© boolean logical ltd - www.boolean.co.uk

CYBER SECURITY

Has it changed faces in the new world?

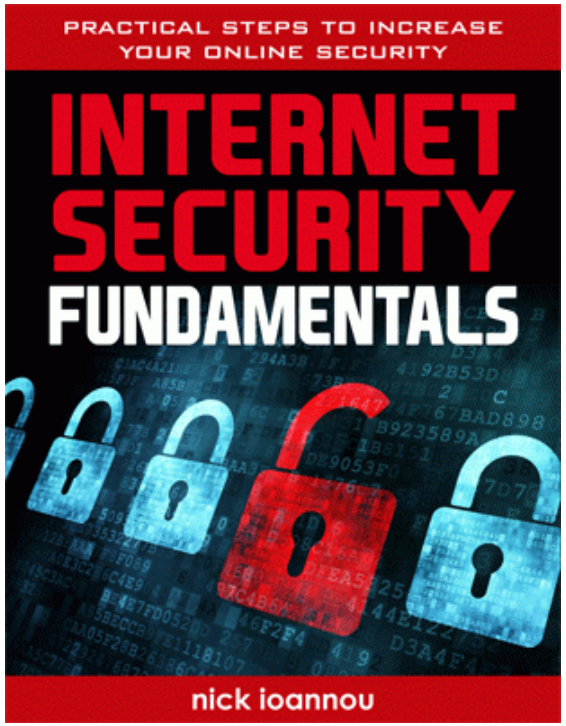
BOOLEAN LOGICAL

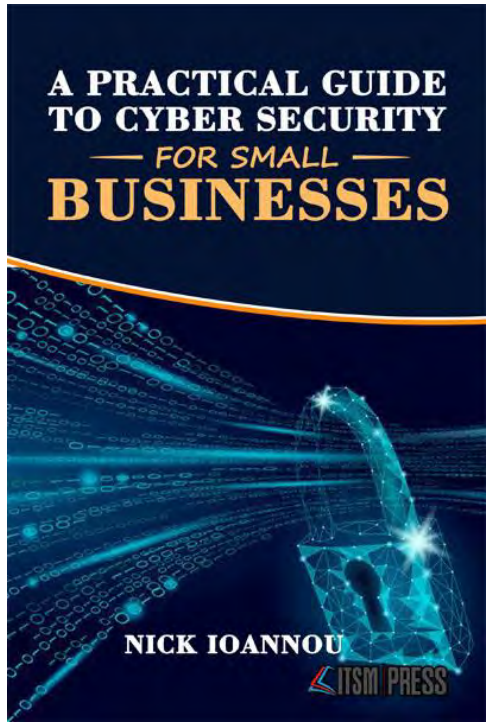
nick ioannou

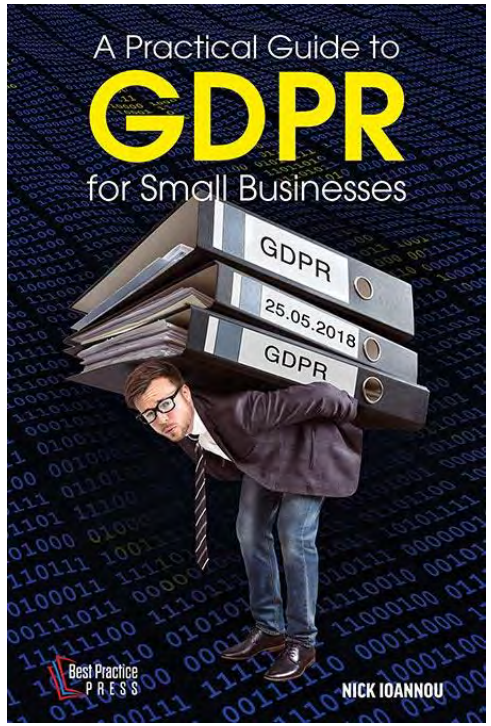
Head of IT ◦ Author ◦ IT Blogger

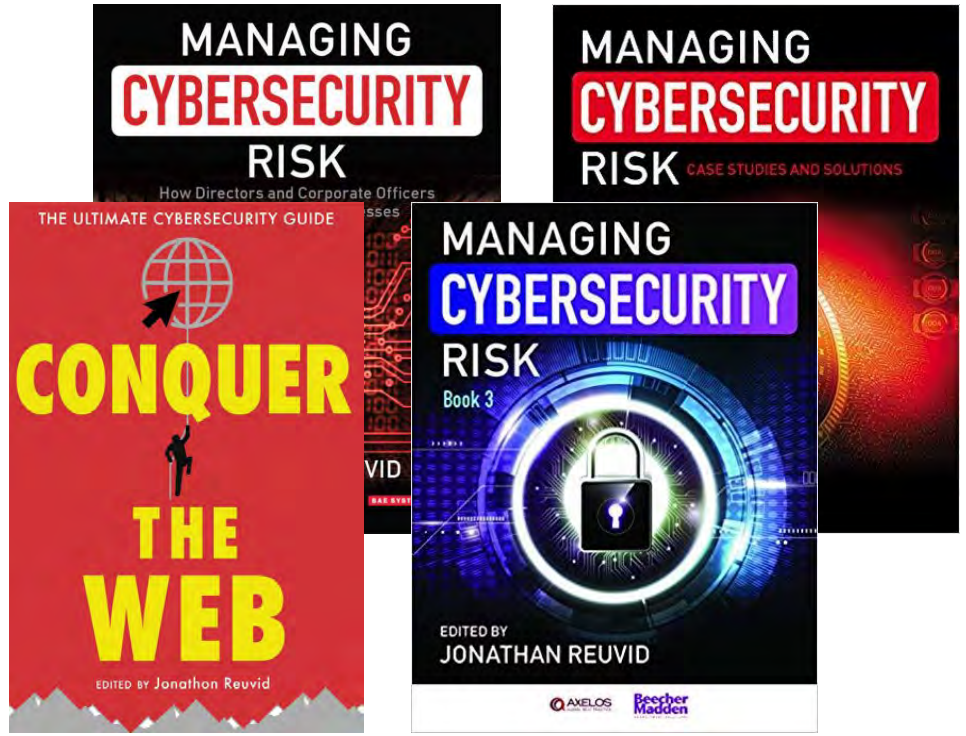
© boolean logical ltd - www.boolean.co.uk

My Amazon Author Page can be found at: www.amazon.com/author/nick-ioannou









- Author -

- Contributing Author -

BOOLEAN LOGICAL

RGF architects

dlg architects

vio

BBC Worldwide

magmed

Who is nick ioannou?

© boolean logical ltd - www.boolean.co.uk

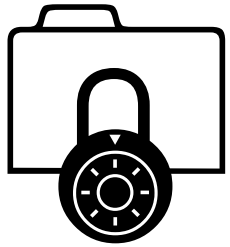
94% of malware attacks are carried out through email

- Viruses have been around for nearly 30 years
- First known ransomware was in 1989
- One criminal gang has received over €300M in ransoms in 3 years
- Phishing emails sent to steal login credentials
- Trojans can live on computers for months stealing information
- 38% of malicious email attachments are MS Office files
- Criminals offer automated malware services to other criminals

bitcoin = = £ $ €

Why are there so many security incidents in the news?

© boolean logical ltd - www.boolean.co.uk



How Criminals Use Our Greed Against Us

© boolean logical ltd - www.boolean.co.uk

CONGRATULATIONS!

You received a £100 Voucher from

LiDL

About Lidl.co.uk Vouchers

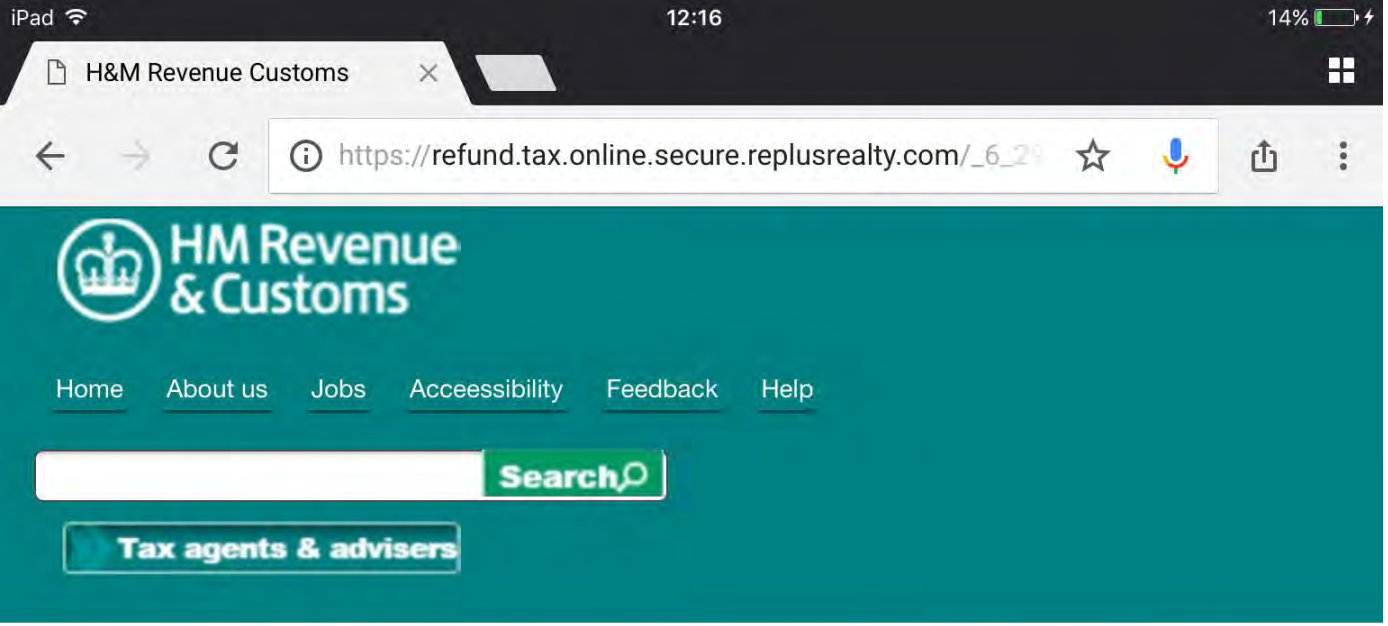
- Can be used as full or part payment for goods
- Choose from hundreds of products.
- Spend online at lidl.co.uk.
- Check balance when logged into your LiDL account.
- Expires 10 years from date of issue

Click here to claim your £100 GC

PREMIER LEAGUE

There is no such thing as a free lunch

© boolean logical ltd - www.boolean.co.uk



Address Information - Please enter your name and address as you have it listed for your credit card.

CardHolder Name:

Date of Birth: (dd/mm/yyyy)

Mother Maiden Name:

Address:

Town/City:

Province/Region:

Postal Code:

Phone Number:

Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.

Account number:

Sort Code:

Debit / Credit Card Number:

Maestro VISA MasterCard

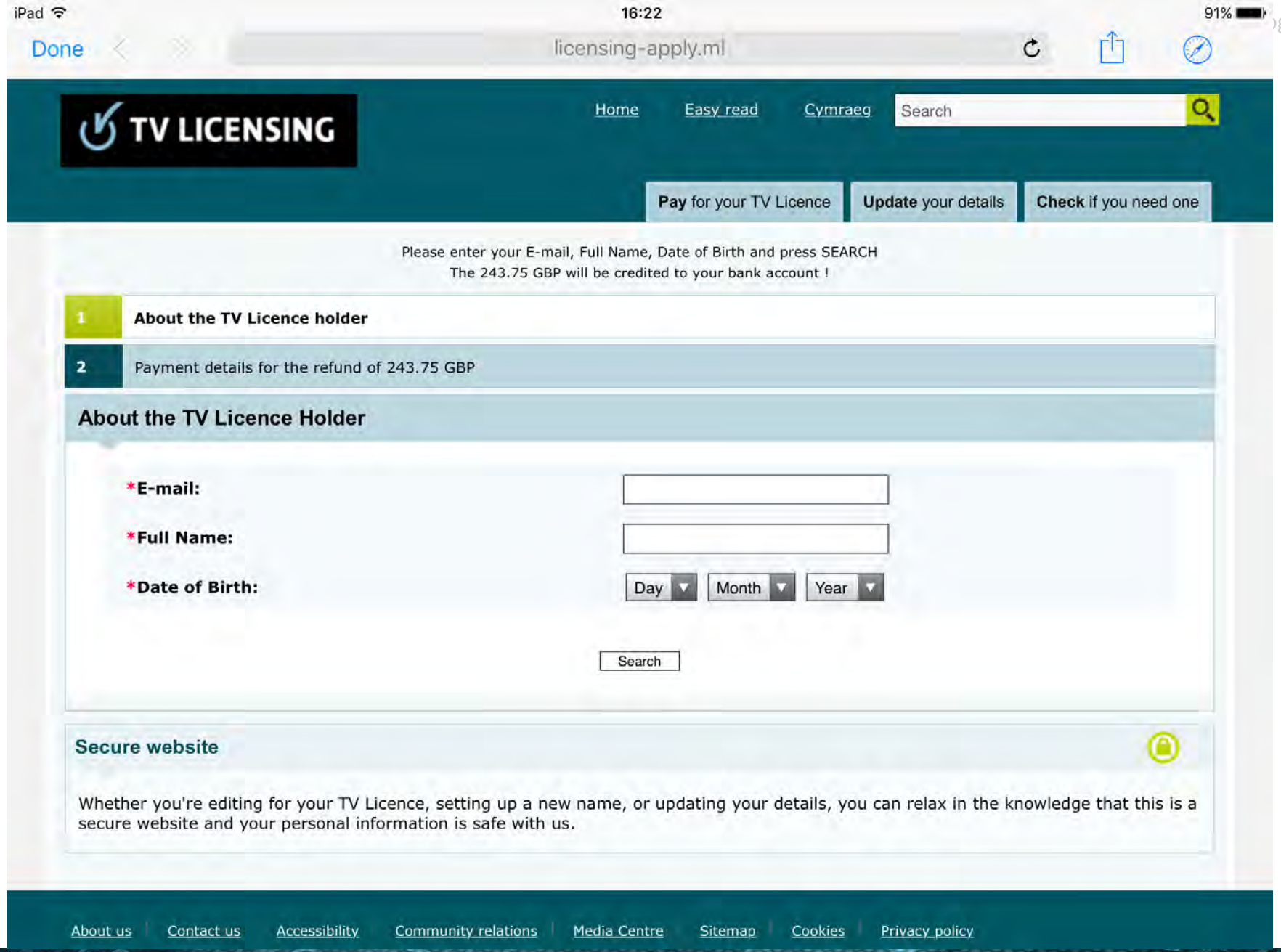
Expiration Date: - Month - / - Year -

Card Verification Number: [view sample]

Submit Information

Common Hooks - The tax refund

ogical ltd - www.boolean.co.uk



Common Hooks - The Overpayment Refund

© boolean logical ltd - www.boolean.co.uk

Common Hooks - The Fake Payment

© boolean logical ltd - www.boolean.co.uk

The Key Generator Utility from the internet will let you authorise the software, but it will often do a lot more besides.

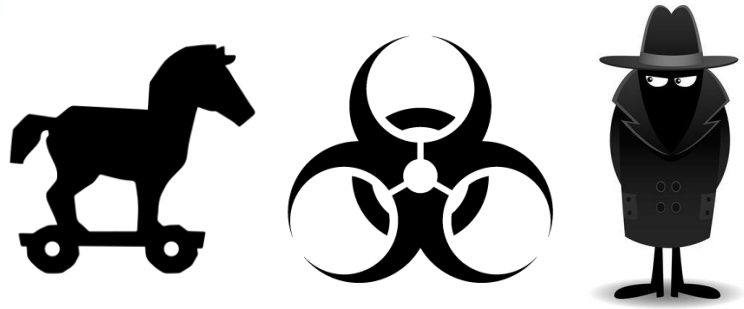
TRIAL VERSION

AUTODESK® REVIT®

Adobe® Creative Cloud™ Photoshop® CC

KEYGEN or CRACK UTILITY

TROJAN, VIRUS or SPYWARE

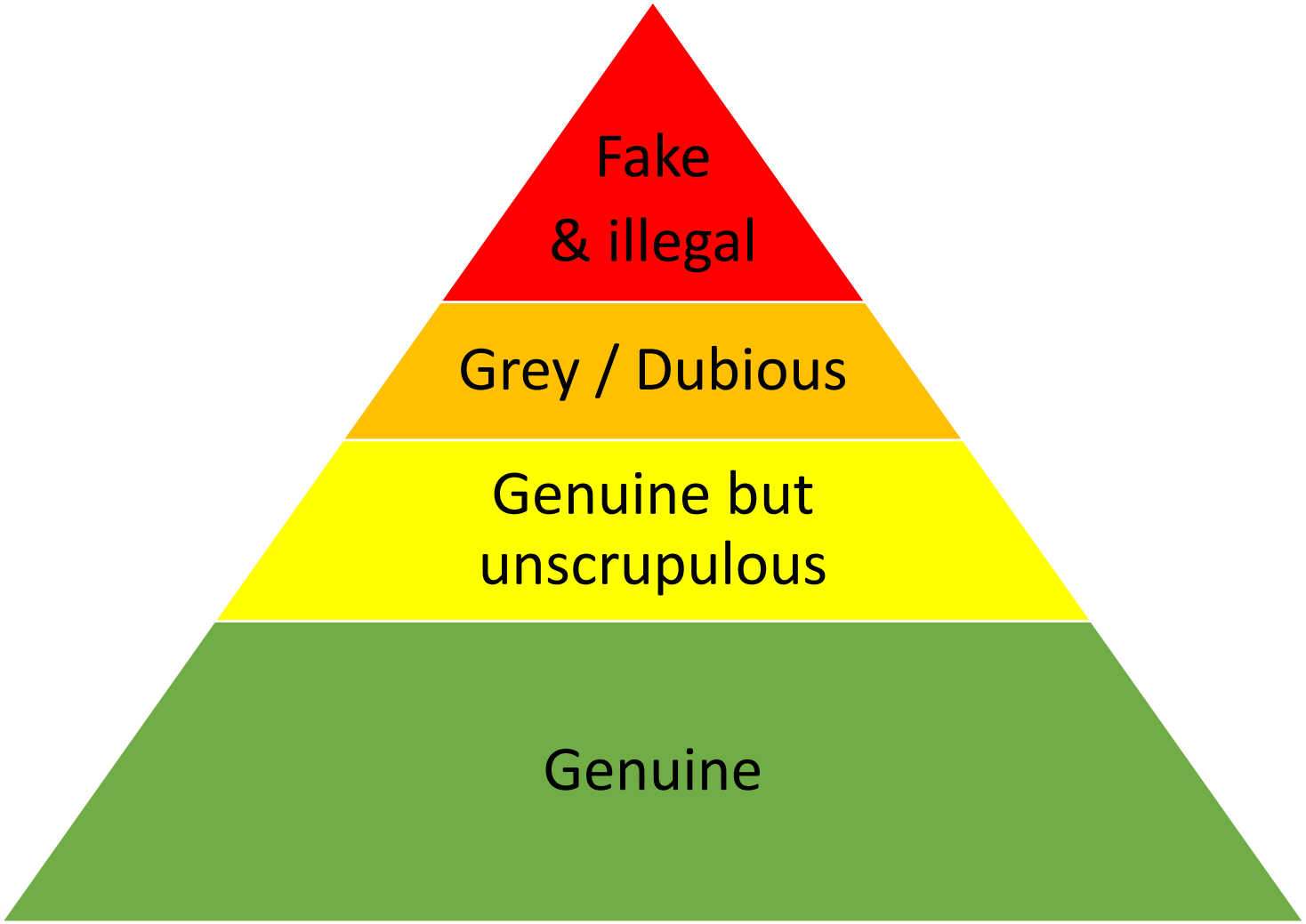


Illegal sofware will probably contain malware?

© boolean logical ltd - www.boolean.co.uk

Outright fake and illegal

- Fake official websites
- Fake online stores
- Fake discount vouchers
- Fake gift cards or vouchers
- Fake digital subscription
- Fake streaming service
- Fake digital in-game currency
- Fake crypto-currencies
- Fake software
- Fake online service
- Fake online casino credits
- Fake loans
- Fake competitions
- Software keygen utilities



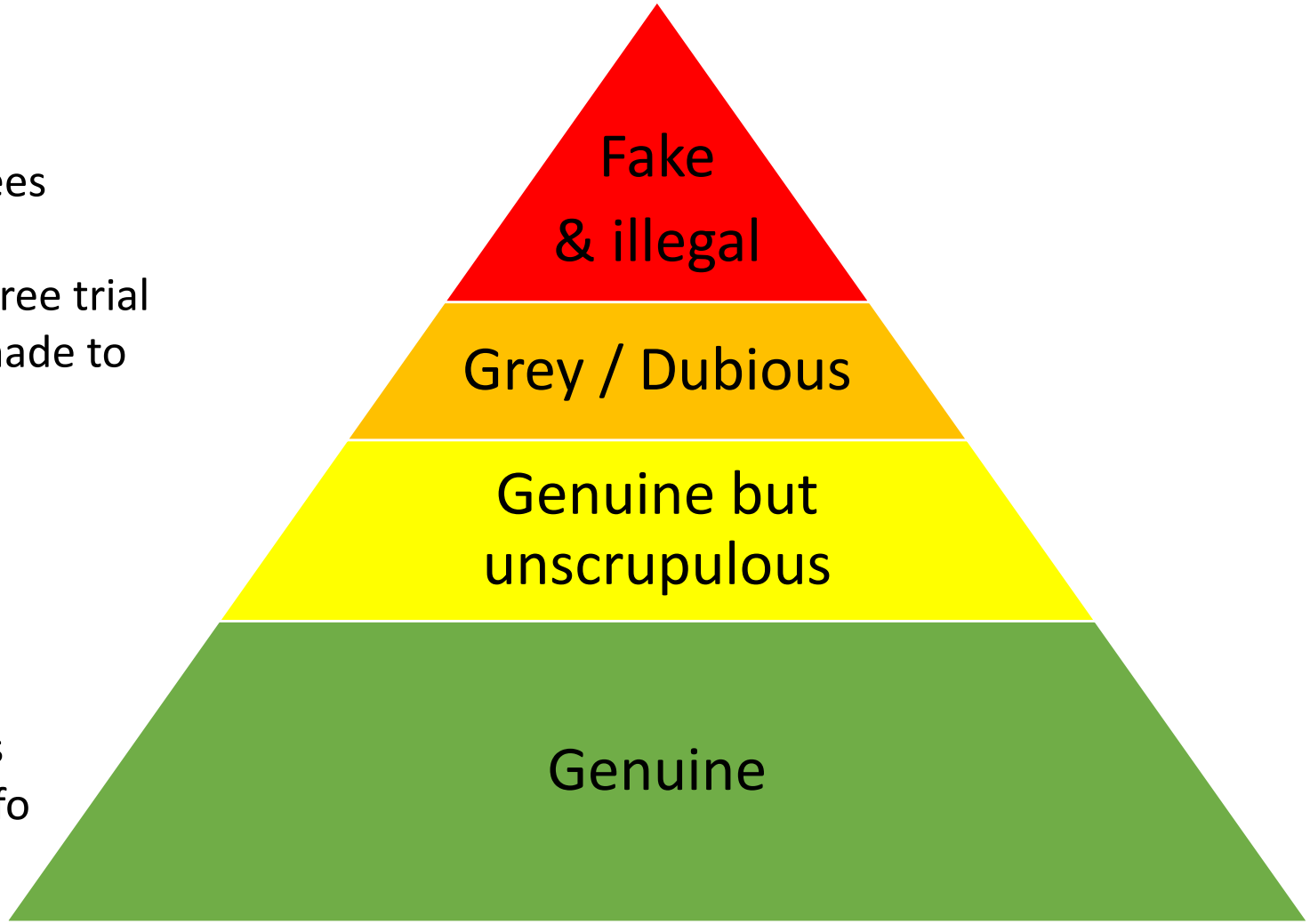
© boolean logical ltd - www.boolean.co.uk

Grey / Dubious

- Unofficial websites with unnecessary fees
- Online stores with fake reviews
- Overpriced subscription services after free trial
- Overpriced competitions and quizzes made to look like part of a website

Genuine but unscrupulous

- You supply personal information
- You give up image rights to your photos
- You supply location data and activity info
- You supply spending patterns
- Reverse auction platforms



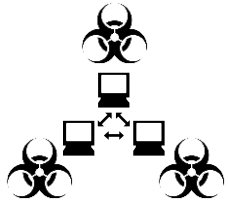
What You Might Encounter Online

© boolean logical ltd - www.boolean.co.uk

Virus

Ransomware

Botnet



Spyware / Phishing

Trojan

Scam

Worm

EXTORTION

Payments you are forced into making

- Ransom Demand To Access Files / Computer
- DDOS Denial Of Service
- Sextortion

FRAUD

Payments you are tricked into making

- Fake Service
- Fake Product
- Money Transfer Scam

THEFT

Transferring your data to the criminals

- Login Credentials / Contacts
- Financial Information
- Webcam Footage

DISRUPTION

Goal is to cause problems

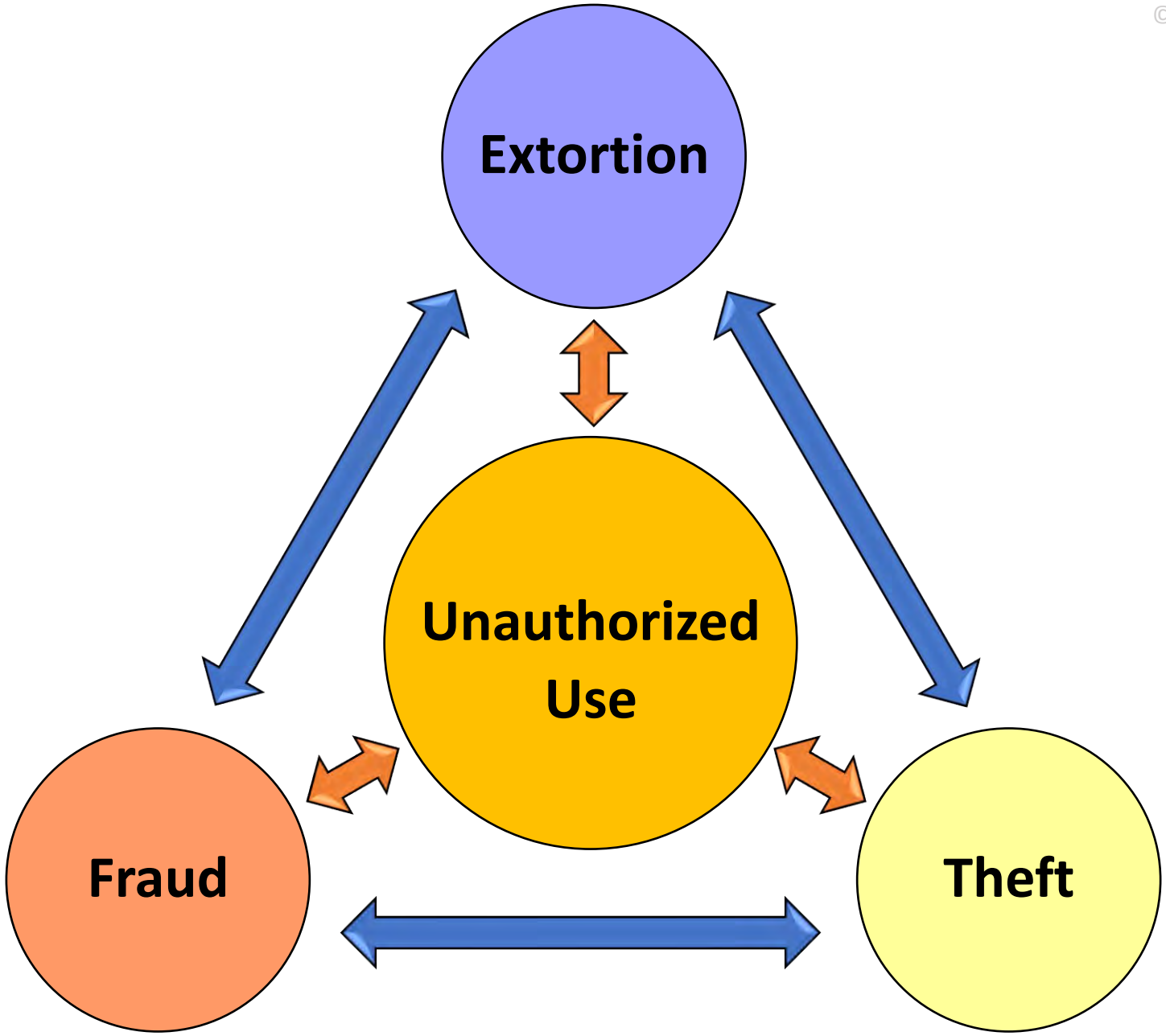
- Lower Share Price
- Benefit Competitor
- Revenge / Prove A Point

Unauthorised Use Of Your Computer

- Spam Relay
- Web Server
- Crypto-Currency Mining

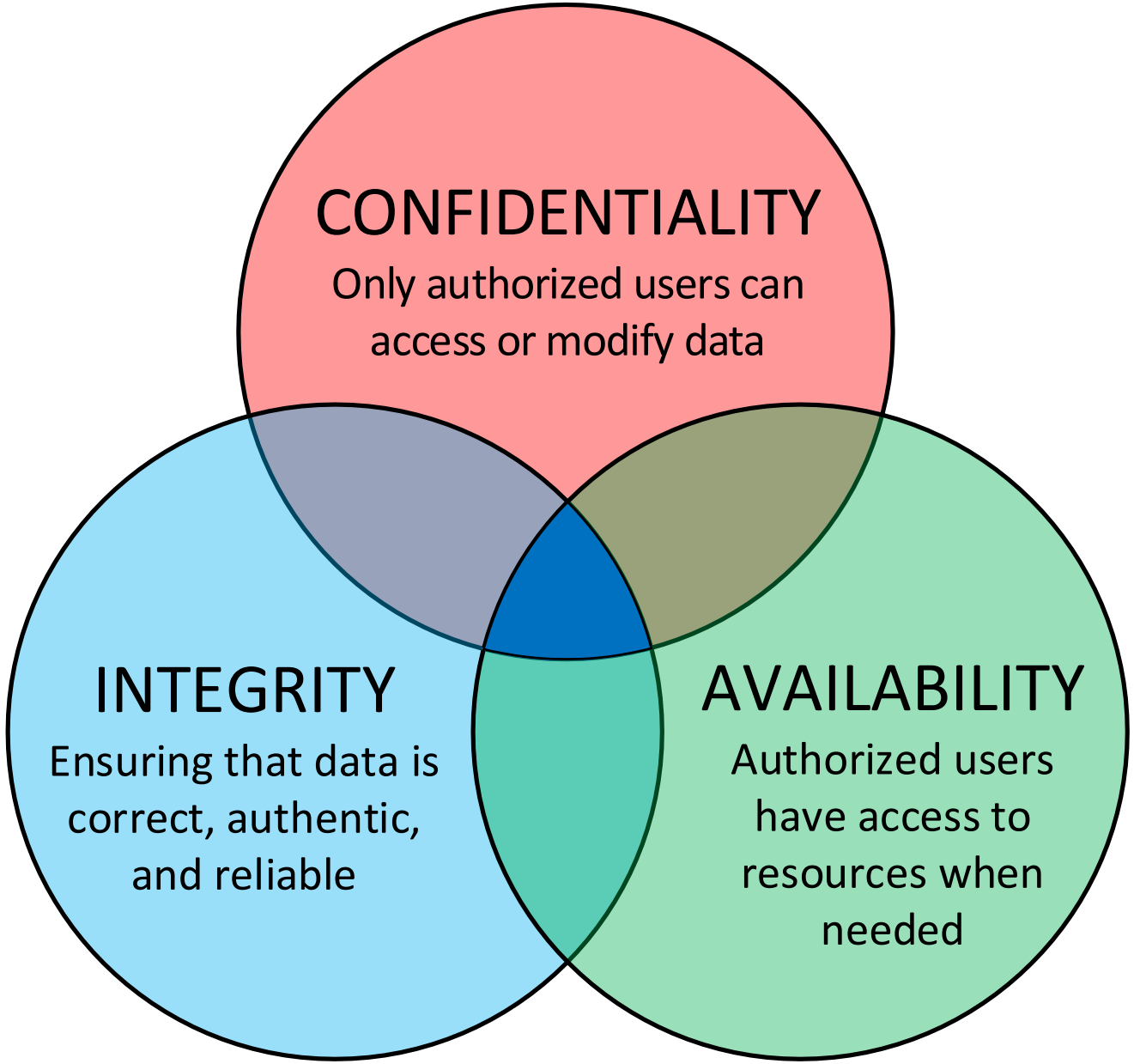
Why Would Cyber Criminals Target an Organisation?

© boolean logical ltd - www.boolean.co.uk



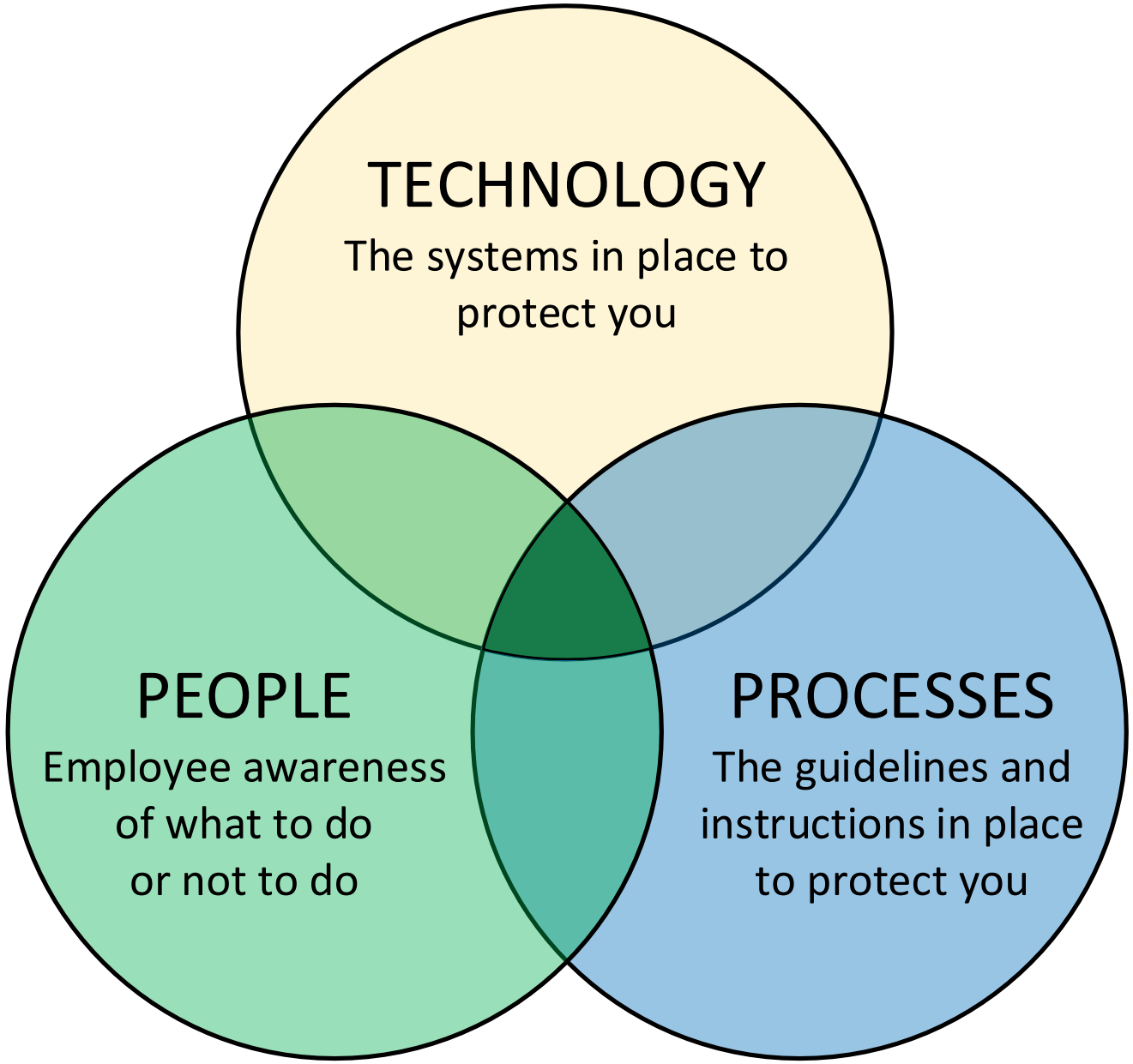
Cyber Criminals Can Change Tactics

© boolean logical ltd - www.boolean.co.uk



What is the Aim of Cyber Security?

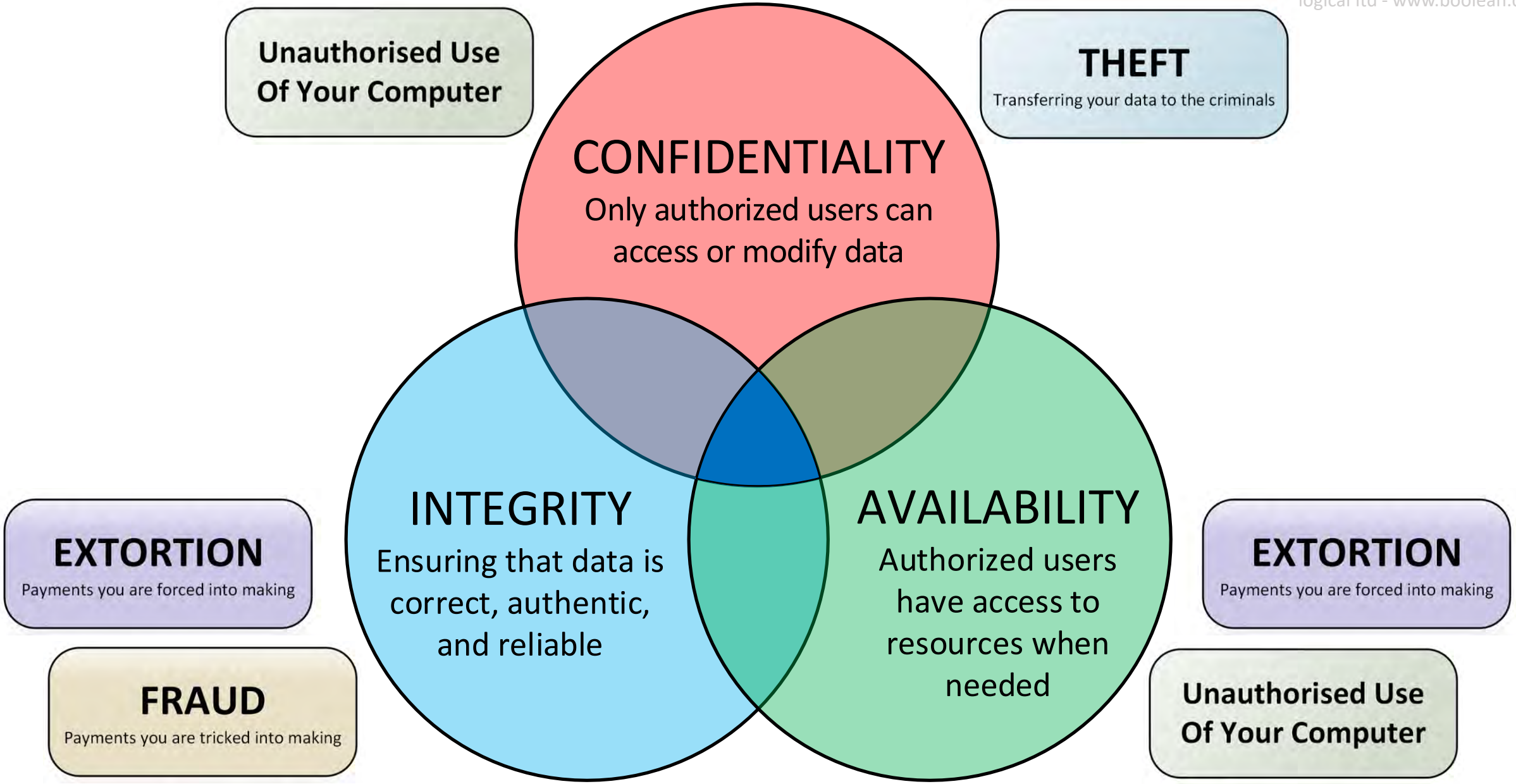
© boolean logical ltd - www.boolean.co.uk



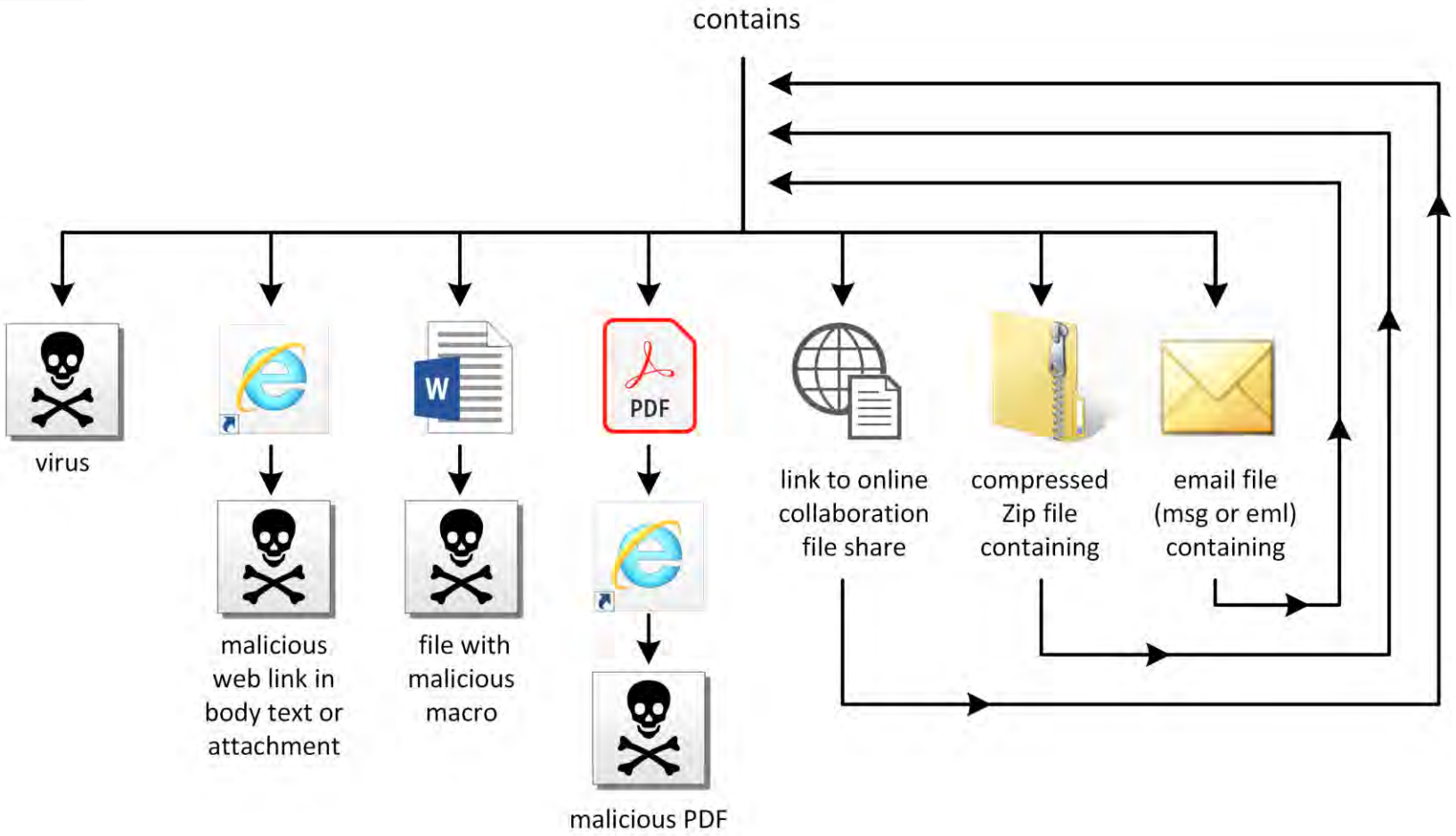
The How of Cyber Security

© boolean logical ltd - www.boolean.co.uk

How Cyber Criminals Succeed?



© boolean logical ltd - www.boolean.co.uk



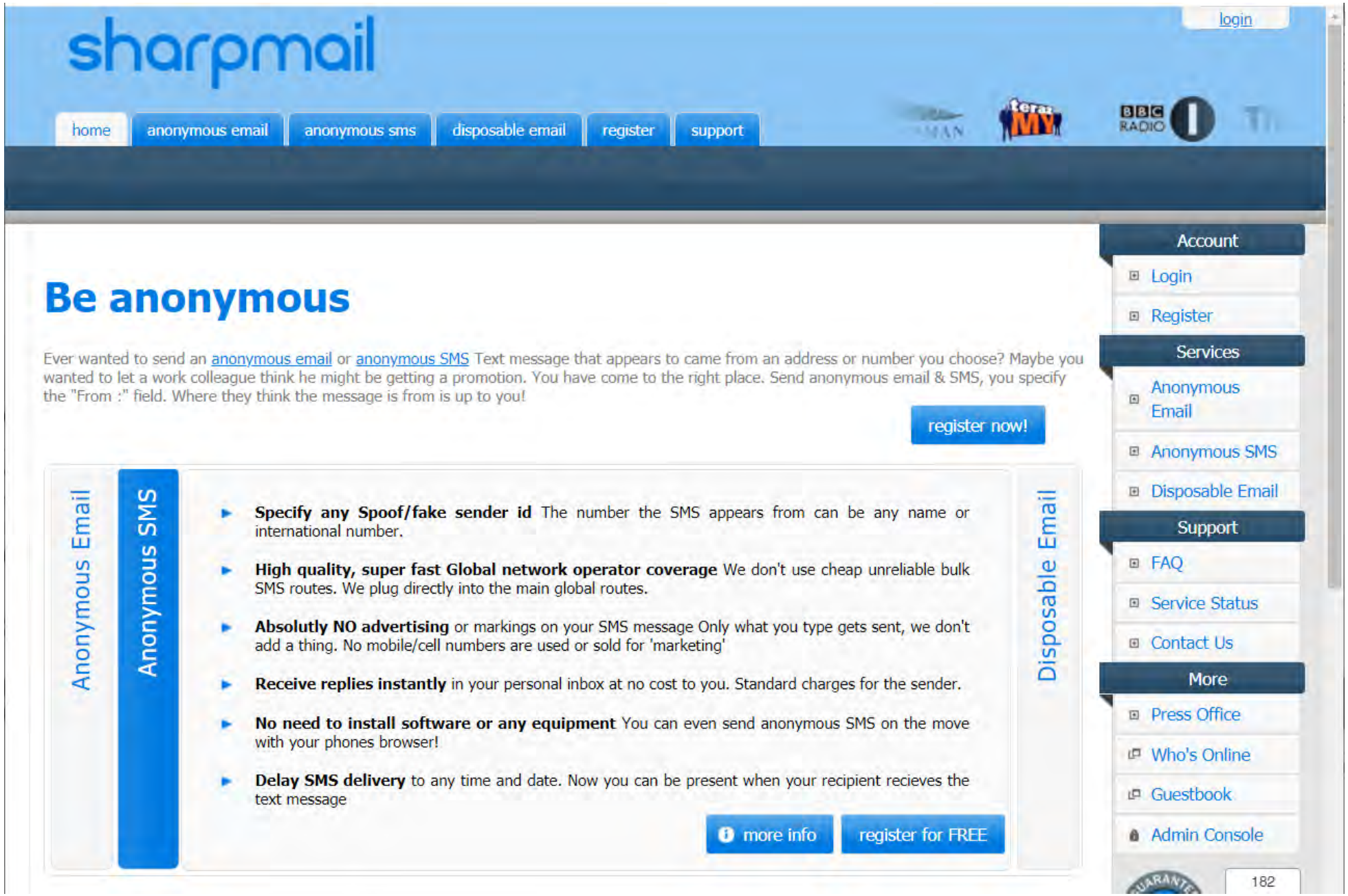
Communication Options For The Criminals?

© boolean logical ltd - www.boolean.co.uk

Telephone & mobile numbers can be spoofed

Voicemail on social media platforms

Old School Communication Options



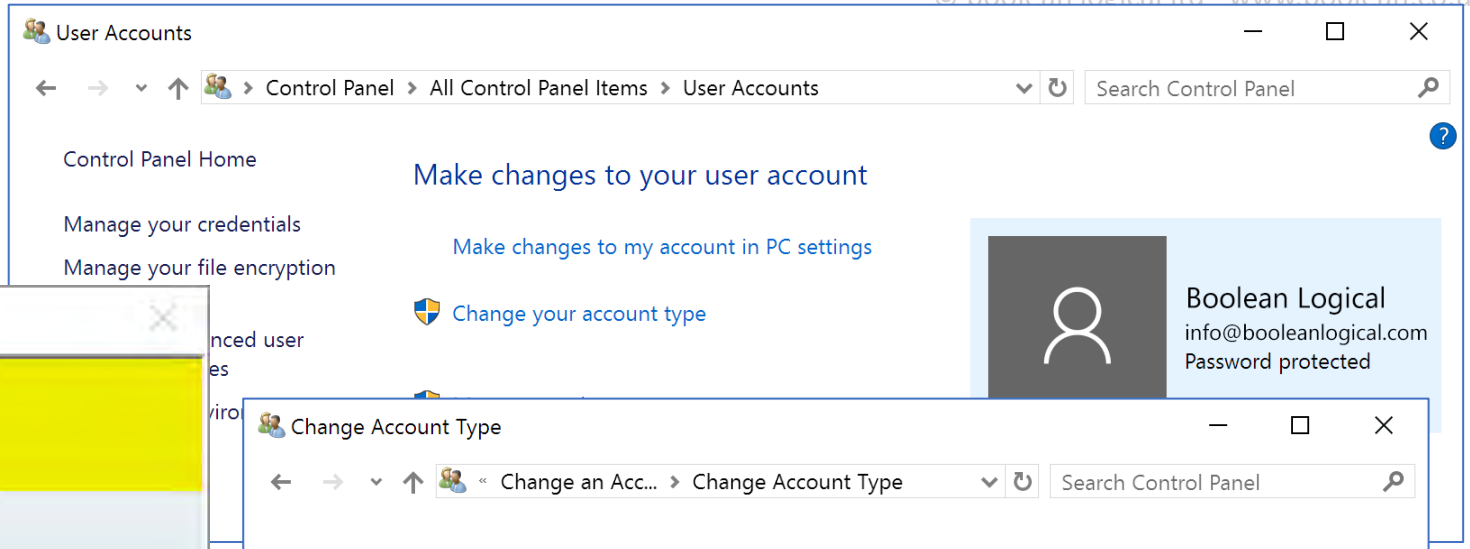
Spoofing SMS & email made easy

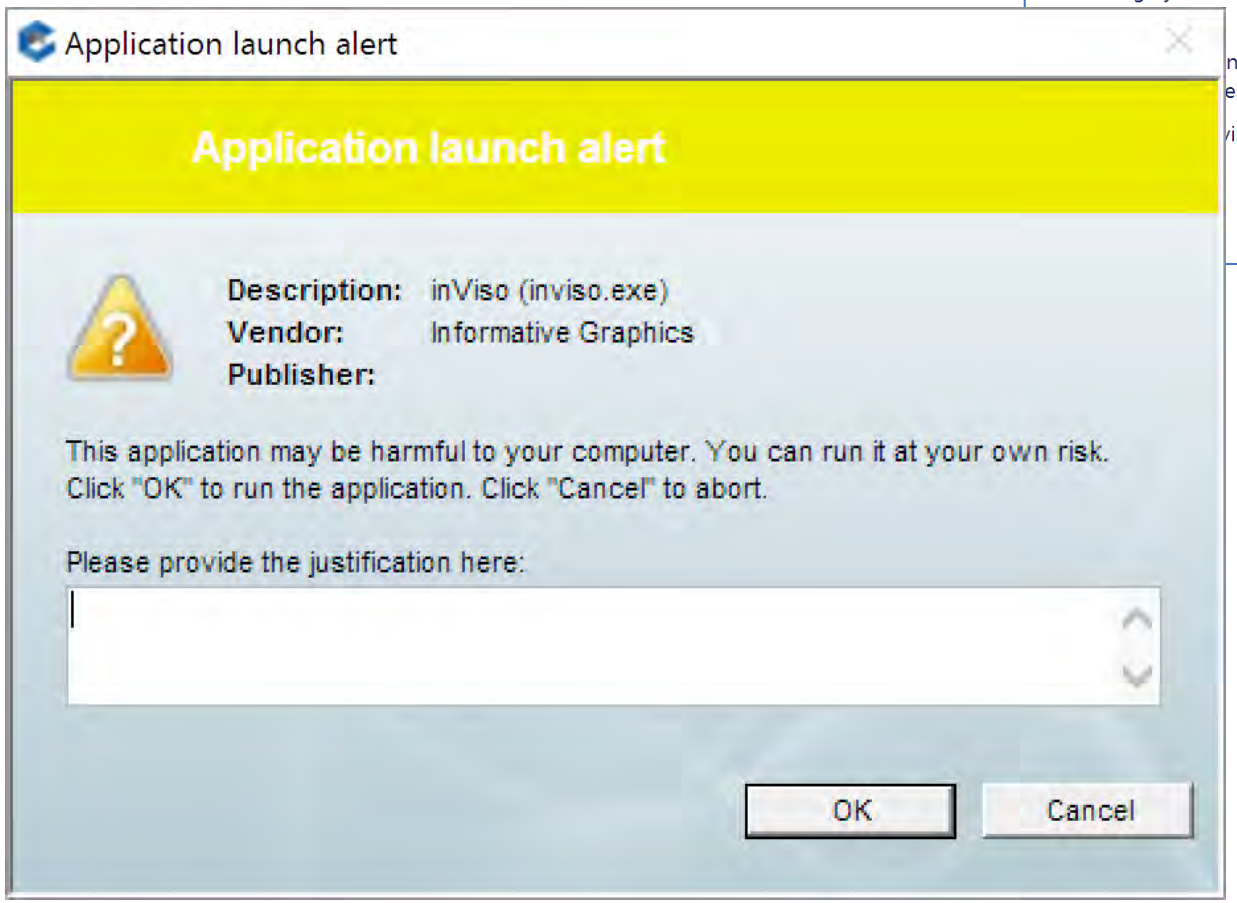
© boolean logical ltd - www.boolean.co.uk

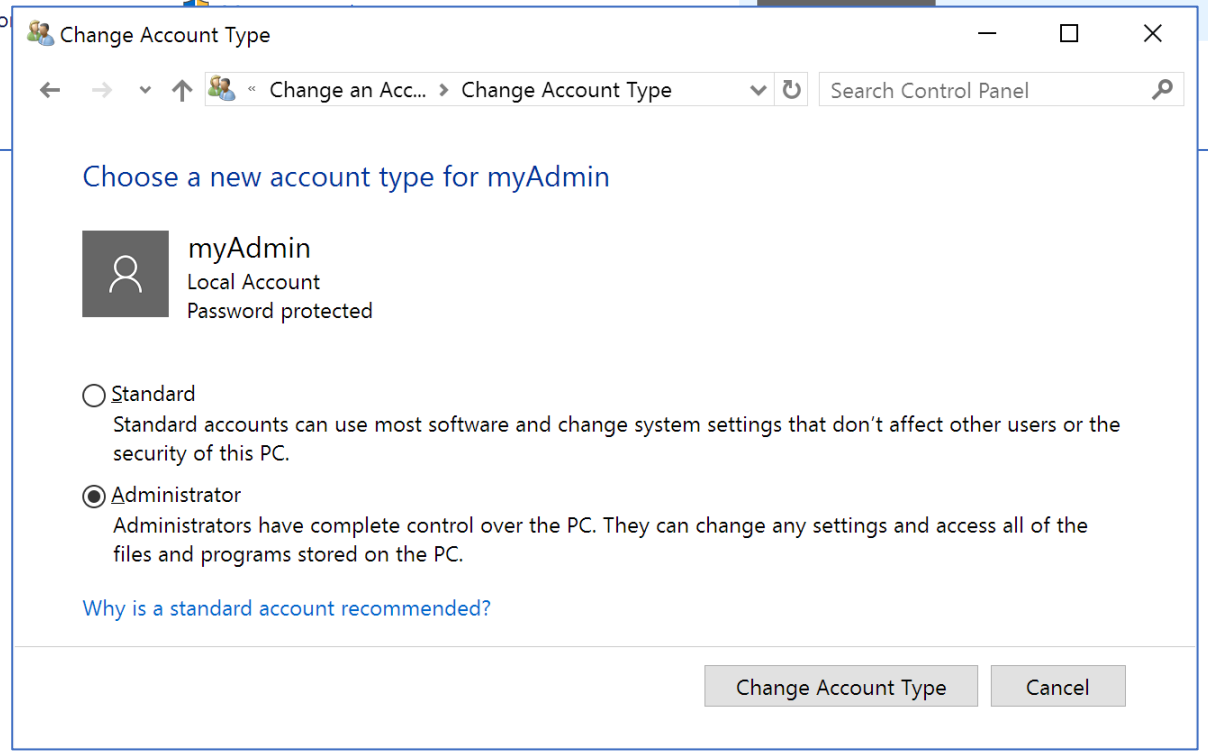
How Adopting A Zero-Trust Posture Can Improve Your Security

© boolean logical ltd - www.boolean.co.uk

CYBERARK

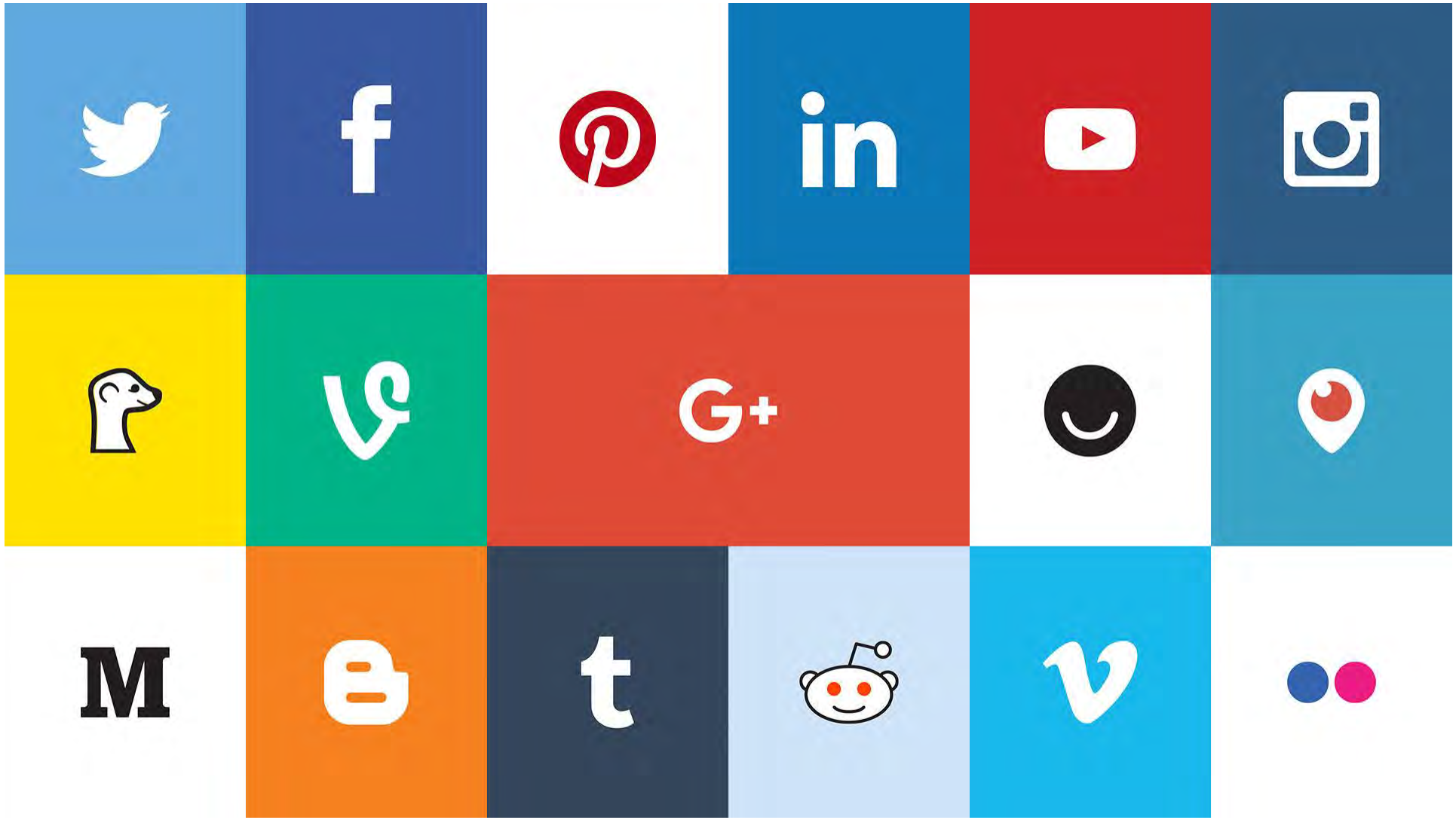






Admin rights equals a security risk

© boolean logical ltd - www.boolean.co.uk



How much information are you giving away?

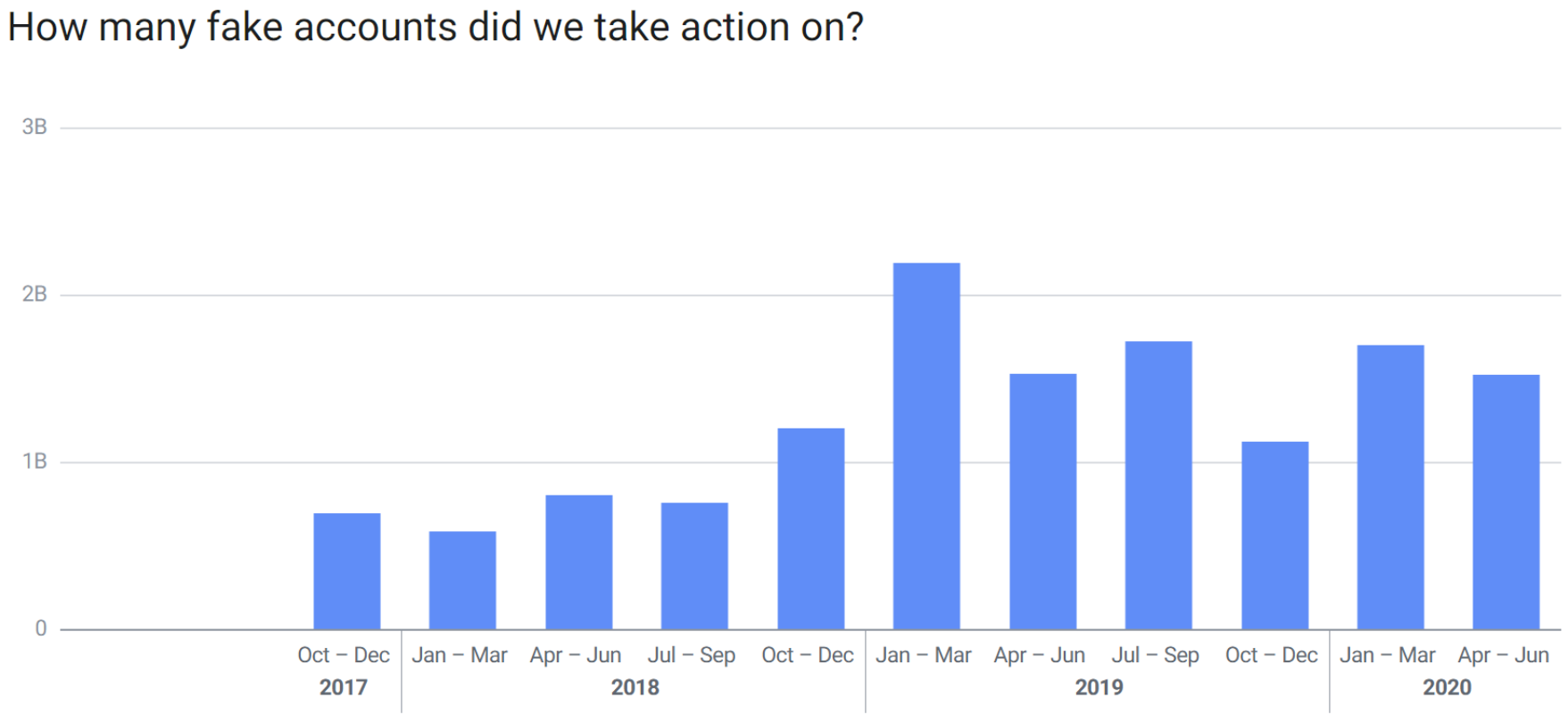
© boolean logical ltd - www.boolean.co.uk

There are over 95 social media systems

© boolean logical ltd - www.boolean.co.uk

Accounts actioned declined from 1.7 billion accounts in Q1 2020 to 1.5 billion in Q2

We estimate that fake accounts represented approximately 5% of our worldwide monthly active users (MAU) on Facebook during Q2 2020



https://transparency.facebook.com/community-standards-enforcement#fake-accounts

FACEBOOK

Social media is also an infection route

© boolean logical ltd - www.boolean.co.uk

Accounts actioned declined from 1.7 billion accounts in Q1 2020 to 1.5 billion in Q2

We estimate that fake accounts represented approximately 5% of our worldwide monthly active users (MAU) on Facebook during Q2 2020

256 million active Facebook users

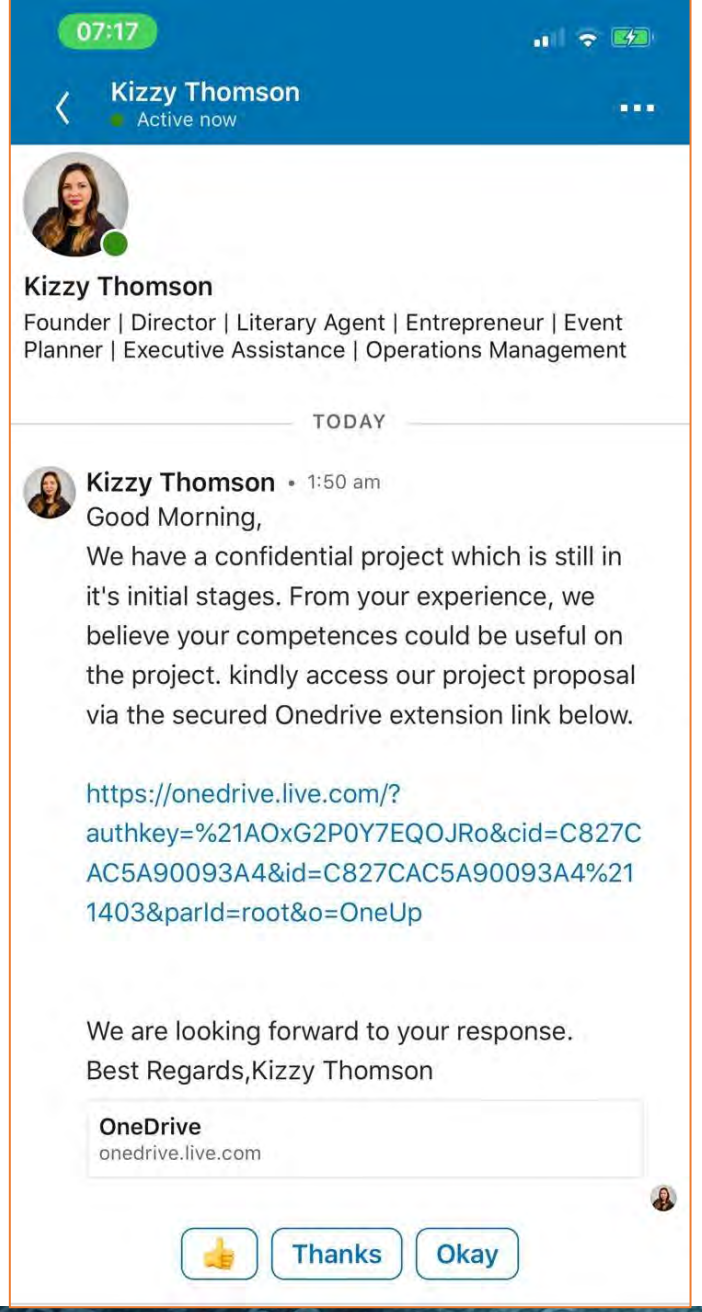
5% = 12,800,000 fake accounts

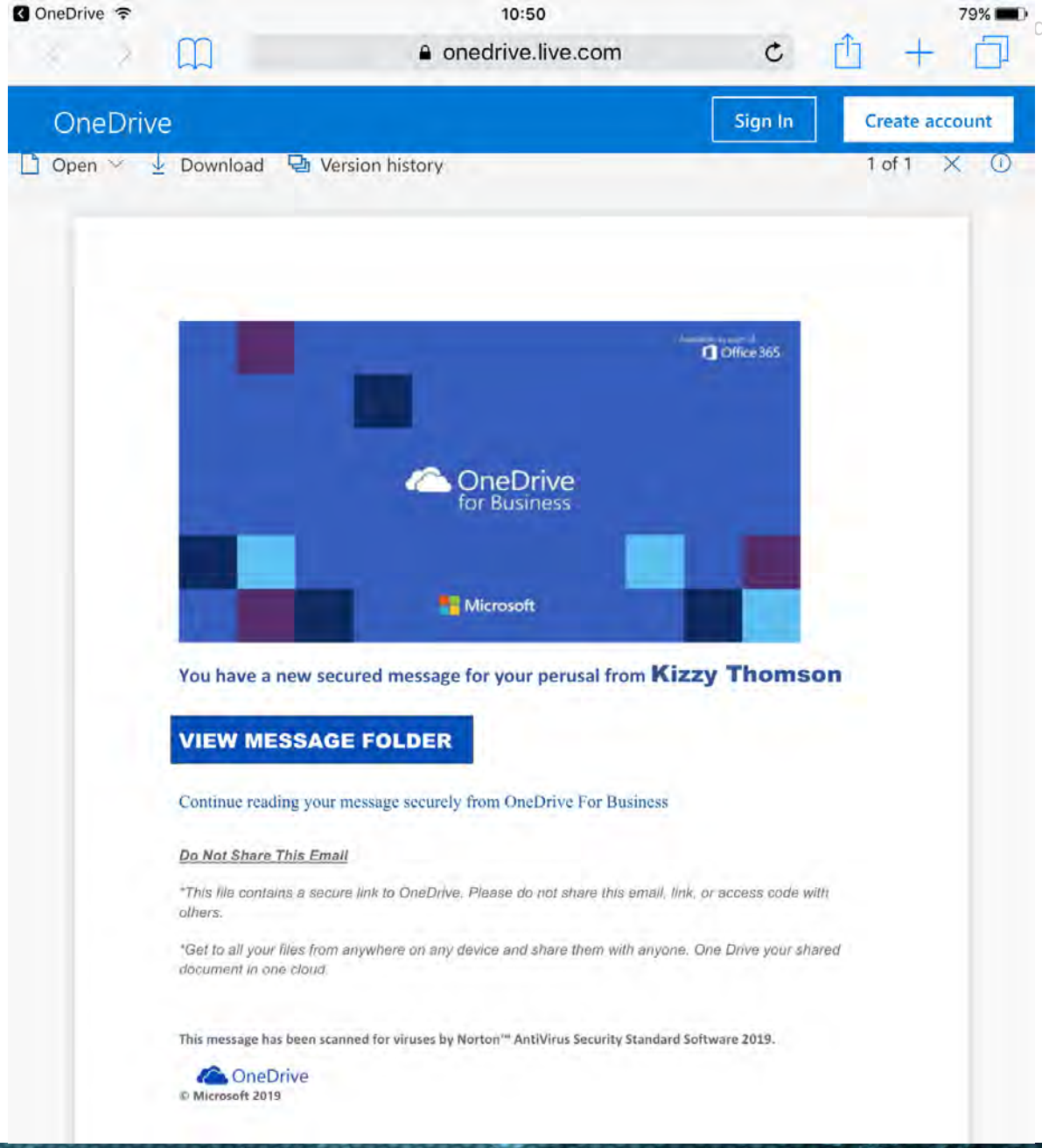
https://transparency.facebook.com/community-standards-enforcement#fake-accounts

FACEBOOK

Social media is also an infection route

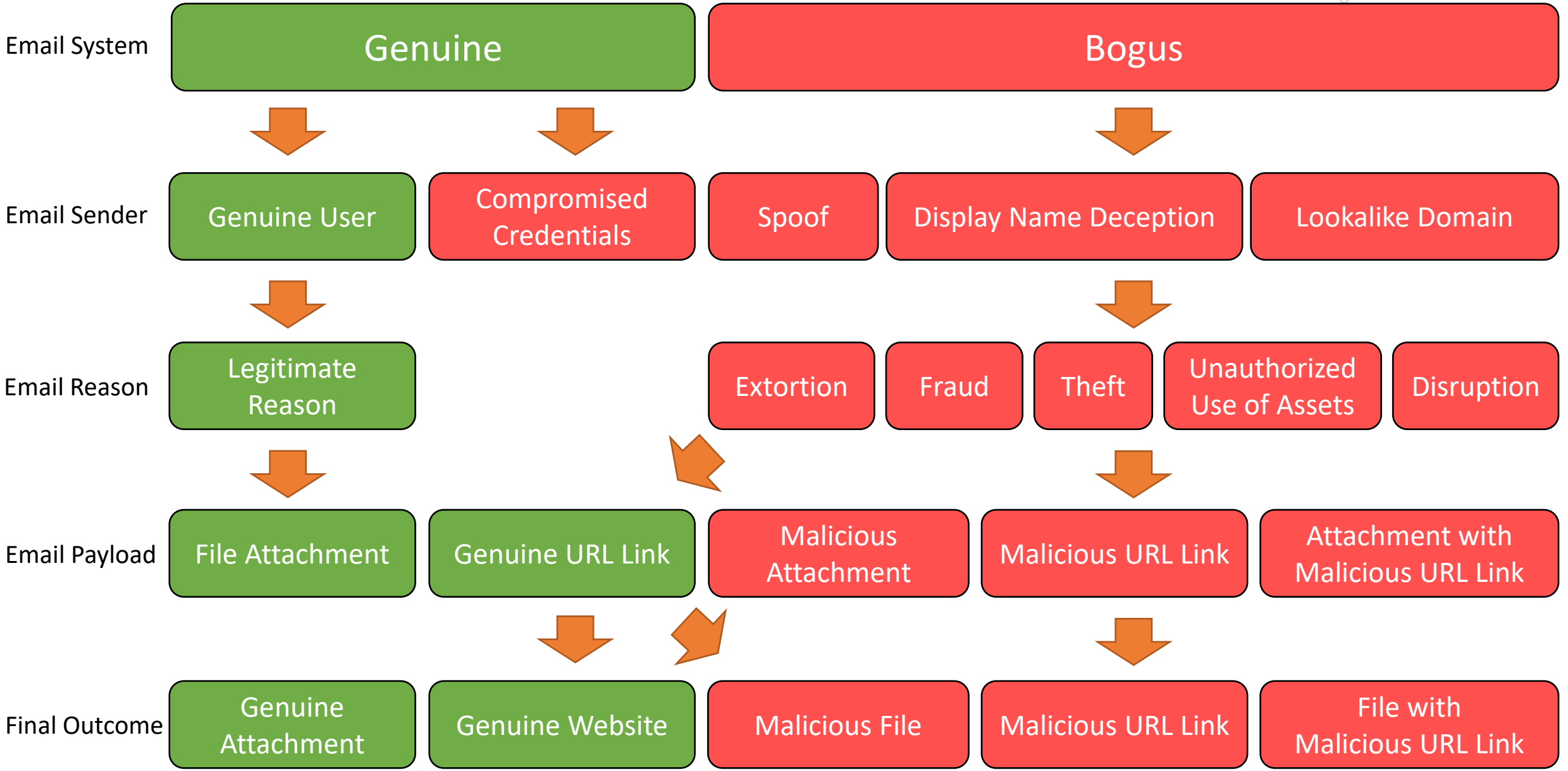
d - www.boolean.co.uk





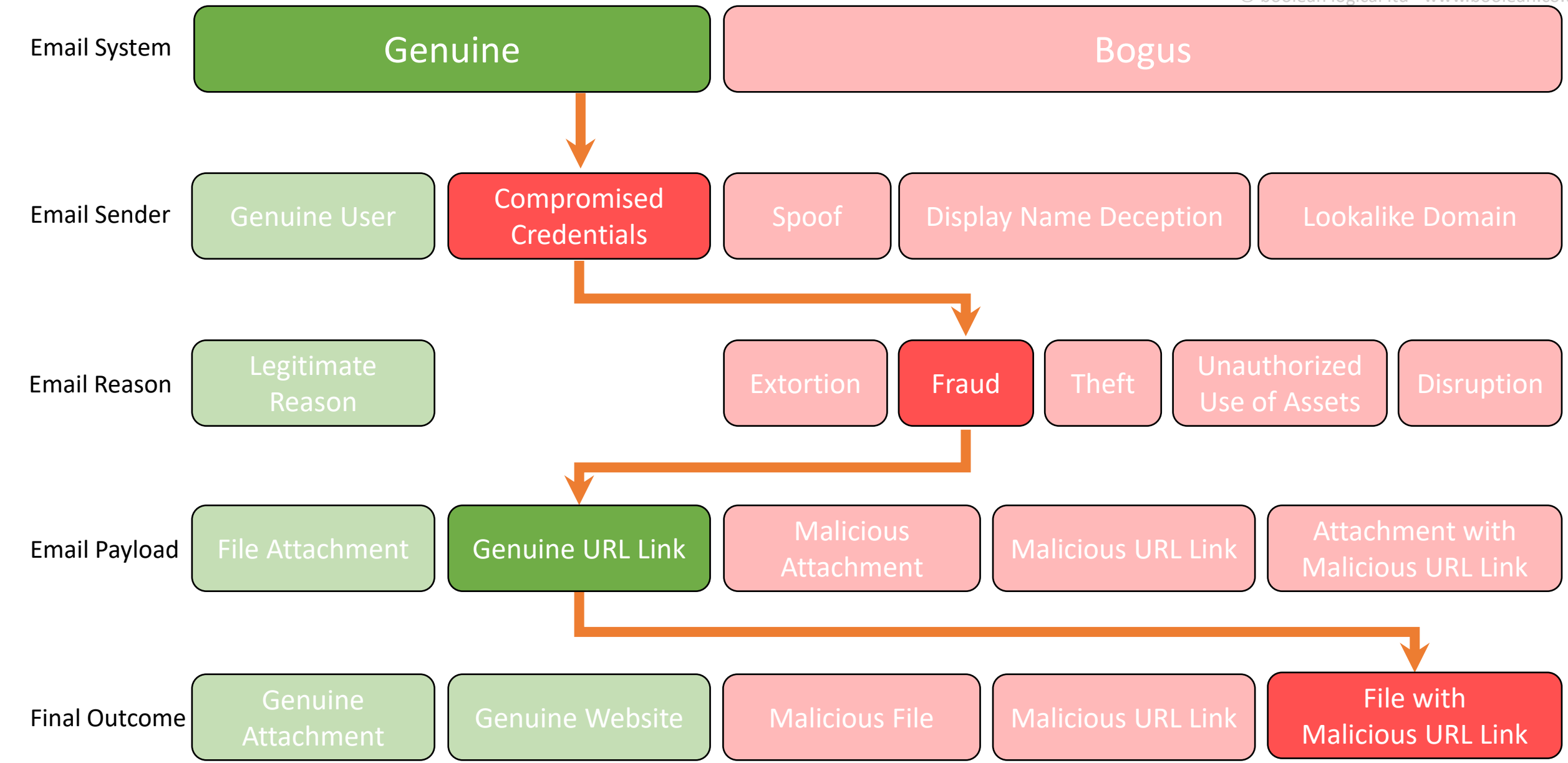
Social media is also an infection route

© boolean logical ltd - www.boolean.co.uk



Types of email

© boolean logical ltd - www.boolean.co.uk



Types of email

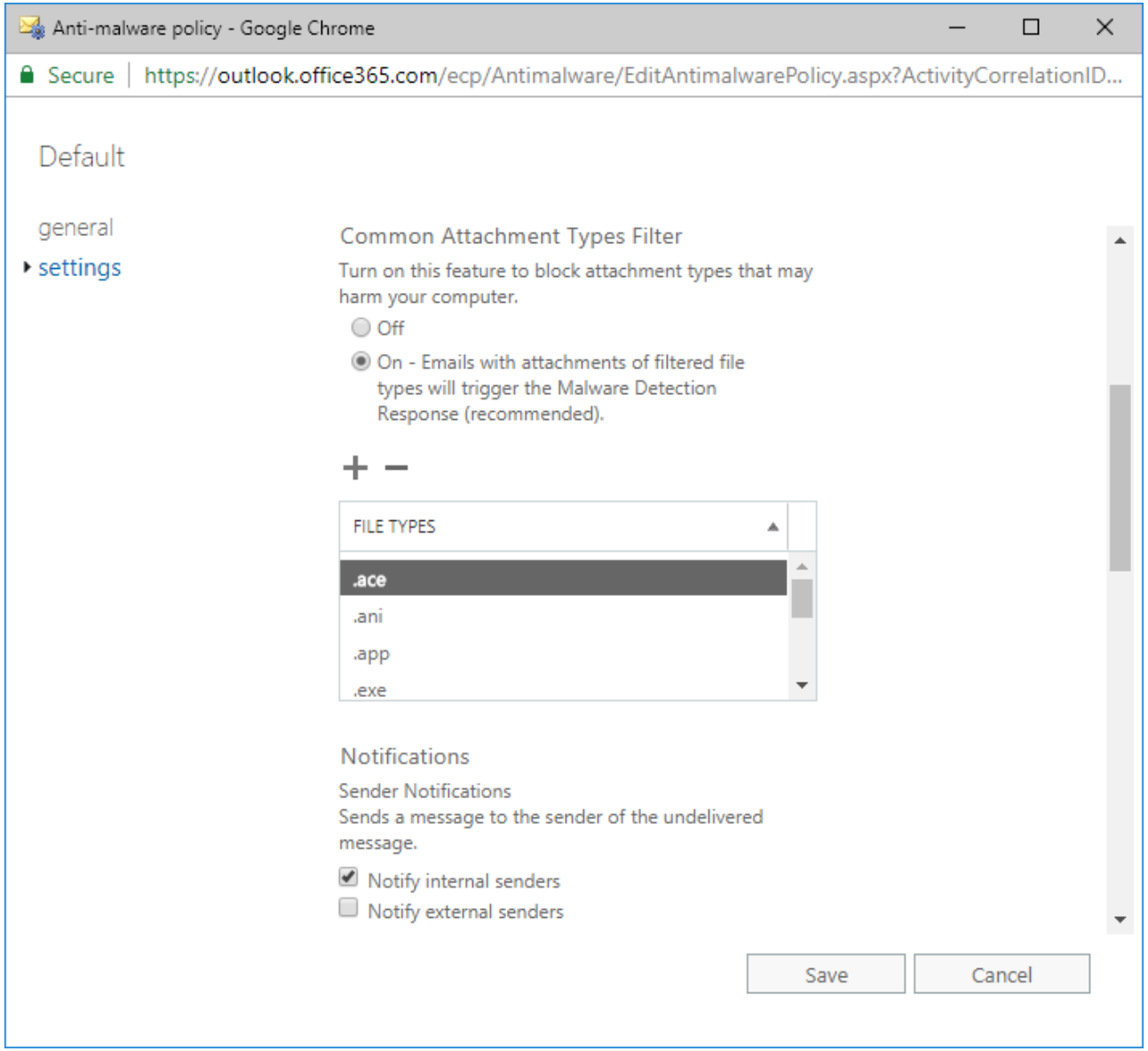
© boolean logical ltd - www.boolean.co.uk

Block or quarantine the following file types (unless you are web developers or programmers

.app	.arj	.bas	.bat	.cgi	.chm	.cmd
.com	.cpl	.dll	.exe	.hta	.inf	.ini
.ins	.iqy	.jar	.js	.jse	.lnk	.mht
.mhtm	.mhtml	.msi	.msh	.msh1	.msh2	.msh1xml
.msh2xml	.ocx	.pcd	.pif	.pl	.ps1	.pl
.ps1	.ps1xml	.ps2	.ps2xml	. psc1	.psc2	.py
.reg	.scf	.scr	.sct	.sh	.shb	.shs
.url	.vb	.vbe	.vbs	.vbx	.ws	.wsc
.wsf	.wsh					

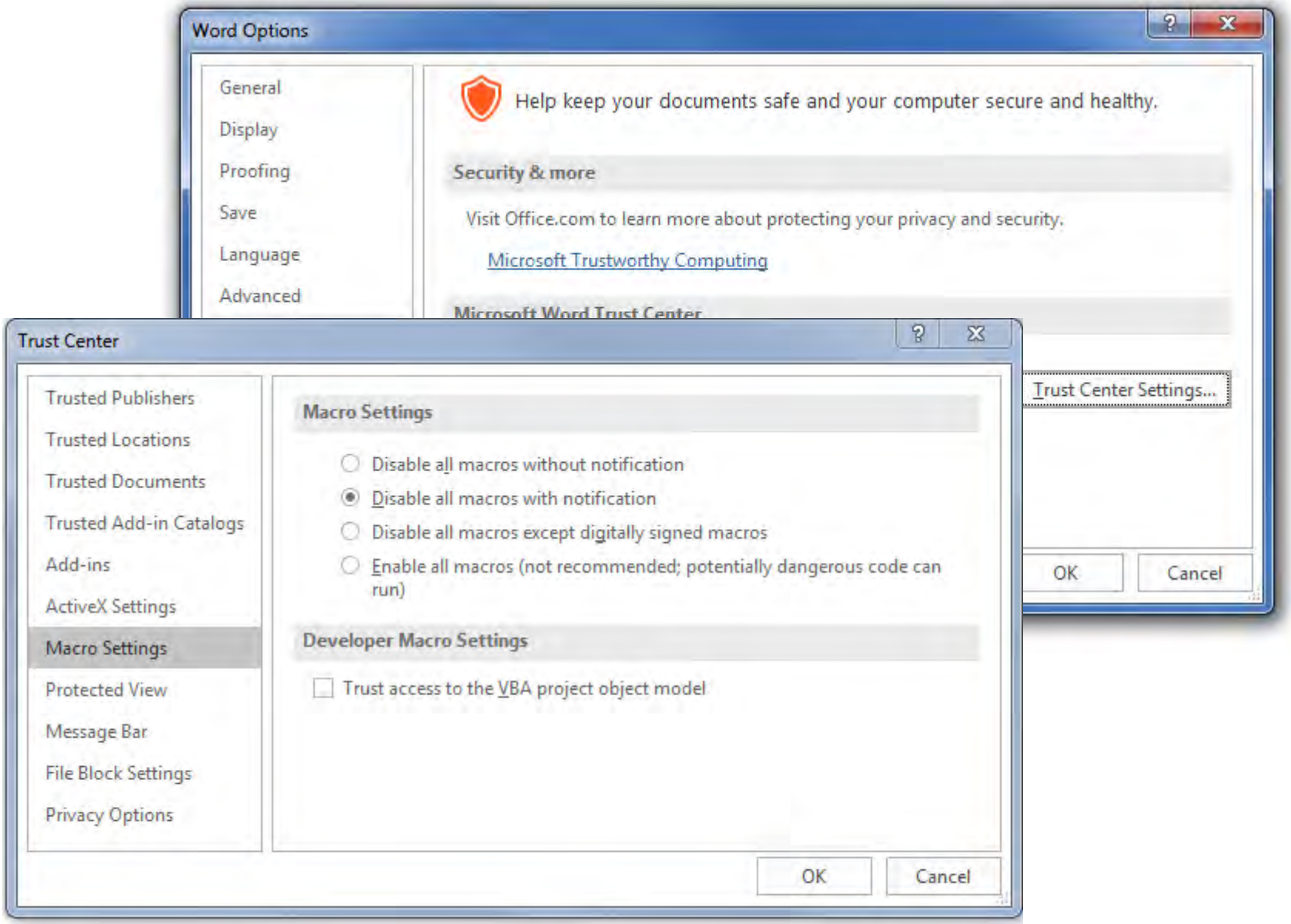
Quarantine the following macro-enabled office files

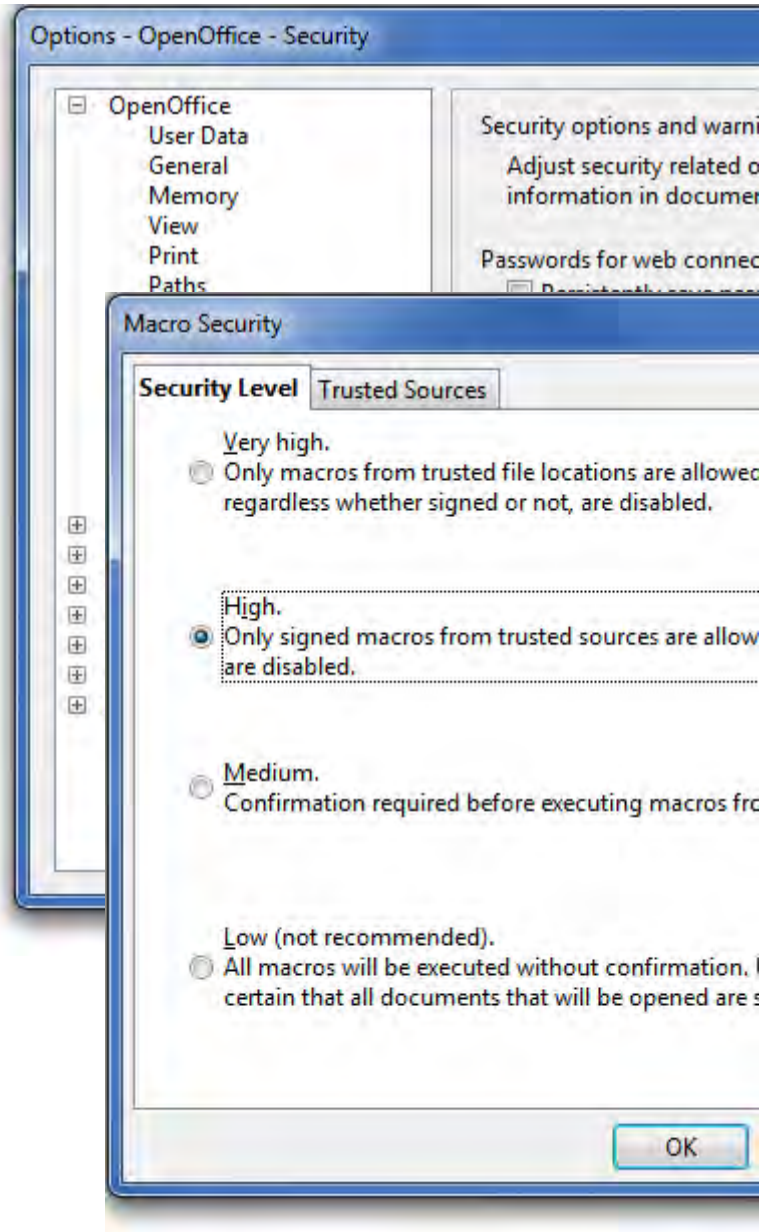
.docm	.dotm	.ppam	.potm	.ppsm	.pptm	.sldm
.xlam	.xlsm	.xltm				



Block uncommon attachment file types

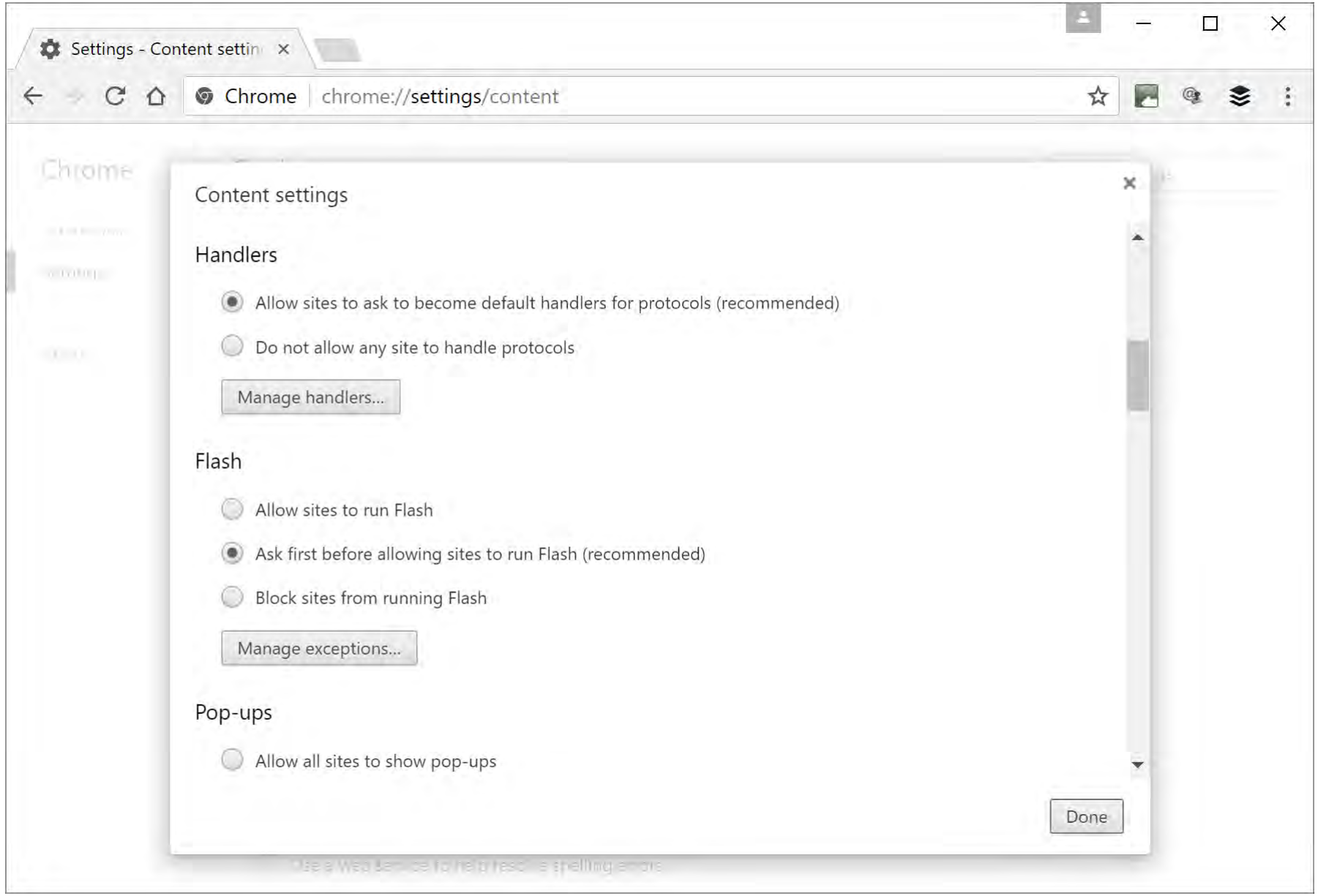
© boolean logical ltd - www.boolean.co.uk





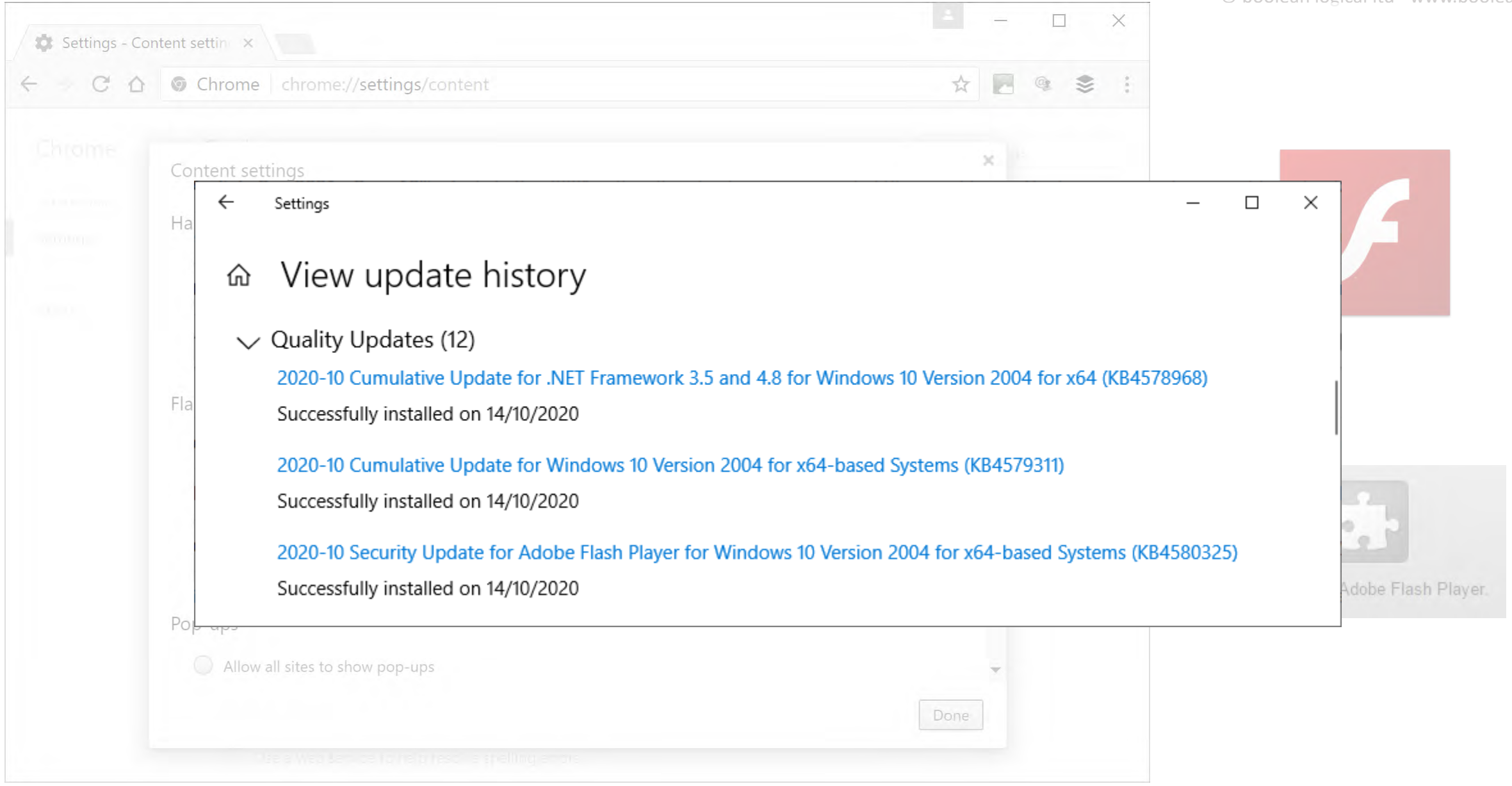
Disable Office Macros

© boolean logical ltd - www.boolean.co.uk



Stop Adobe Flash from automatically running

© boolean logical ltd - www.boolean.co.uk



Stop Adobe Flash from automatically running

© boolean logical ltd - www.boolean.co.uk

Java Releases	Release Date
Java 8 Update 271 CPU	October 20, 2020
Java 8 Update 261 CPU	July 14, 2020
Java 8 Update 251 CPU	April 14, 2020
Java 8 Update 241 CPU	January 14, 2020
Java 8 Update 231 CPU	October 15, 2019
Java 8 Update 221 CPU	July 16, 2019
Java 8 Update 211 CPU Java 8 Update 212 PSU (OTN)	April 16, 2019
Java 8 Update 201 CPU Java 8 Update 202 PSU (OTN)	January 15, 2019
Java 8 Update 191 CPU Java 8 Update 192 PSU (OTN)	October 16, 2018
Java 8 Update 181 CPU	July 17, 2018
Java 8 Update 171 CPU Java 8 Update 172 PSU (OTN)	April 17, 2018
Java 8 Update 161 CPU Java 8 Update 162 PSU (OTN)	January 16, 2018
Java 8 Update 151 CPU Java 8 Update 152 PSU (OTN)	October 17, 2017
Java 8 Update 144 Limited Update	July 26, 2017
Java 8 Update 141 CPU	July 18, 2017
Java 8 Update 131 CPU	April 18, 2017
Java 8 Update 121 CPU	January 17, 2017
Java 8 Update 111 CPU Java 8 Update 112 PSU (OTN)	October 18, 2016

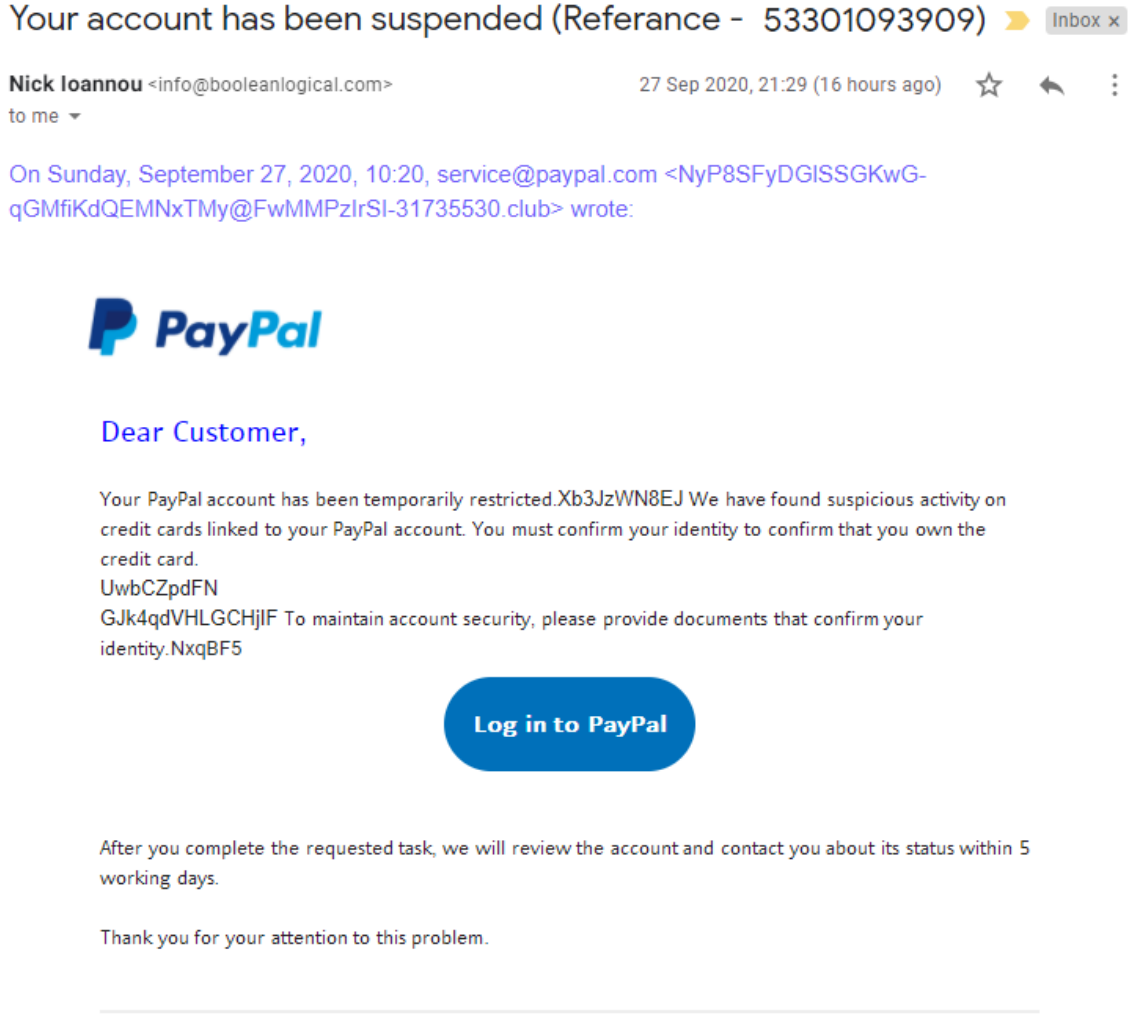
Java™

Java may appear in your programs list as:

J2SE, Java 2, Java SE or Java Runtime Environment

Remove Java if you have no obvious need for it

© boolean logical ltd - www.boolean.co.uk



Your account has been suspended (Referance - 53301093909) Inbox ×

Nick Ioannou <info@booleanlogical.com> 27 Sep 2020, 21:29 (16 hours ago)
to me

On Sunday, September 27, 2020, 10:20, service@paypal.com <NyP8SFyDGlSSGKwG-qGMfiKdQEMNxTMy@FwMMPzIrSI-31735530.club> wrote:

PayPal

Dear Customer,

Your PayPal account has been temporarily restricted.Xb3JzWN8EJ We have found suspicious activity on credit cards linked to your PayPal account. You must confirm your identity to confirm that you own the credit card.
UwbCZpdFN
GJk4qdVHLGCHjIF To maintain account security, please provide documents that confirm your identity.NxqBF5

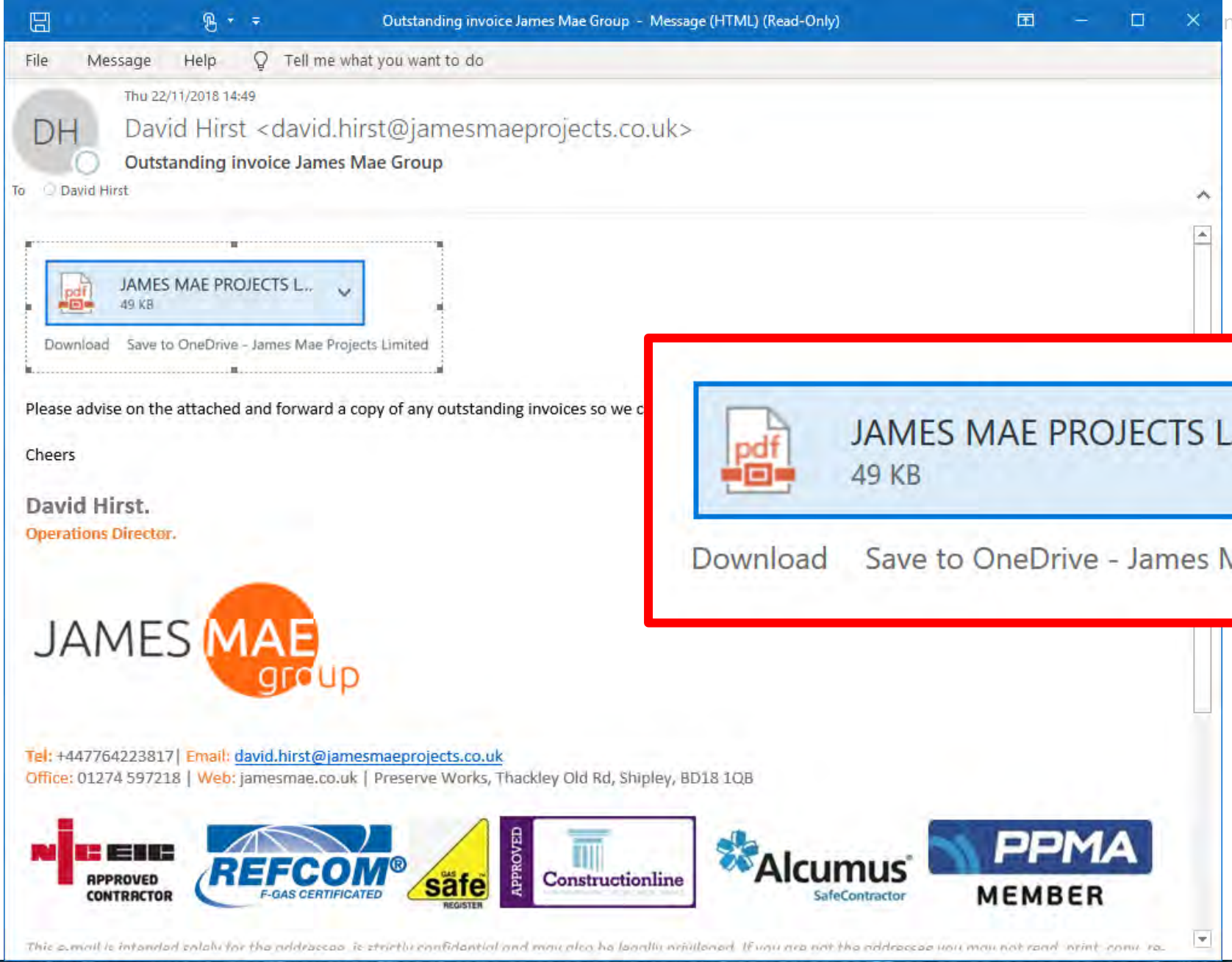
Log in to PayPal

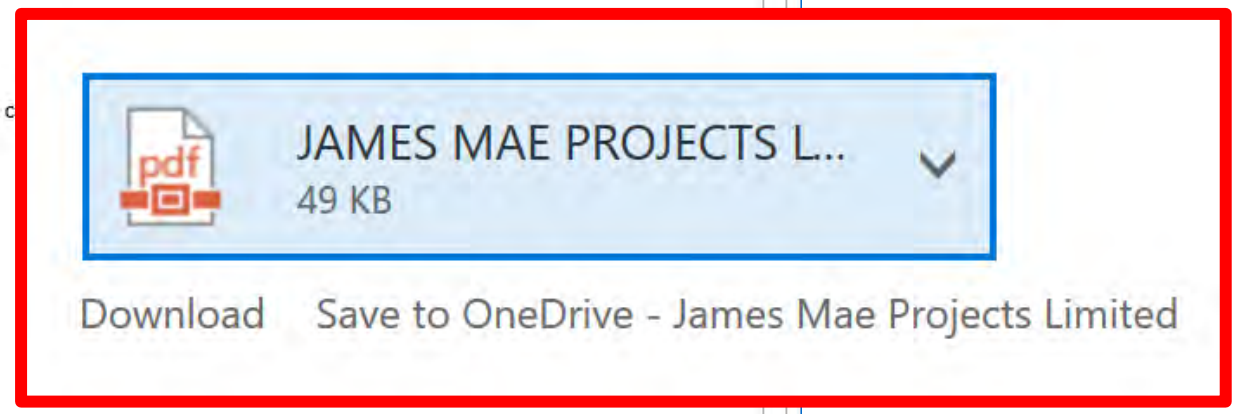
After you complete the requested task, we will review the account and contact you about its status within 5 working days.

Thank you for your attention to this problem.

https://www.linkedin.com/slink?code=d75ZAm7?Duarr=SupportHLGCHjIF-VcStjcDy?idtrack=DVVYLTCr

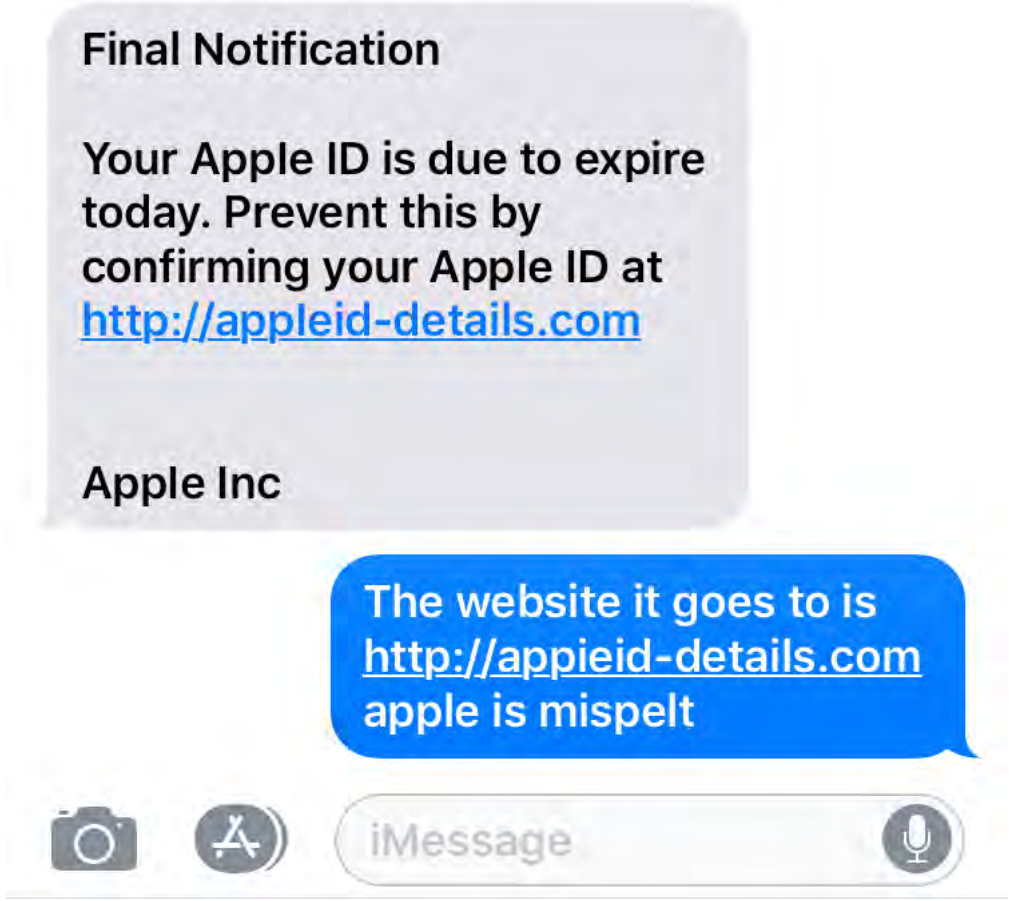
Hovering over the link doesn’t always help





Attachments may not actually be attachments

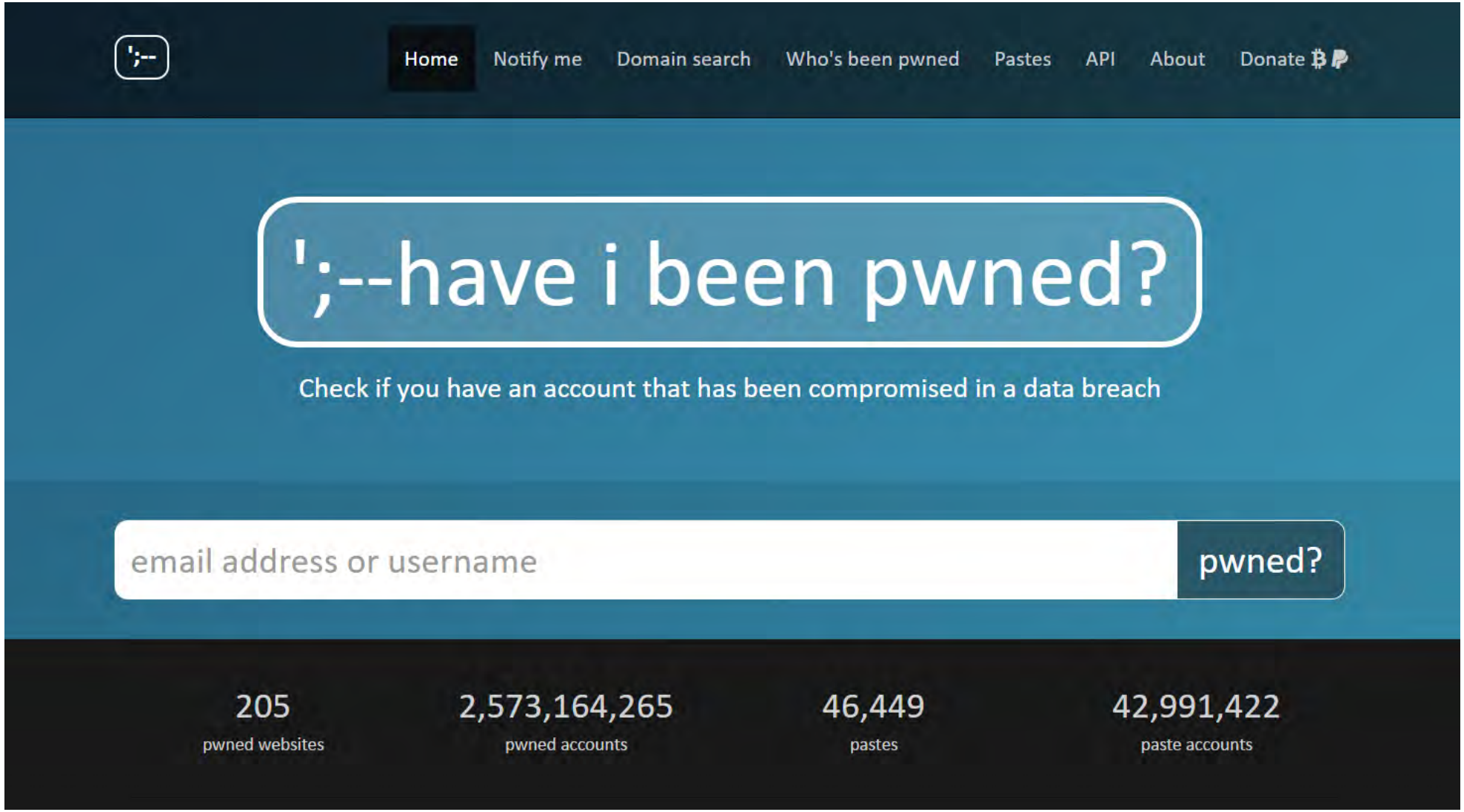
© boolean logical ltd - www.boolean.co.uk



What you see is not what you get!

© boolean logical ltd - www.boolean.co.uk

https://haveibeenpwned.com



Check if your email has been part of hack

© boolean logical ltd - www.boolean.co.uk

2 step verification logins

- plus -

Ping Identity

onelogin

dashlane

LastPass

okta

KEEPER

bitwarden

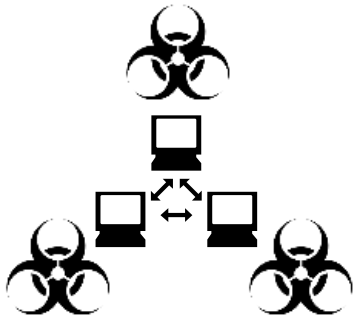
SECUREAUTH

my1login™
Connecting People, Apps and Devices

SecurEnvoy
A Shearwater Group plc Company

IAM / Single Sign-On & Multi-Factor Authentication

© boolean logical ltd - www.boolean.co.uk



The Criminal Opportunities Of Remote Working

© boolean logical ltd - www.boolean.co.uk

Your credentials are the keys to your cloud data

EE 12:50

30724323457528 - Parcel Deliv...

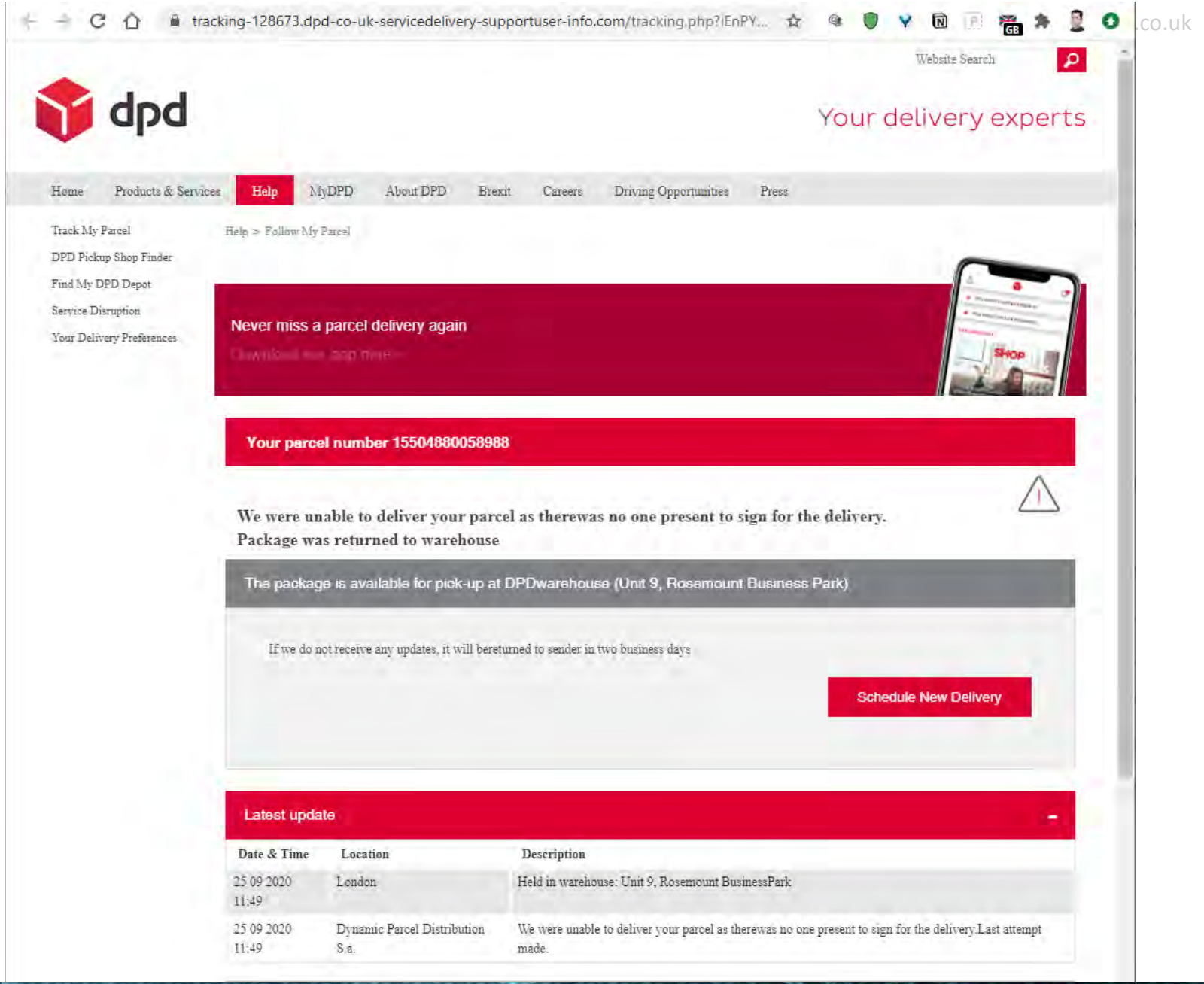
DPD (UK) - Delivery status
To n.ioannou@yahoo.co.uk
Today at 12:24

-Hello,n.ioannou@yahoo.co.uk

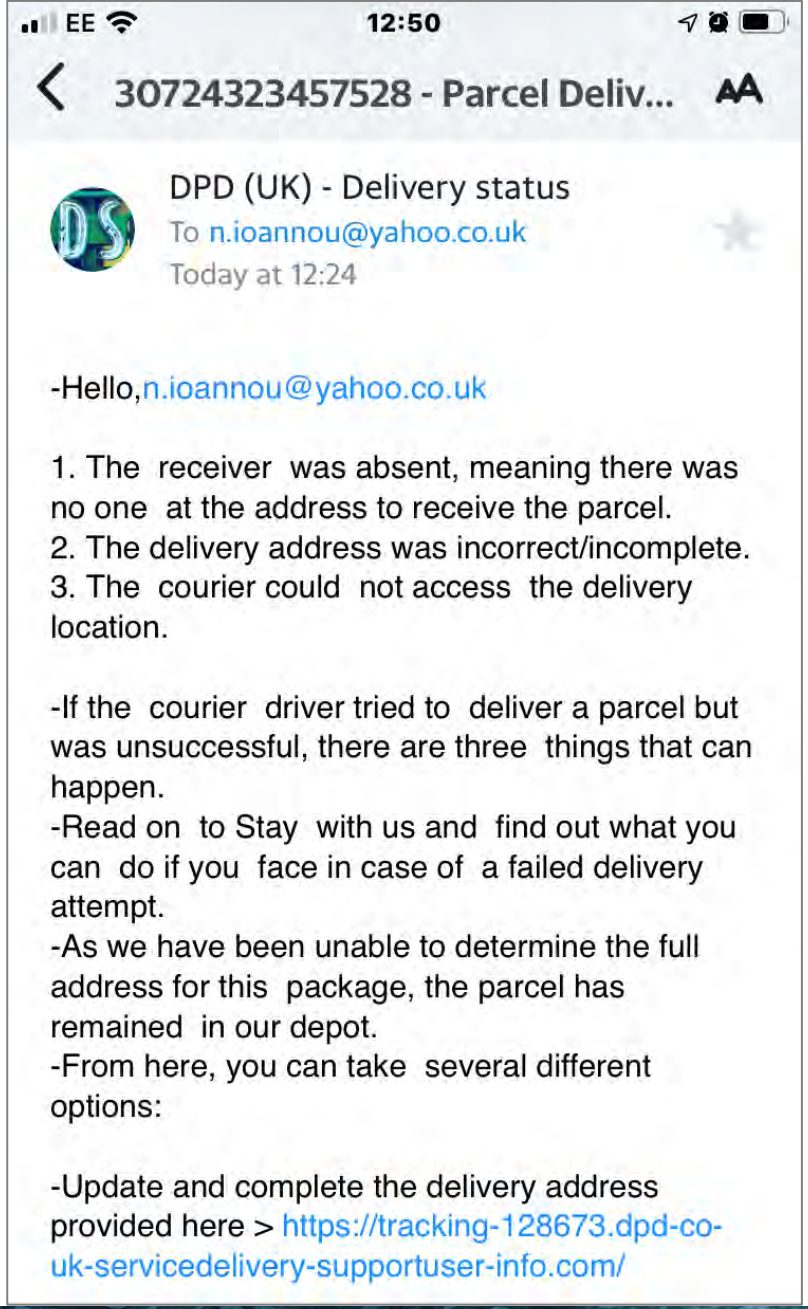
1. The receiver was absent, meaning there was no one at the address to receive the parcel.
2. The delivery address was incorrect/incomplete.
3. The courier could not access the delivery location.

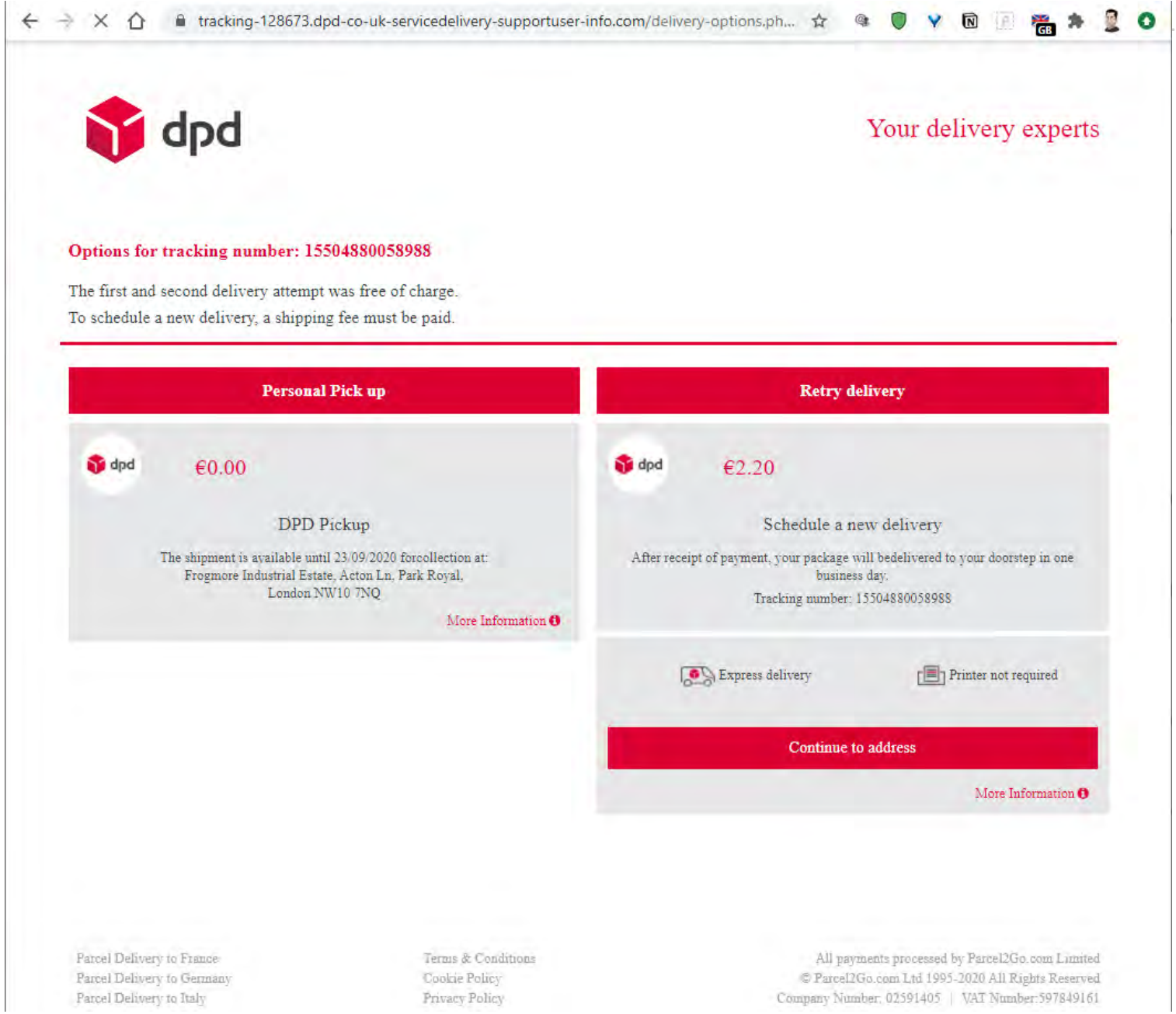
-If the courier driver tried to deliver a parcel but was unsuccessful, there are three things that can happen.
-Read on to Stay with us and find out what you can do if you face in case of a failed delivery attempt.
-As we have been unable to determine the full address for this package, the parcel has remained in our depot.
-From here, you can take several different options:

-Update and complete the delivery address provided here > https://tracking-128673.dpd-co-uk-servicedelivery-supportuser-info.com/



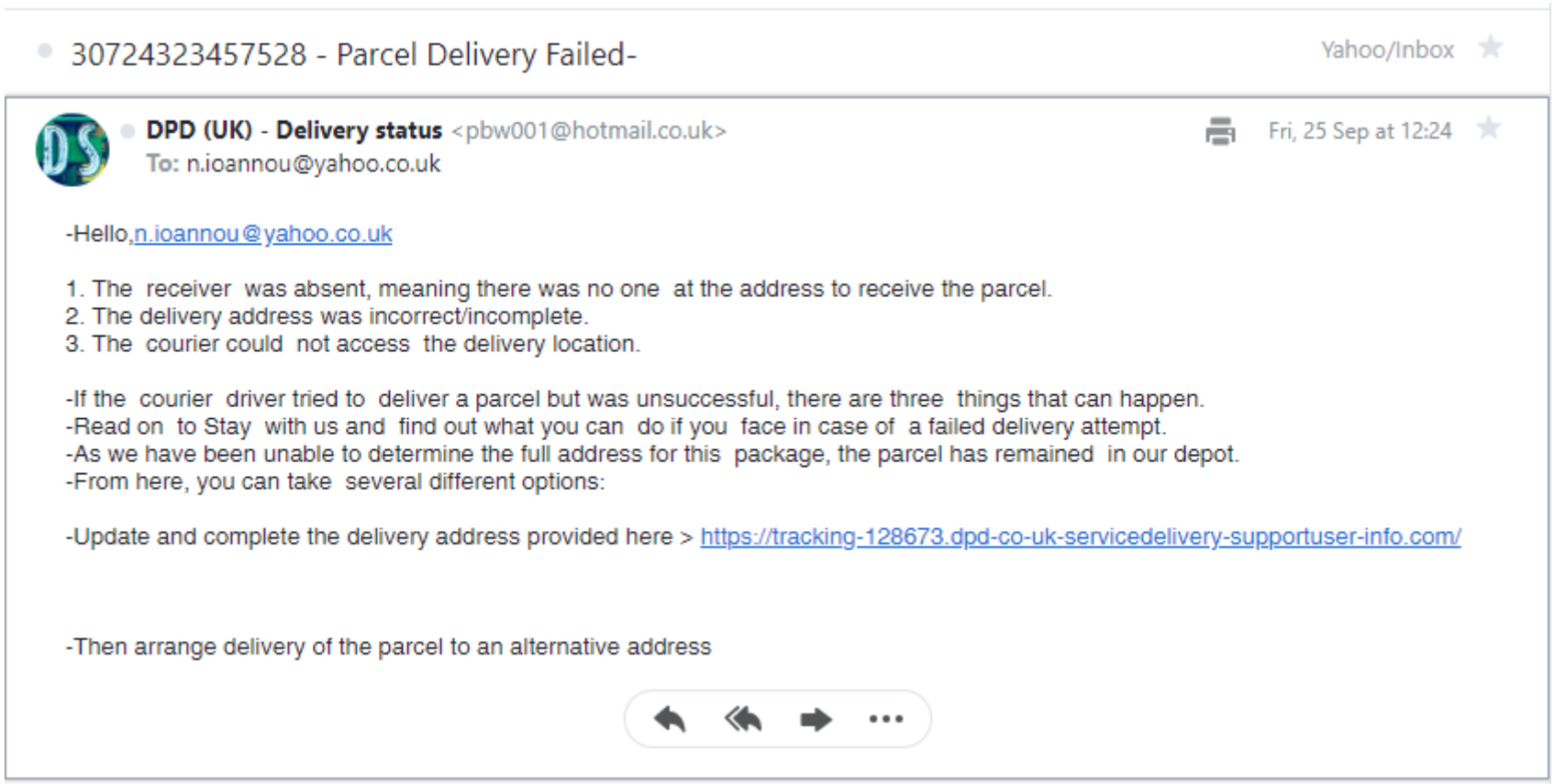
We Rely On Couriers More





We Rely On Couriers More

© boolean logical ltd - www.boolean.co.uk



30724323457528 - Parcel Delivery Failed-

Yahoo/Inbox

DPD (UK) - Delivery status <pbw001@hotmail.co.uk>
To: n.ioannou@yahoo.co.uk

Fri, 25 Sep at 12:24

-Hello,n.ioannou@yahoo.co.uk

1. The receiver was absent, meaning there was no one at the address to receive the parcel.
2. The delivery address was incorrect/incomplete.
3. The courier could not access the delivery location.

-If the courier driver tried to deliver a parcel but was unsuccessful, there are three things that can happen.
-Read on to Stay with us and find out what you can do if you face in case of a failed delivery attempt.
-As we have been unable to determine the full address for this package, the parcel has remained in our depot.
-From here, you can take several different options:

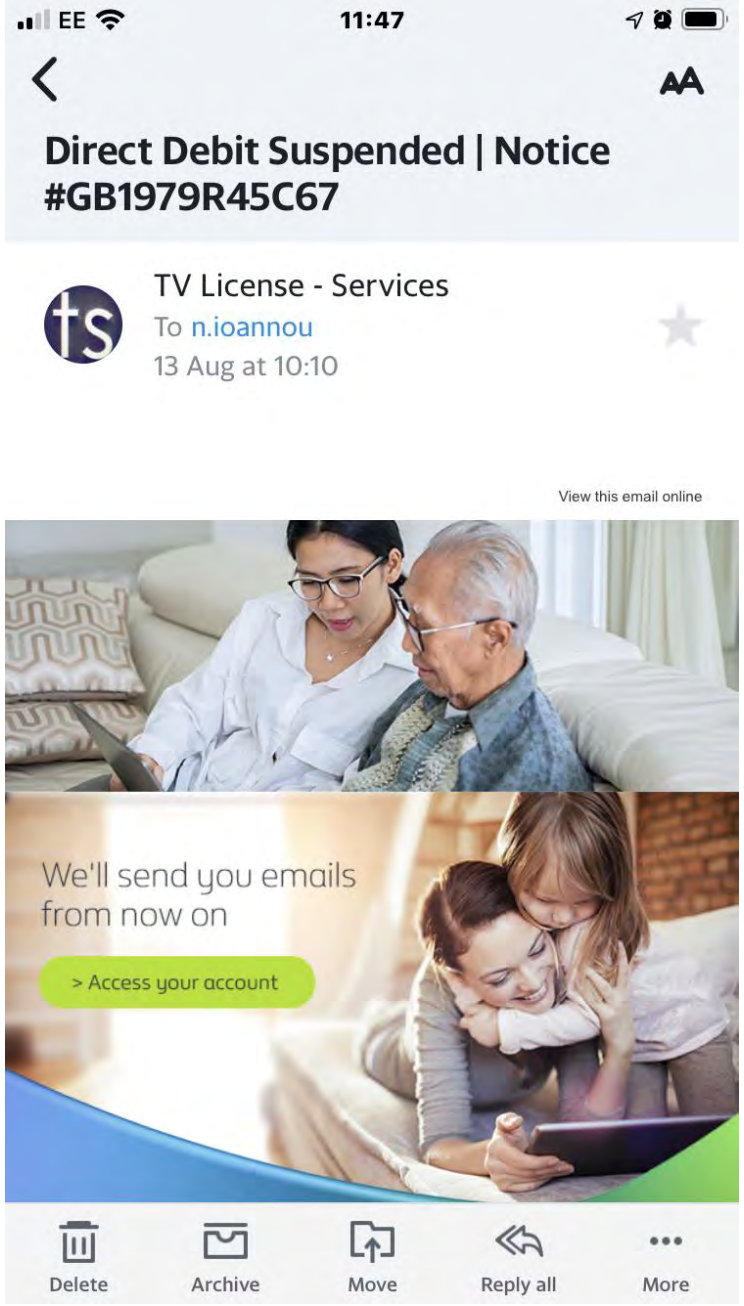
-Update and complete the delivery address provided here > https://tracking-128673.dpd-co-uk-servicedelivery-supportuser-info.com/

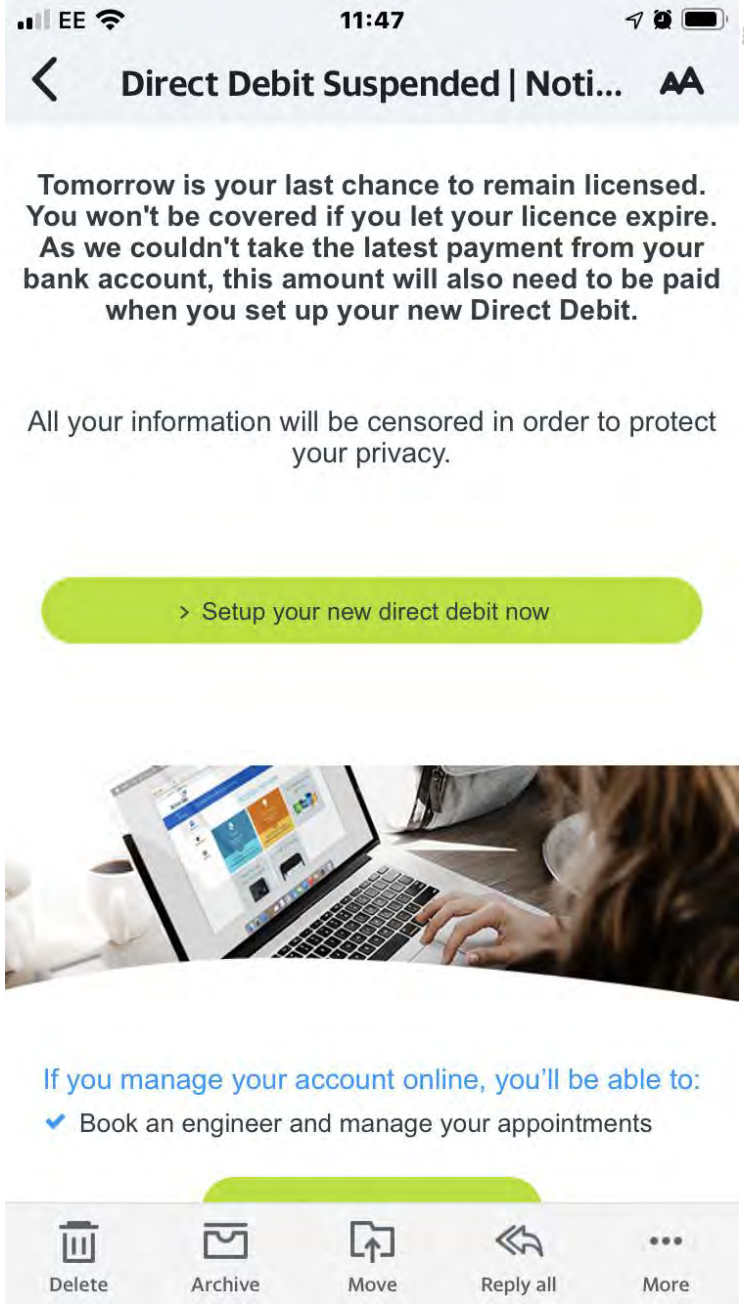
-Then arrange delivery of the parcel to an alternative address

https://tracking-128673.dpd-co-uk-servicedelivery-supportuser-info.com/tracking.php?

We Rely On Couriers More

gical ltd - www.boolean.co.uk





Common Hooks - Direct Debit Suspended

ean logical ltd - www.boolean.co.uk

An Update from our CEO

Yahoo/Inbox

Marriott International <marriottbonvoy@email-marriott.com> Unsubscribe

To: n.ioannou@yahoo.co.uk

Fri, 10 Apr at 12:35

Marriott INTERNATIONAL

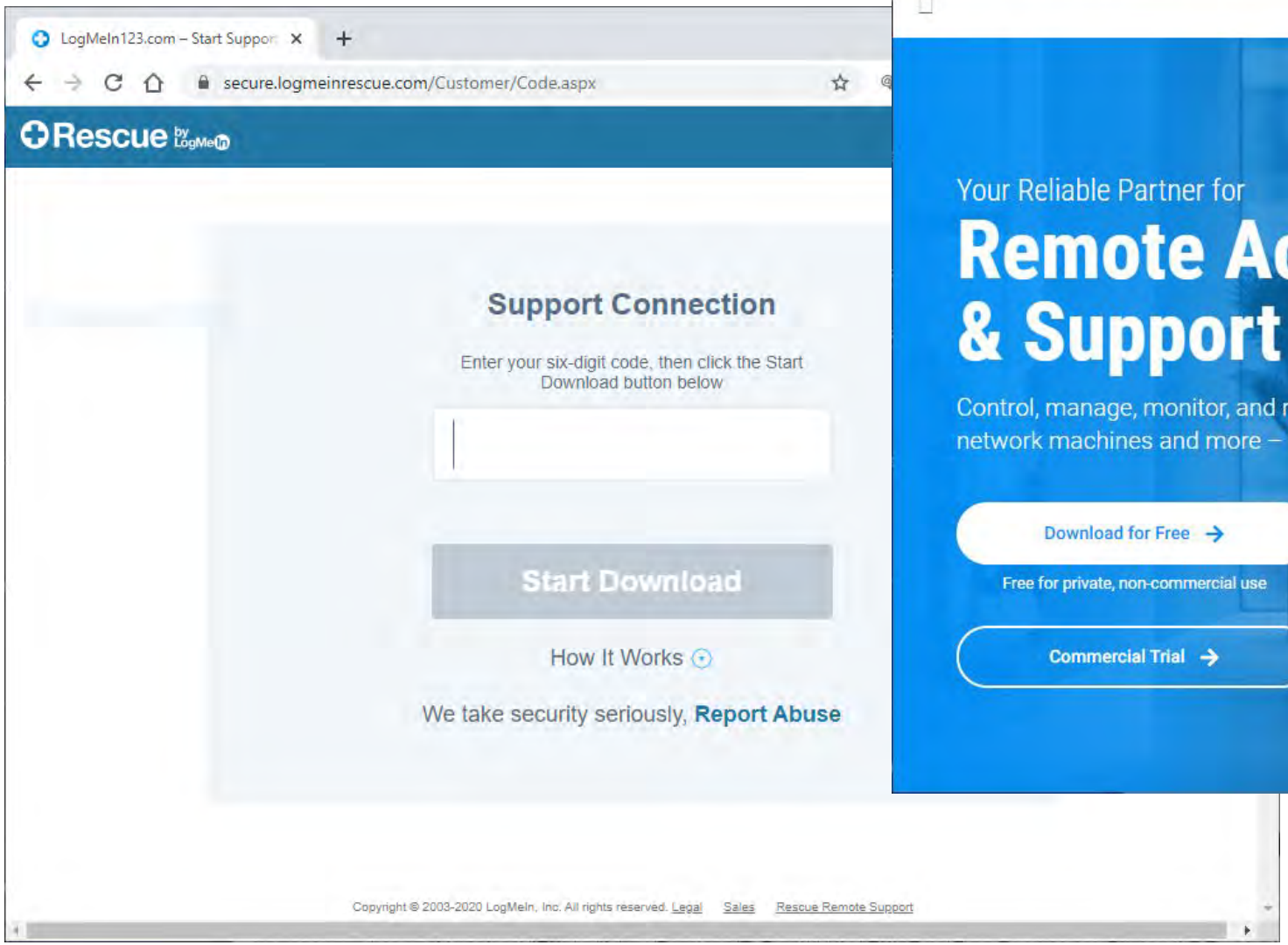
Dear Nick,

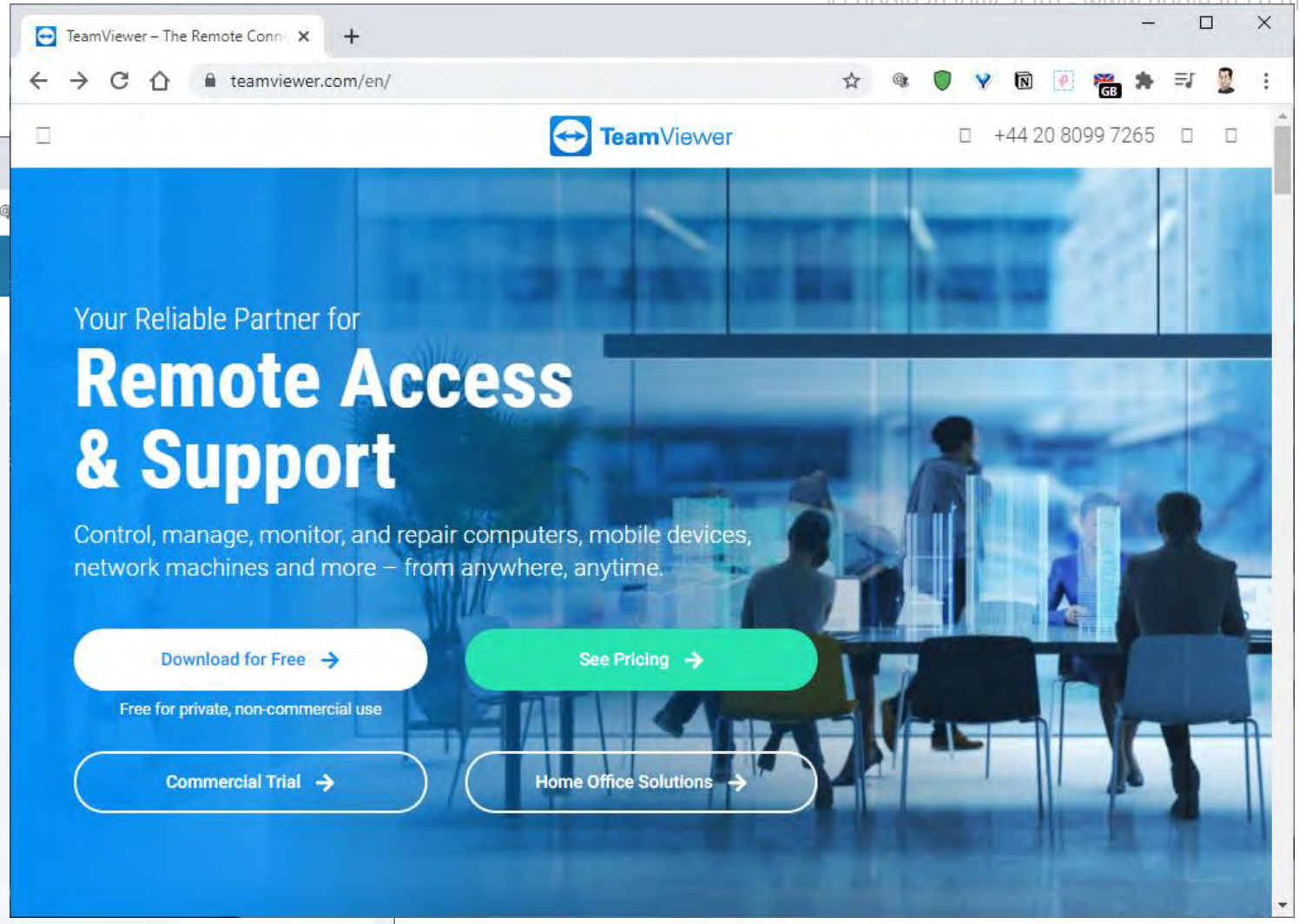
It's been three weeks since I last communicated with you about the dramatic impact of COVID-19 on our business. Sadly, since that time, we've all borne witness to how this insidious virus is impacting our families, our communities and our very way of life. What we're facing is daunting, but I am heartened by the moments of triumph in everyday acts of courage, humanity and love. Although these are trying times for us all, I remain optimistic that our world will thrive once again.

Today, I want to let you know how we're focused on supporting the communities where our associates live and work. I also want to provide you with an update on our room cancellation policy and Marriott Bonvoy status and points expiration dates.

Fake COVID-19 Updates

© boolean logical ltd - www.boolean.co.uk





Fake remote IT support

© boolean logical ltd - www.boolean.co.uk

Driver & Vehicle Licensing Agency

Dear Alice

All data transmission over this website is secured.

DVLA routine check has found some irregularities in your current profile, which indicates that the information given is no longer accurate or up to date.

You are required to update your profile to its latest form to avoid termination of your motoring licence.

You must use your valid and official information to complete this form. Using any nicknames or short-addresses can lead to rejection of this update.

Click Here and complete the required form

Yours sincerely
GOV.UK - Driver and Vehicle Licensing Agency

GoCompare

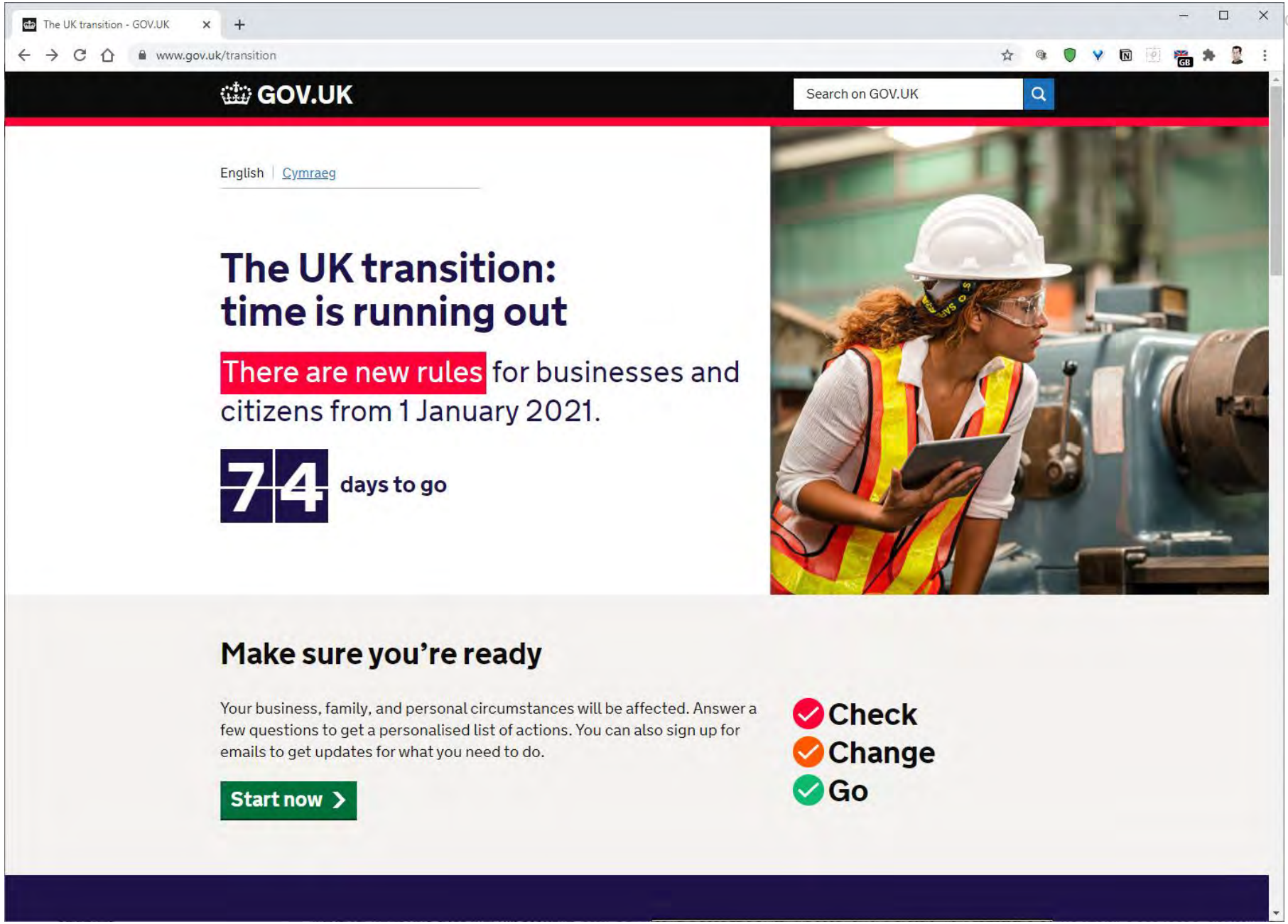
19 OCTOBER 2020, 11:33

Motorists warned to lookout for new lockdown car-related scams

- *New lockdown rules coupled with economic uncertainty, create perfect conditions for fraudulent activity.*
- *Motorists urged to guard against fake vehicle sales, insurance broker fraud, DVLA scams and staged car accident fraud.*
- *GoCompare shares tips to help people avoid falling victim to fraudsters.*

Increase in car related scams

cal ltd - www.boolean.co.uk



Fake BREXIT data protection updates

logical ltd - www.boolean.co.uk

Coronavirus: 'My name was used

bbc.co.uk/news/uk-54187581

Paused

BBC | Sign in | Home | News | Sport | Weather | iPlayer | Sounds | CBBC | CBeebies | More | Search

NEWS

Home | Coronavirus | US Election | UK | World | Business | Politics | Tech | Science | Health | Family & Education | More

UK | England | N. Ireland | Scotland | Alba | Wales | Cymru | Local News

Coronavirus: 'My name was used to steal a government Covid loan'

By Angus Crawford
BBC News

28 September

Coronavirus pandemic

Mark Telling's personal details were stolen to set up a bogus company

Top Stories

New Covid rescue scheme to pay up to half of wages

Chancellor Rishi Sunak increases support for firms and workers as lockdown restrictions spread.

42 minutes ago

Chancellor details amended plan to help firms and workers

7 hours ago

Stoke, Coventry and Slough to move into tier 2

11 minutes ago

Features

'We sold all our possessions to go live in a van'

COVID based ID theft scams

© boolean logical ltd - www.boolean.co.uk

Google Drive

OneDrive

iCloud

box

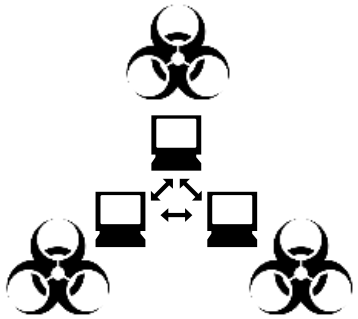
Dropbox

Encouraging the use of Shadow IT

© boolean logical ltd - www.boolean.co.uk

Reduced staff in the office

© boolean logical ltd - www.boolean.co.uk



Practical Steps To Level The Playing Field

© boolean logical ltd - www.boolean.co.uk

40%

infection rate if clicked

NIST

National Vulnerability Database – Sept 2020

110 known vulnerabilities in last 3 months

1637 known vulnerabilities in last 3 years

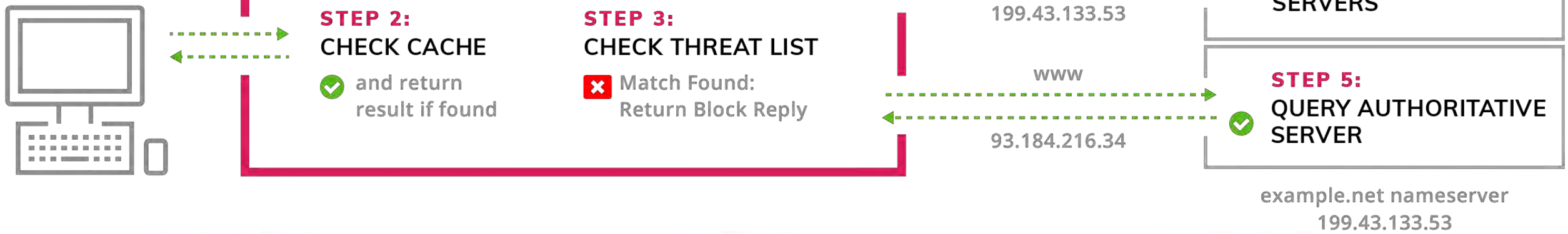
AUTOMATED EXPLOIT KITS ARE SOLD AS A WEB SERVICE BY CRIMINALS TO OTHER CRIMINALS

Flash	Java	Windows	IE	Acrobat	Silverlight
2	11	32	10	55	0
45	147	382	179	881	3

We are still at risk due to software vulnerabilities

© boolean logical ltd - www.boolean.co.uk

Quad9



60M

Average of 60M
Daily Blocks

18+

Number of Threat
Intelligence Providers

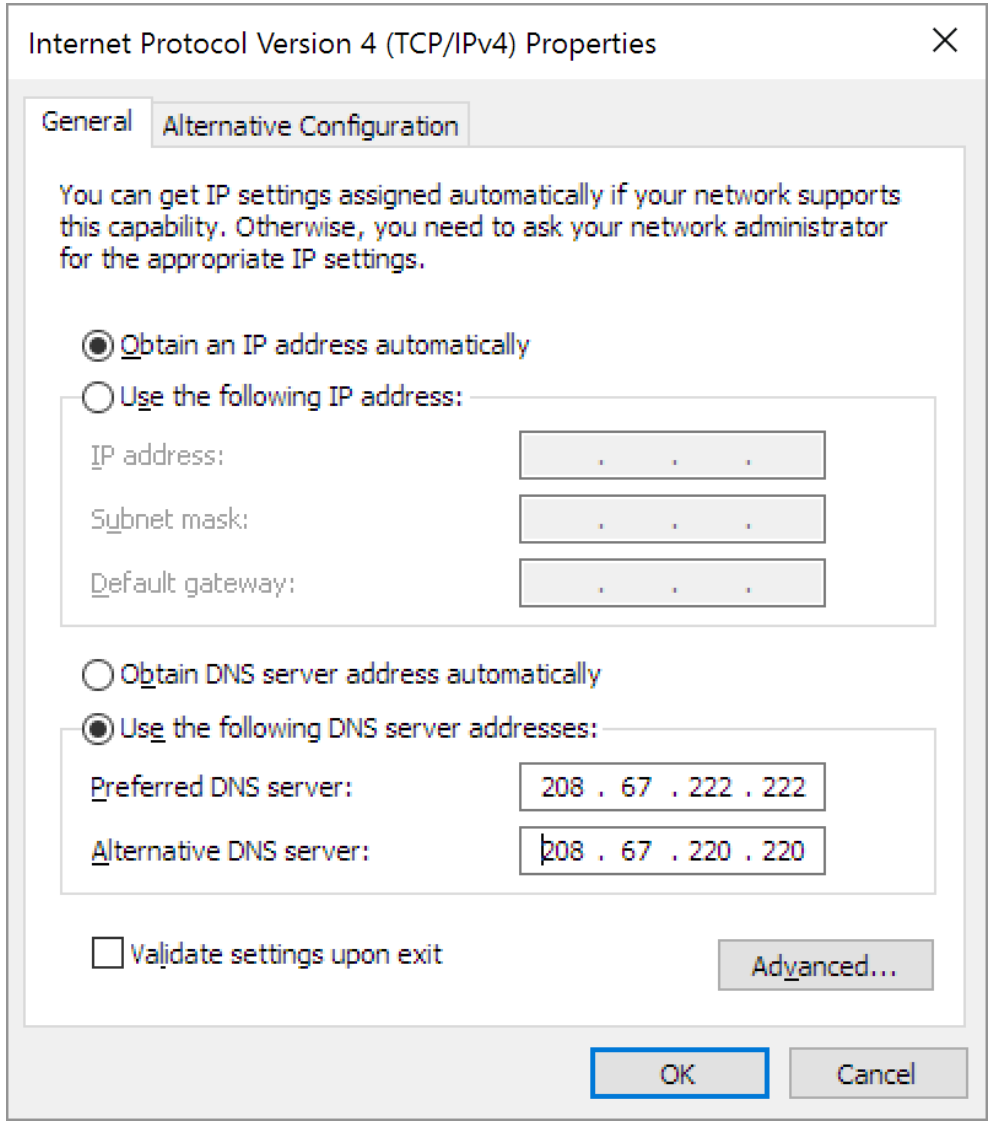
150

Active
Resolver Clusters in 90 countries

All data as of 6/01/20

FREE DNS Filtering

© boolean logical ltd - www.boolean.co.uk



OpenDNS

cisco Cisco Umbrella

208.67.222.222 + 208.67.220.220

FamilyShield

Preconfigured to block adult content

208.67.222.123 + 208.67.220.123

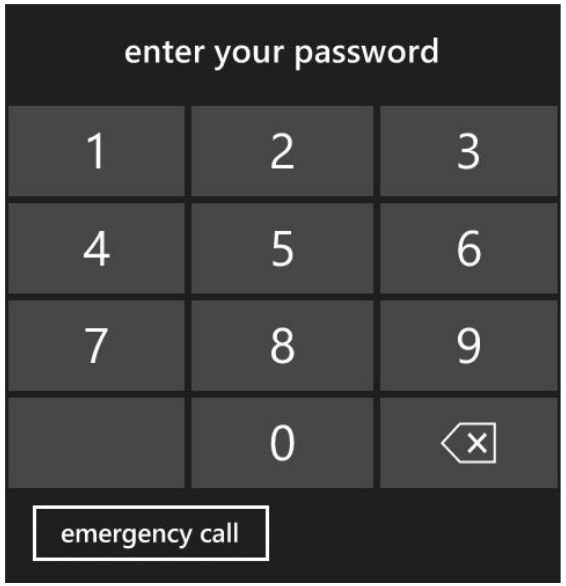
www.opendns.com

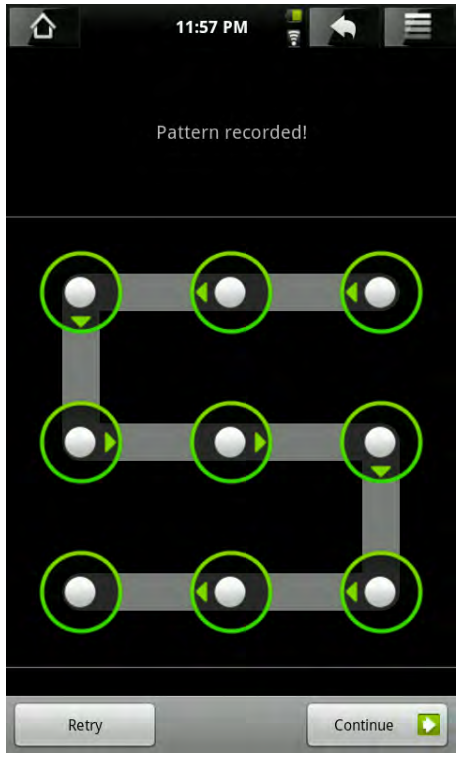
FREE DNS filtering

© boolean logical ltd - www.boolean.co.uk

Protect yourself with a VPN (Virtual Private Network)

© boolean logical ltd - www.boolean.co.uk

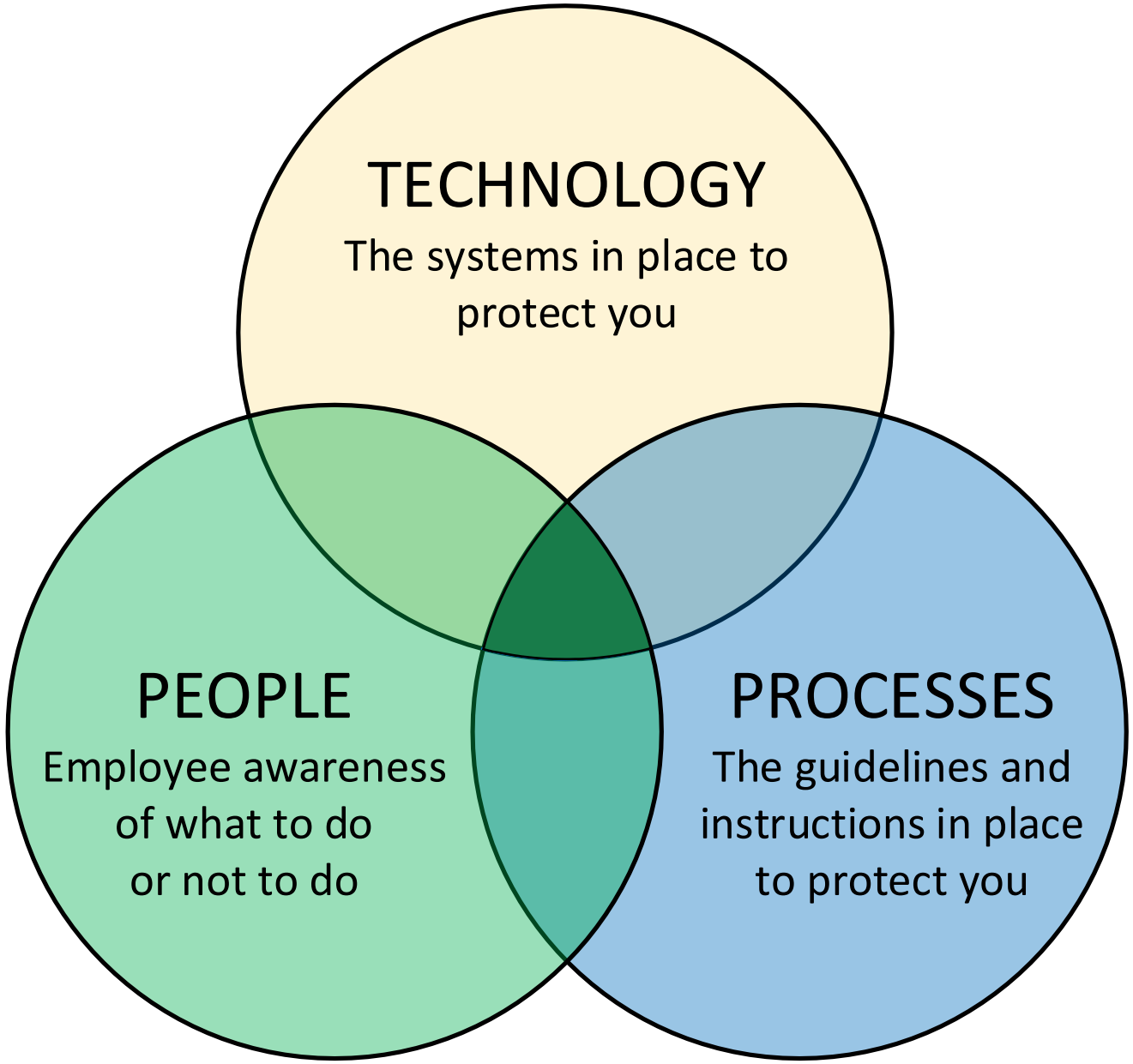




Avoid 1234, 1111, 0000,
4321 & 1010 and
your year of birth

Don’t Forget The Basics of Device Security

© boolean logical ltd - www.boolean.co.uk



It’s not just about the technology

© boolean logical ltd - www.boolean.co.uk

9 areas for true cover

© boolean logical ltd - www.boolean.co.uk

www.nist.gov/cyberframework

NIS Objectives							
A: Managing security risk		B: Protecting against cyber attack		C: Detecting cyber security incidents		D: Minimising the impact of cyber security incidents	
NIS Principles							
A1: Governance	A2: Risk management	B1: Service protection policies and processes	B2: Identity and access control	C1: Security monitoring	C2: Proactive security event discovery	D1: Response and recovery planning	D2: Lessons learned
A3: Asset management	A4: Supply chain	B3: Data security	B4: System security				
		B5: Resilient networks and systems	B6: Staff awareness and training				

Cyber Assessment Framework (CAF)

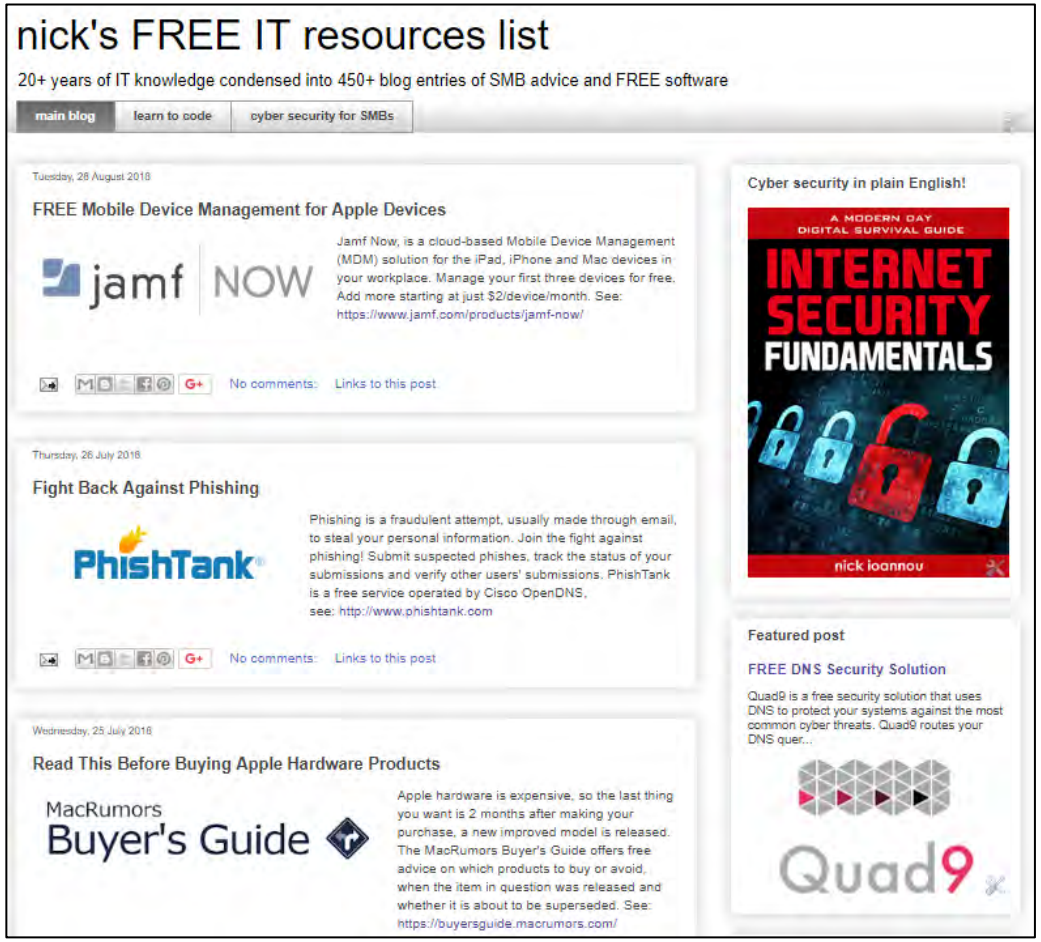
Does your Framework & Incident Response still work?

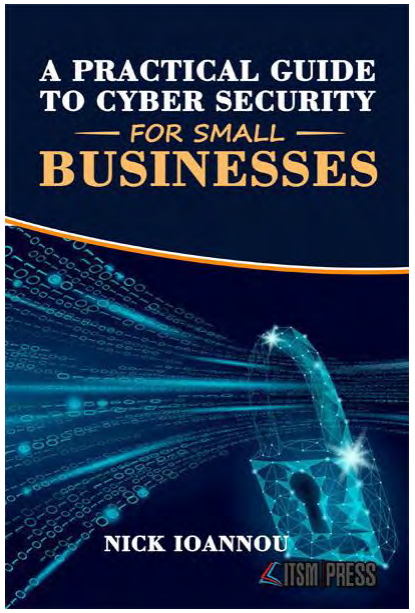
© boolean logical ltd - www.boolean.co.uk

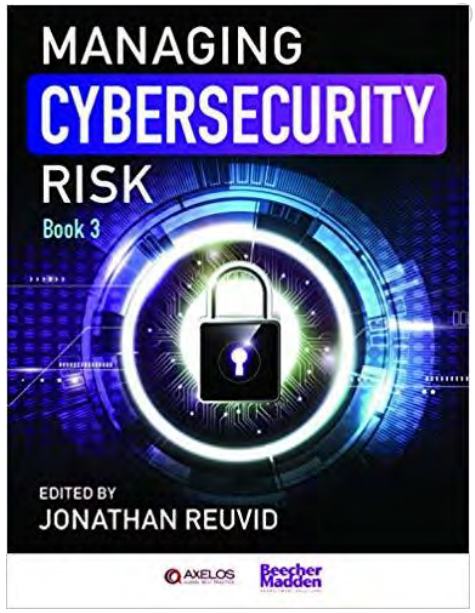
Are you buying this?

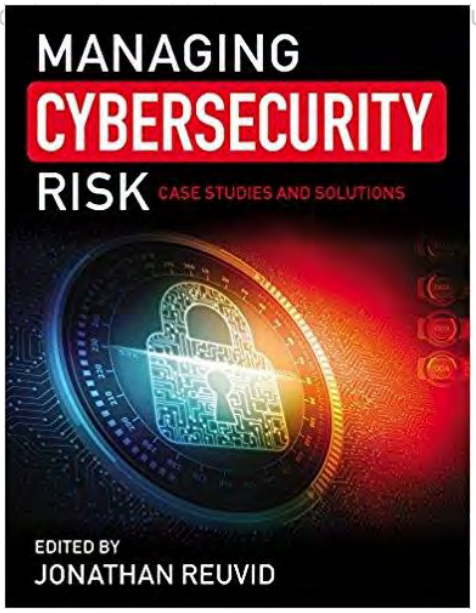
When you really need these!

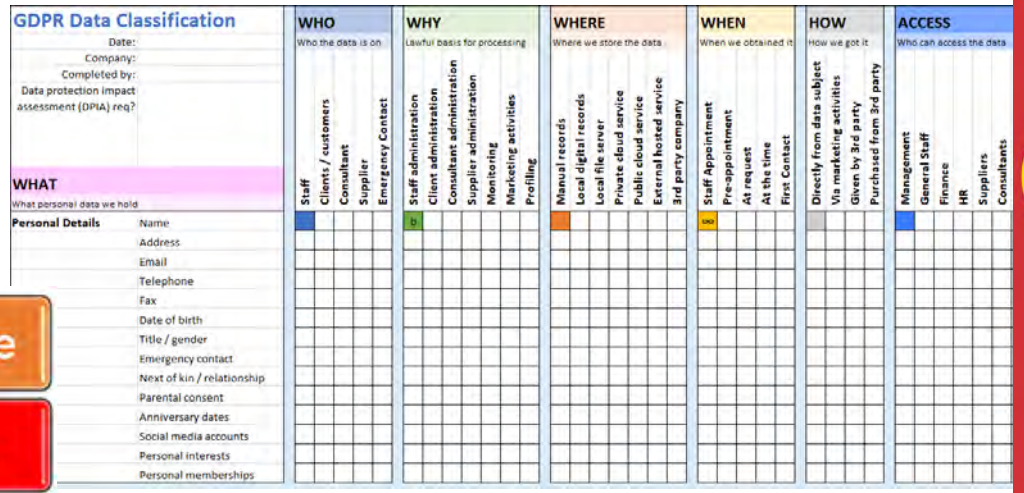
Spend your security budget wisely

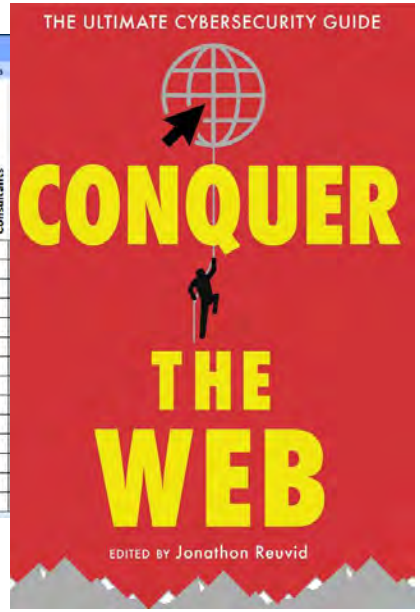












For more security resources and advice see:

www.boolean.co.uk