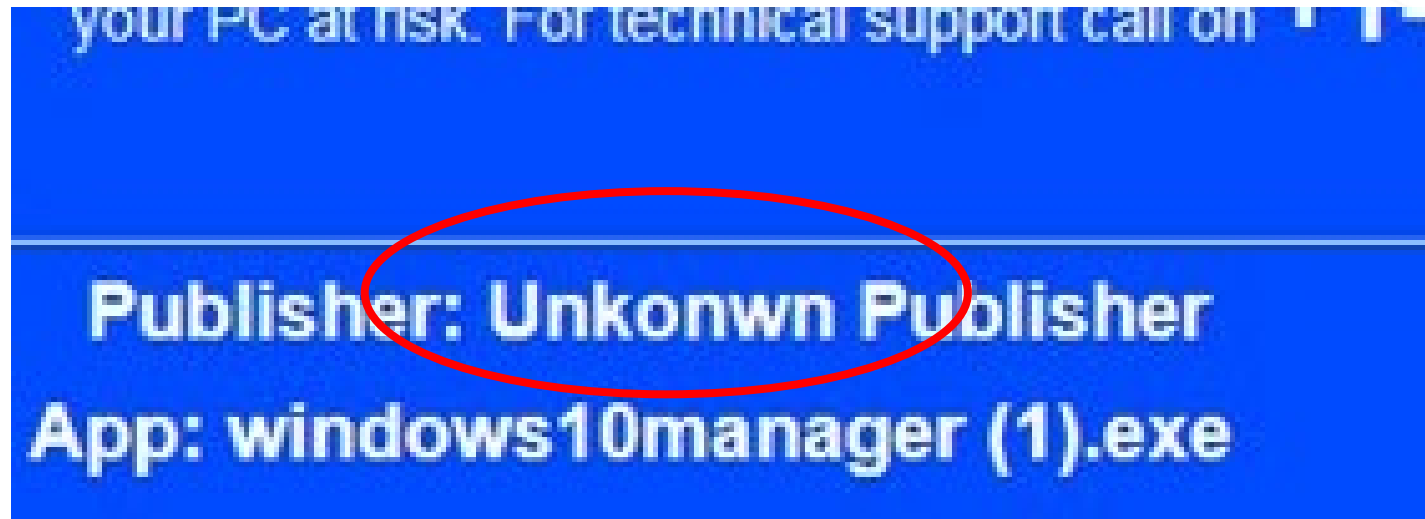
[View Account Information](#)

Sincerely,
Apple

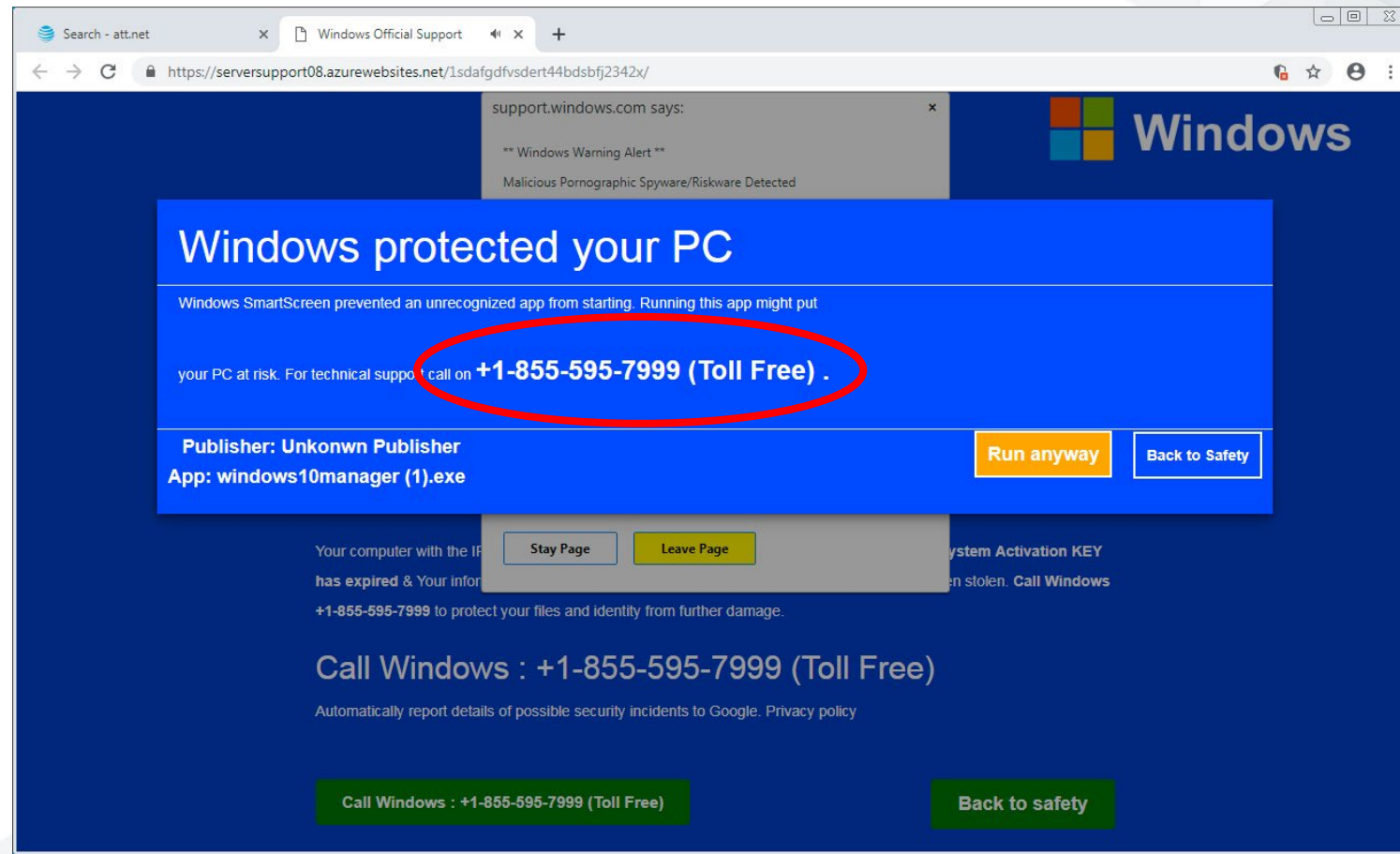
Popups



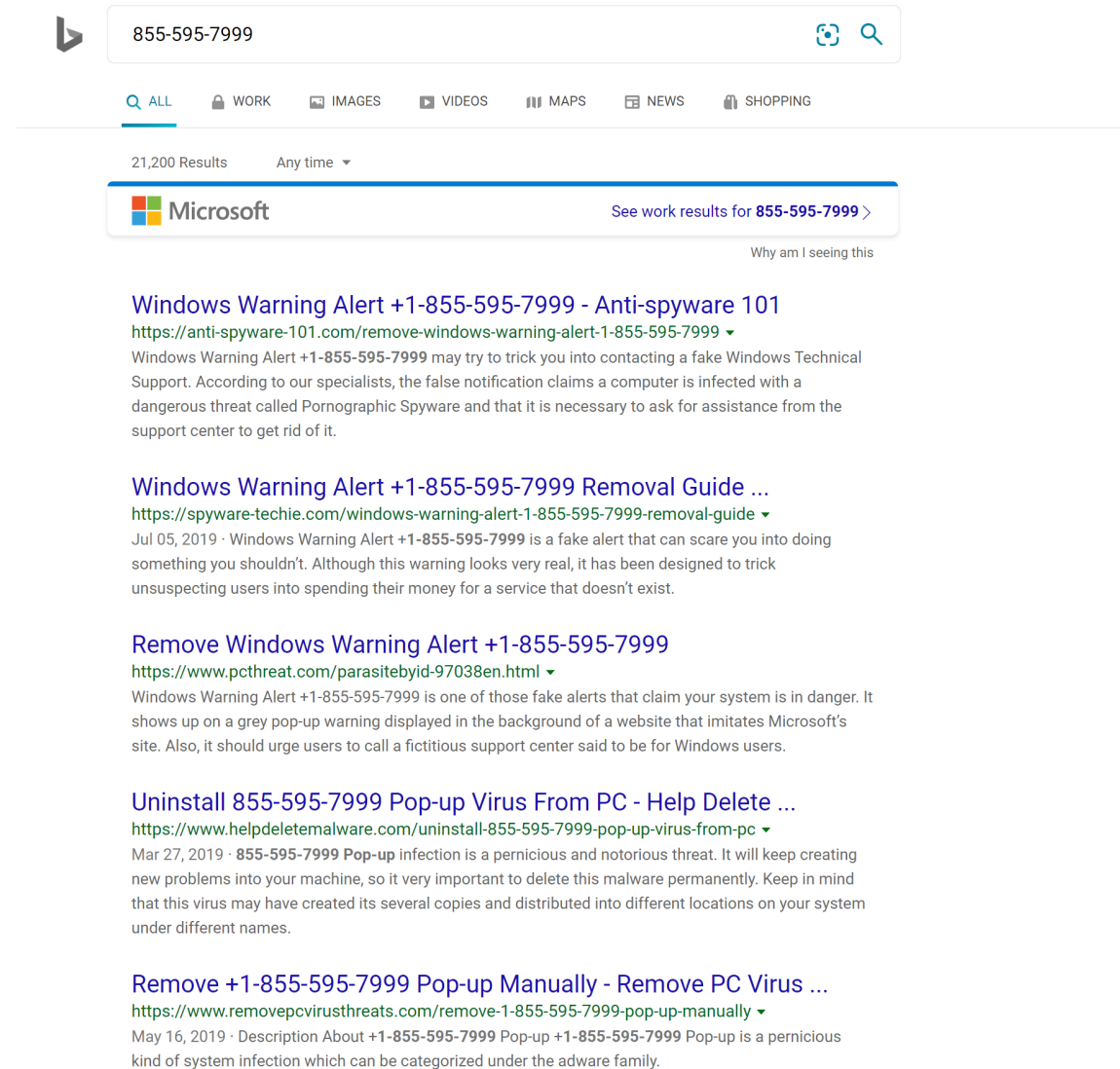
Popups



Popups



When in doubt...search



The screenshot shows a search engine interface with a search bar containing the text "855-595-7999". Below the search bar, there are tabs for "ALL", "WORK", "IMAGES", "VIDEOS", "MAPS", "NEWS", and "SHOPPING". The search results are displayed below the tabs, showing 21,200 results. The first result is titled "Windows Warning Alert +1-855-595-7999 - Anti-spyware 101" and includes a URL: <https://anti-spyware-101.com/remove-windows-warning-alert-1-855-595-7999>. The second result is titled "Windows Warning Alert +1-855-595-7999 Removal Guide ..." and includes a URL: <https://spyware-techie.com/windows-warning-alert-1-855-595-7999-removal-guide>. The third result is titled "Remove Windows Warning Alert +1-855-595-7999" and includes a URL: <https://www.pcthreat.com/parasitebyid-97038en.html>. The fourth result is titled "Uninstall 855-595-7999 Pop-up Virus From PC - Help Delete ..." and includes a URL: <https://www.helpdeletemalware.com/uninstall-855-595-7999-pop-up-virus-from-pc>. The fifth result is titled "Remove +1-855-595-7999 Pop-up Manually - Remove PC Virus ..." and includes a URL: <https://www.removepcvirusthreats.com/remove-1-855-595-7999-pop-up-manually>.

855-595-7999

Q ALL WORK IMAGES VIDEOS MAPS NEWS SHOPPING

21,200 Results Any time ▾

Microsoft See work results for 855-595-7999 >

Why am I seeing this

Windows Warning Alert +1-855-595-7999 - Anti-spyware 101
<https://anti-spyware-101.com/remove-windows-warning-alert-1-855-595-7999> ▾
Windows Warning Alert +1-855-595-7999 may try to trick you into contacting a fake Windows Technical Support. According to our specialists, the false notification claims a computer is infected with a dangerous threat called Pornographic Spyware and that it is necessary to ask for assistance from the support center to get rid of it.

Windows Warning Alert +1-855-595-7999 Removal Guide ...
<https://spyware-techie.com/windows-warning-alert-1-855-595-7999-removal-guide> ▾
Jul 05, 2019 · Windows Warning Alert +1-855-595-7999 is a fake alert that can scare you into doing something you shouldn't. Although this warning looks very real, it has been designed to trick unsuspecting users into spending their money for a service that doesn't exist.

Remove Windows Warning Alert +1-855-595-7999
<https://www.pcthreat.com/parasitebyid-97038en.html> ▾
Windows Warning Alert +1-855-595-7999 is one of those fake alerts that claim your system is in danger. It shows up on a grey pop-up warning displayed in the background of a website that imitates Microsoft's site. Also, it should urge users to call a fictitious support center said to be for Windows users.

Uninstall 855-595-7999 Pop-up Virus From PC - Help Delete ...
<https://www.helpdeletemalware.com/uninstall-855-595-7999-pop-up-virus-from-pc> ▾
Mar 27, 2019 · **855-595-7999 Pop-up** infection is a pernicious and notorious threat. It will keep creating new problems into your machine, so it very important to delete this malware permanently. Keep in mind that this virus may have created its several copies and distributed into different locations on your system under different names.

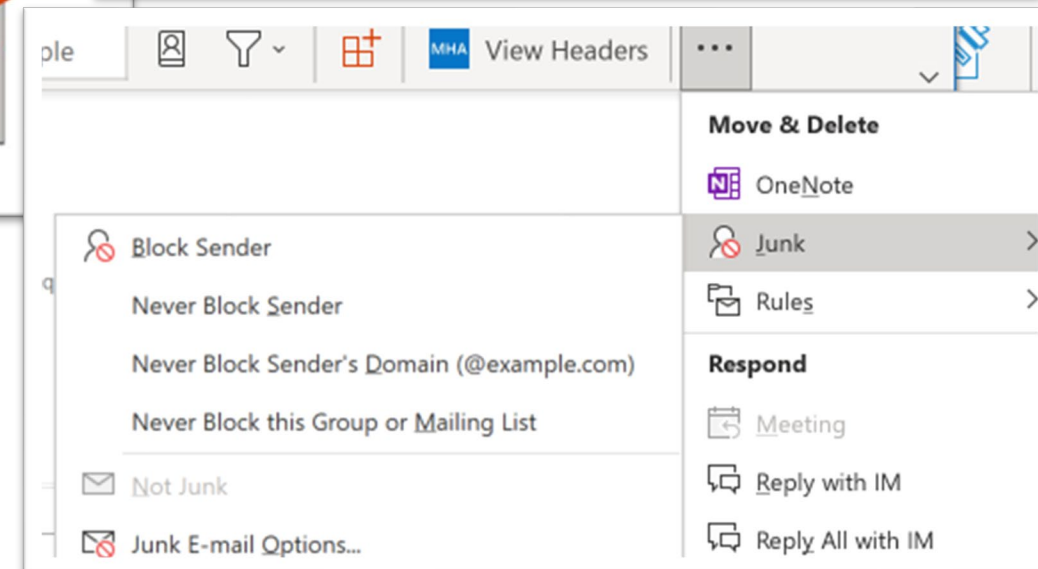
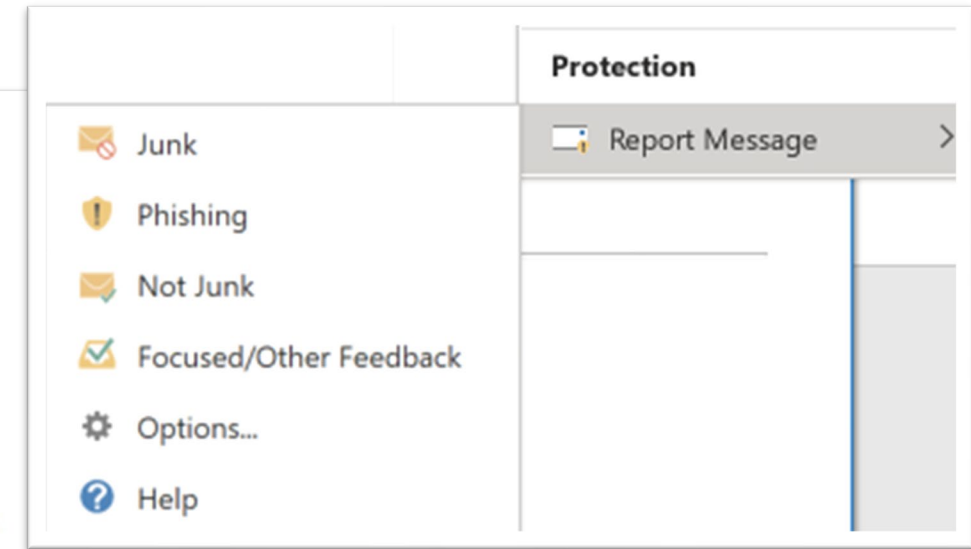
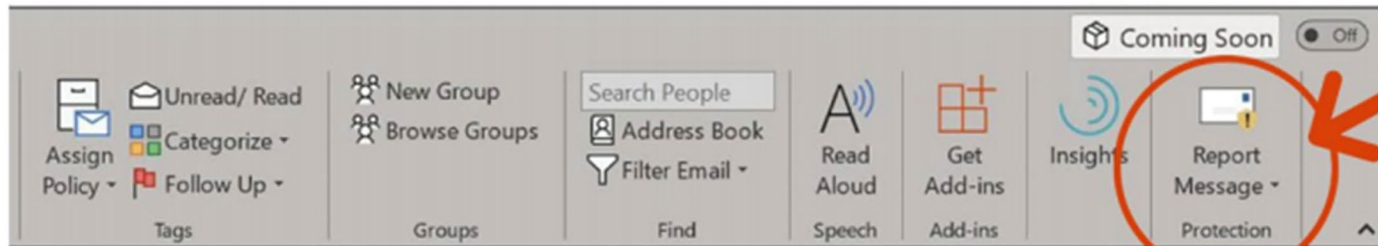
Remove +1-855-595-7999 Pop-up Manually - Remove PC Virus ...
<https://www.removepcvirusthreats.com/remove-1-855-595-7999-pop-up-manually> ▾
May 16, 2019 · Description About +1-855-595-7999 Pop-up +1-855-595-7999 Pop-up is a pernicious kind of system infection which can be categorized under the adware family.

What can you do about phishing?

If you see something, say something

Anytime you think you have received a phish, immediately report it, even if you didn't interact with the mail or respond.

You can use the **Report Message** button on the **Home** tab to report phishing emails quickly.





Password is like your
home key





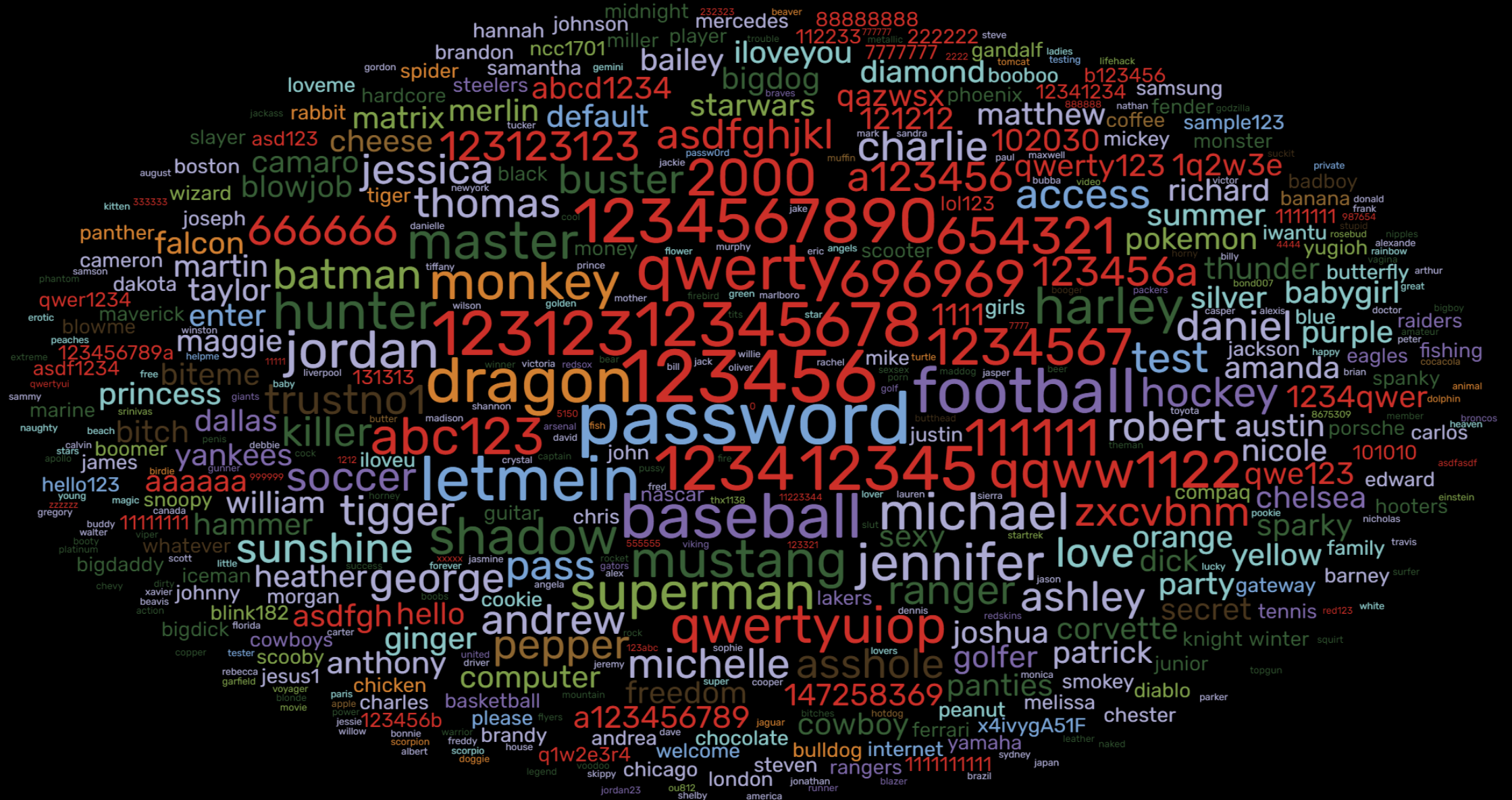
帳戶跟個人資料和家門鑰匙一樣重要

Most Common Passwords

Is yours here?

select a category below to filter

alphanumeric animal fluffy food macho names nerdy rebellious security sports



Time it takes a Hacker to Brute Force your password

@coders.bro

Numbers of Character	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 Secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Are you in green zone?

<https://haveibeenpwned.com/>

PASSWORDS ARE LIKE UNDERWEARS



Password replacement offerings

Standards-based private key authentication that is convenient and more secure than a password



Biometric (FIDO2)



MFA App



FIDO2 security keys



智方便
iAM Smart

"iAM Smart" Functions

Authentication

Needless to remember different account names and passwords

Personalised Notifications

Receive the news and updates of the government online services



"e-ME" Form Filling

Needless to fill in the same personal details repeatedly

Digital Signing

Digital signing with legal backing

「智方便」的功能

身份認證

無需記住不同的戶口名稱與密碼

個人化提示

接收政府網上服務最新資訊及提示



「填表通」

無需重複填寫個人資料

數碼簽署

作出具法律效力的個人簽署

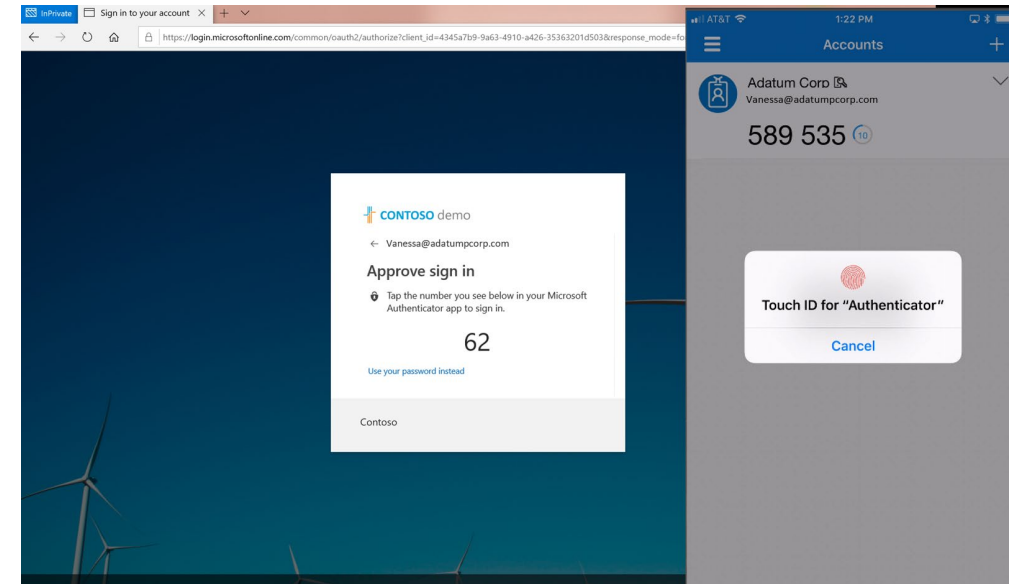
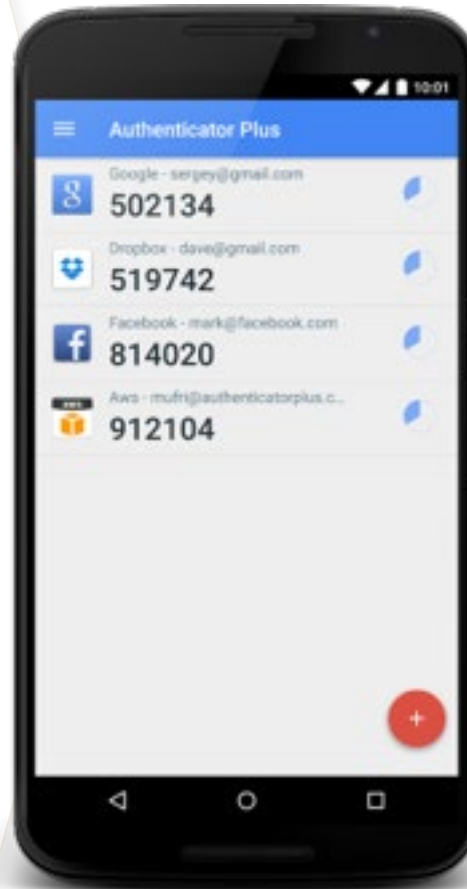
What's more



How to **Secure** your
**SMART
SPEAKER**
when **Working Remotely**







Multifactor Authentication

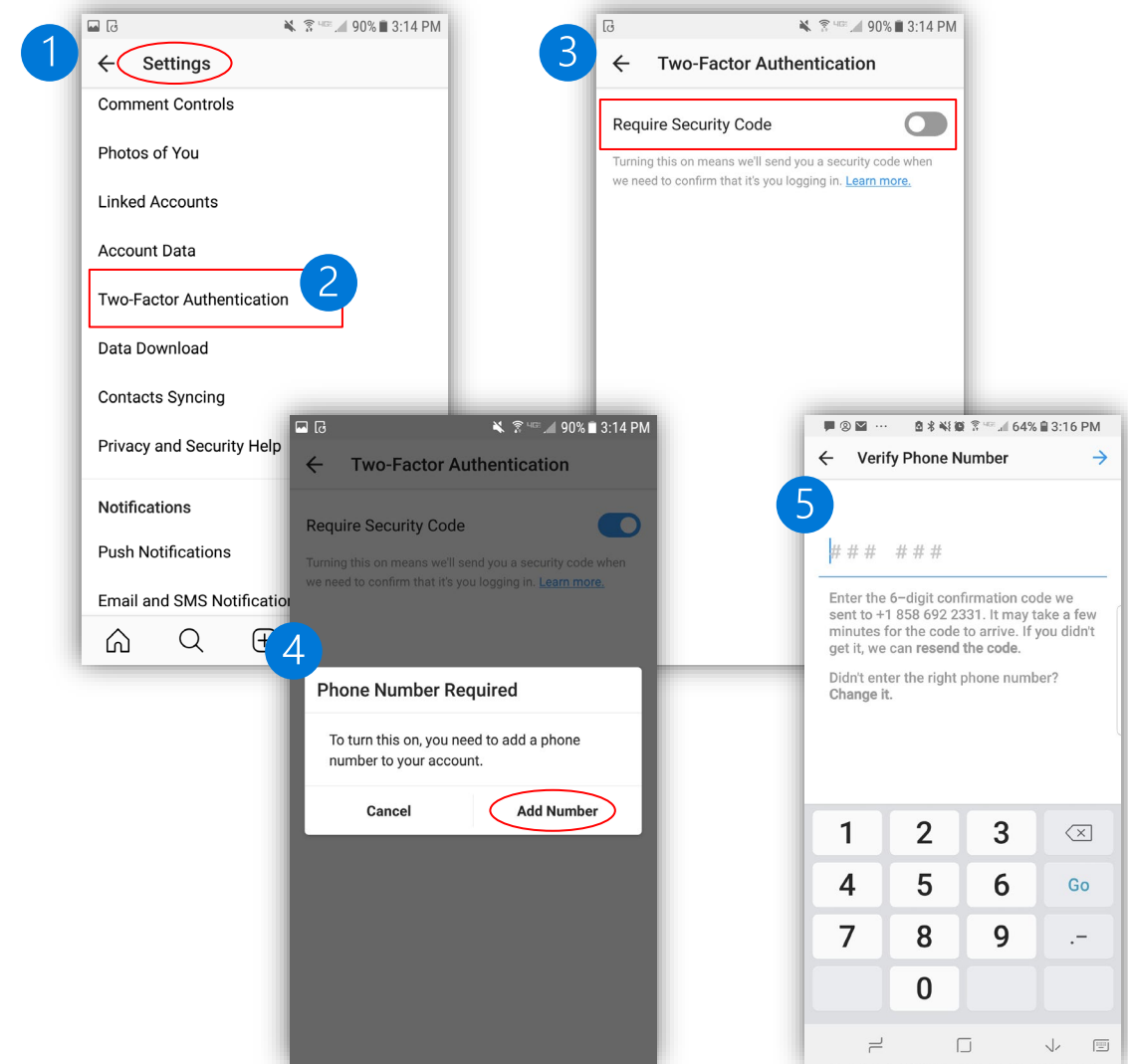


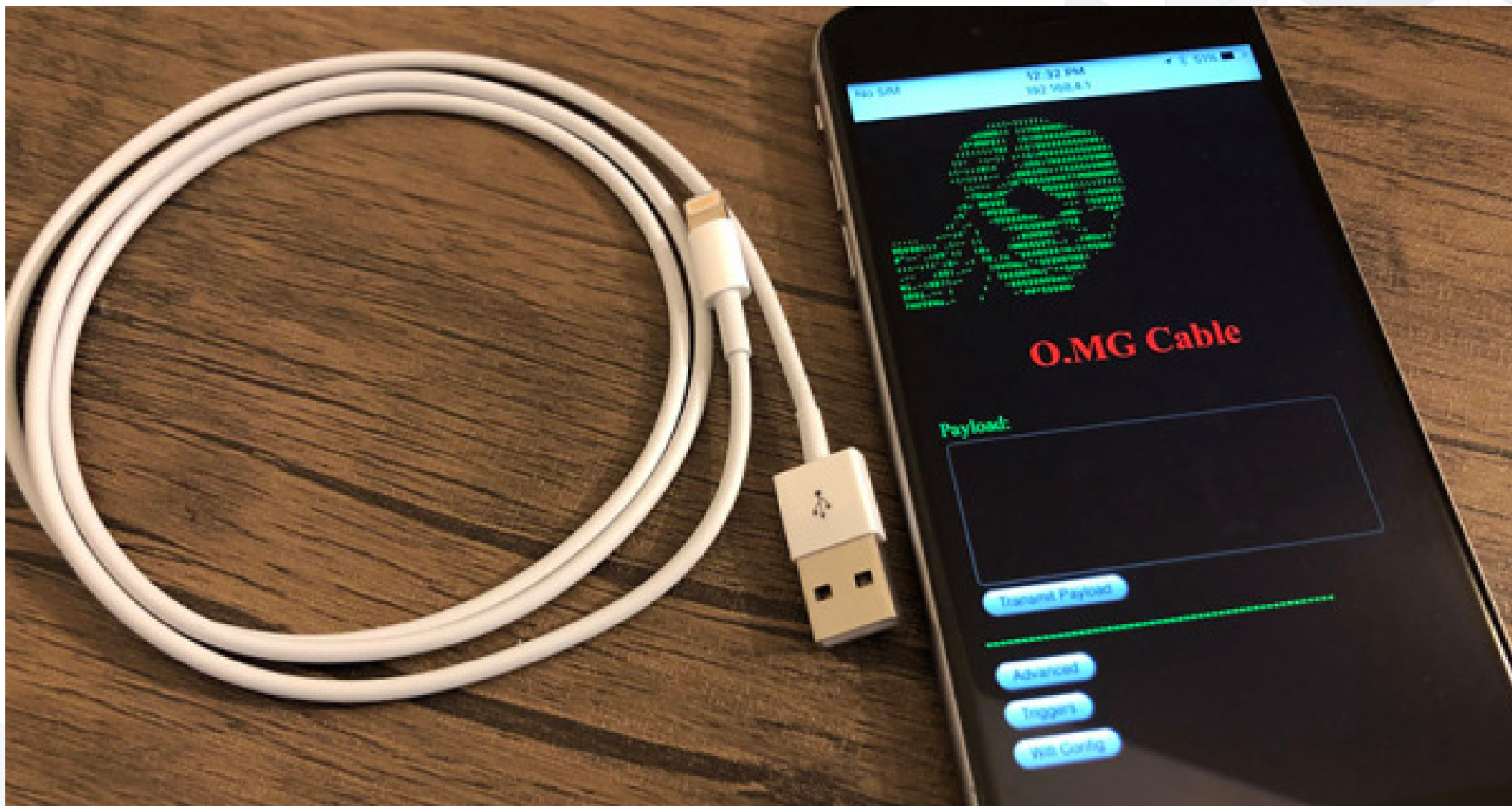
Use two-factor authentication with Instagram














You must have a confirmed telephone number for your Instagram account to use two-factor authentication. When you enter a telephone number to turn on two-factor authentication it will become the confirmed number for your account.

1. Go to your profile and tap  (iPhone) or  (Android) in the top right
2. Scroll down and tap Two-Factor Authentication
3. Tap  Require Security Code to move to the on position
4. If your account doesn't have a confirmed phone number, you'll be asked to enter a phone number. After entering the phone number, tap Next (iPhone) or  (Android).
5. A code will be sent to you. Enter that code and tap Next.





Tips on Cybersecurity

-  Don't click malicious link nor open attachment inside email or instant message from suspicious senders
-  Don't access websites which are not work-related using company devices
-  Don't connect to rogue Wi-Fi hotspots
-  Look carefully for URL that looks legitimate (e.g.: Spelling or Encrypted icon)
-  Be careful of 3rd party app
-  Out of Office Autoreply
-  Mindful of Social Media Usage
-  Take note of Smart Home Assistance devices
-  Do change password in regular basis
-  Do report to your IT for any security incident
-  Stay up-to-date of your devices



You're up to date
Last checked: Today, 17:02

Always verify
Believe nobody
Check everything



ABOUT THE CLOUD SECURITY ALLIANCE

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”



**BUILDING SECURITY BEST PRACTICES
FOR NEXT GENERATION IT**



**GLOBAL, NOT-FOR-PROFIT
ORGANIZATION**



**RESEARCH AND EDUCATIONAL
PROGRAMS**



**CLOUD PROVIDER CERTIFICATION –
CSA STAR**

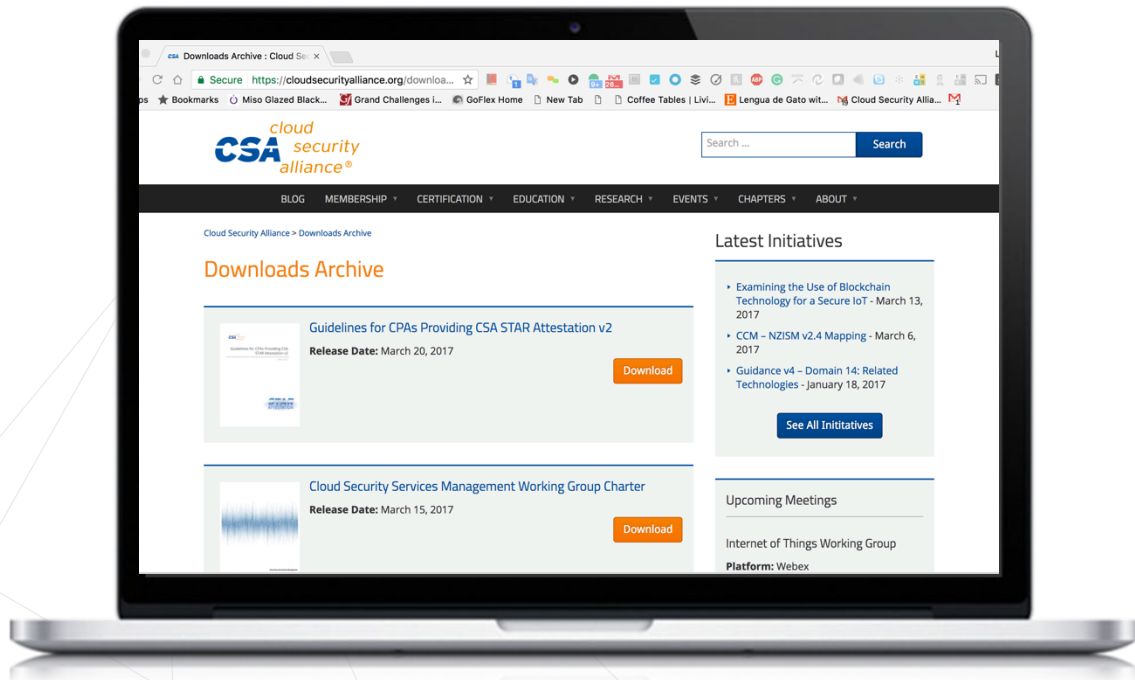


USER CERTIFICATION – CCSK



**THE GLOBALLY AUTHORITATIVE
SOURCE FOR TRUST IN THE CLOUD**

THANK YOU



Contact CSA

Email: chairman@csahkm.org

Twitter: @Cloudsa

Site: www.cloudsecurityalliance.org

Learn: www.cloudsecurityalliance.org/research/cloudbytes

Download: www.cloudsecurityalliance.org/download

GDPR Resource center: <https://gdpr.cloudsecurityalliance.org>

