Ignorance Is No Defence

Cyber-crime – Will it really affect me?

Identity Theft Typically Private

Copyright Theft Typically Commercial

Personal Data Theft Typically Private and Commercial

Fraud Typically Private and Commercial

Denial of Service & Ransomware Typically Commercial

JPMorgan Chase & Co.

Anthem.

TalkTalk

ABTA
The Travel Association

Carphone Warehouse

in

target data

KASPERSKY lab

wonga.com

NETFLIX

moonpig.com

YAHOO!

BRITISH AIRWAYS

RSA

SONY

Cyber-crime Is Flourishing!

But it is not just the big guys

SMEs in every sector are under attack from Ransomware, Hacking & Fraud

Accountants, Builders, Charities, Construction Firms, Estate Agents, Financial Advisers, Funeral Directors, Hi-tech Firms, Insurance Brokers & Companies*, IT Firms, Landlords & Property Owners, Local Councils & Government Agencies, Manufacturers, Motor Trade, NHS, Pharmaceuticals, Retailers, Solicitors, Surveyors, Transportation Firms…to name some*

Throughout the country

Cyber-crime Is Flourishing!

We only hear about the BIG cyber-crime cases

But there are many more small ones

SMEs are an easier target for cyber criminals

Cyber-crime Is Flourishing!

SME cyber-crime remains hidden

Seeing is believing

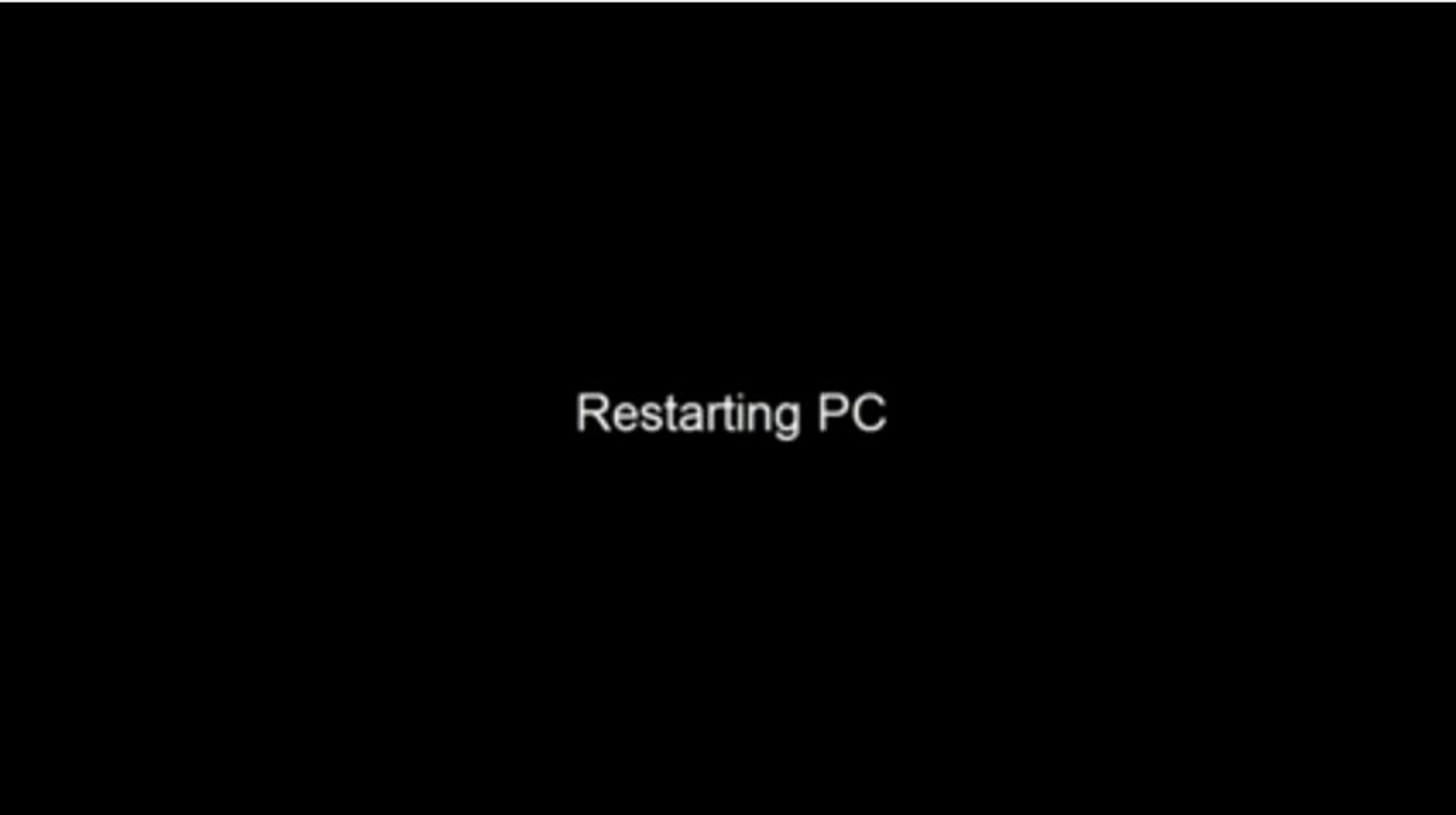
We are too small to matter

Good Luck!

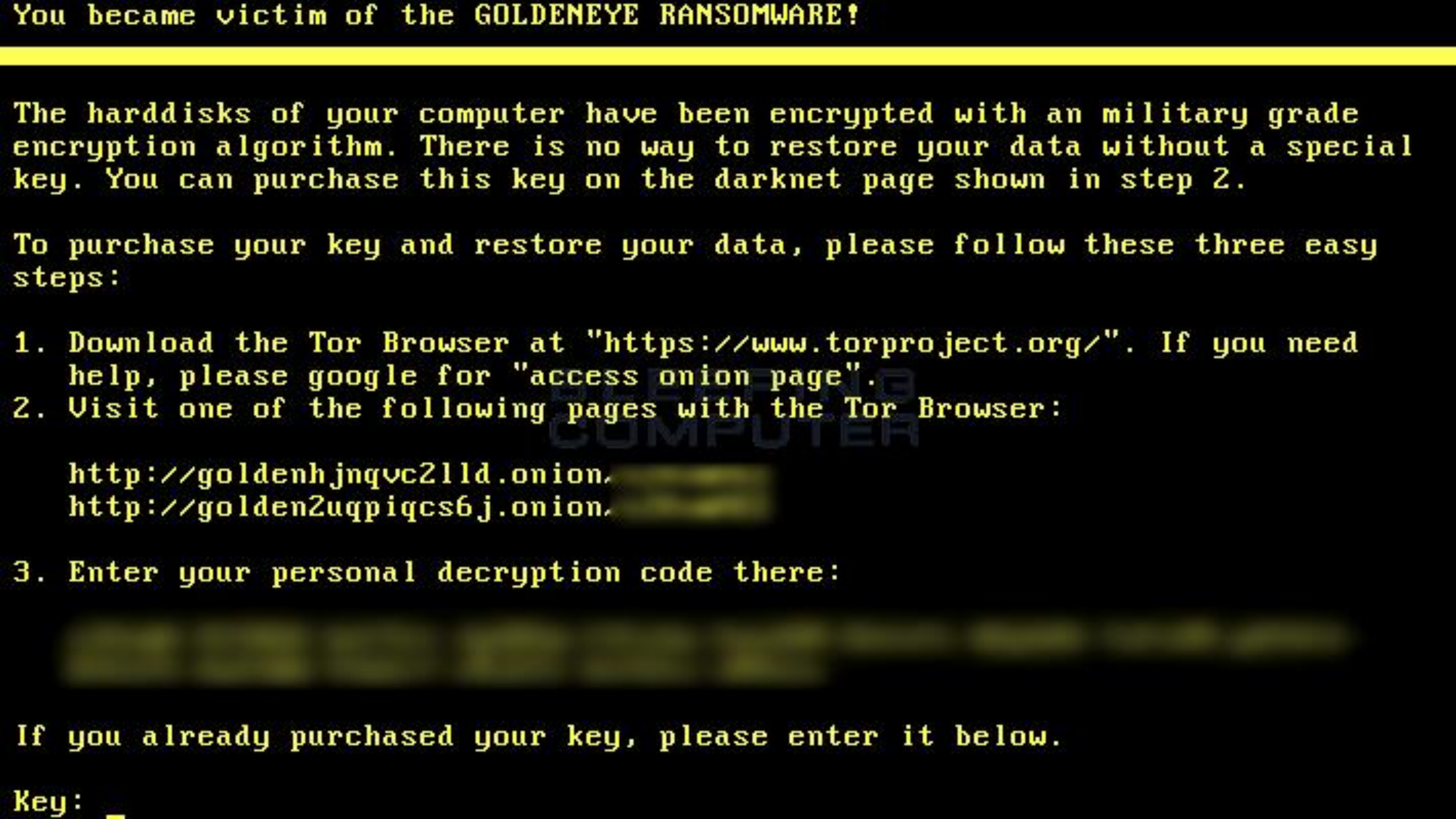
The Risks Are Real

It is just not worth the risk

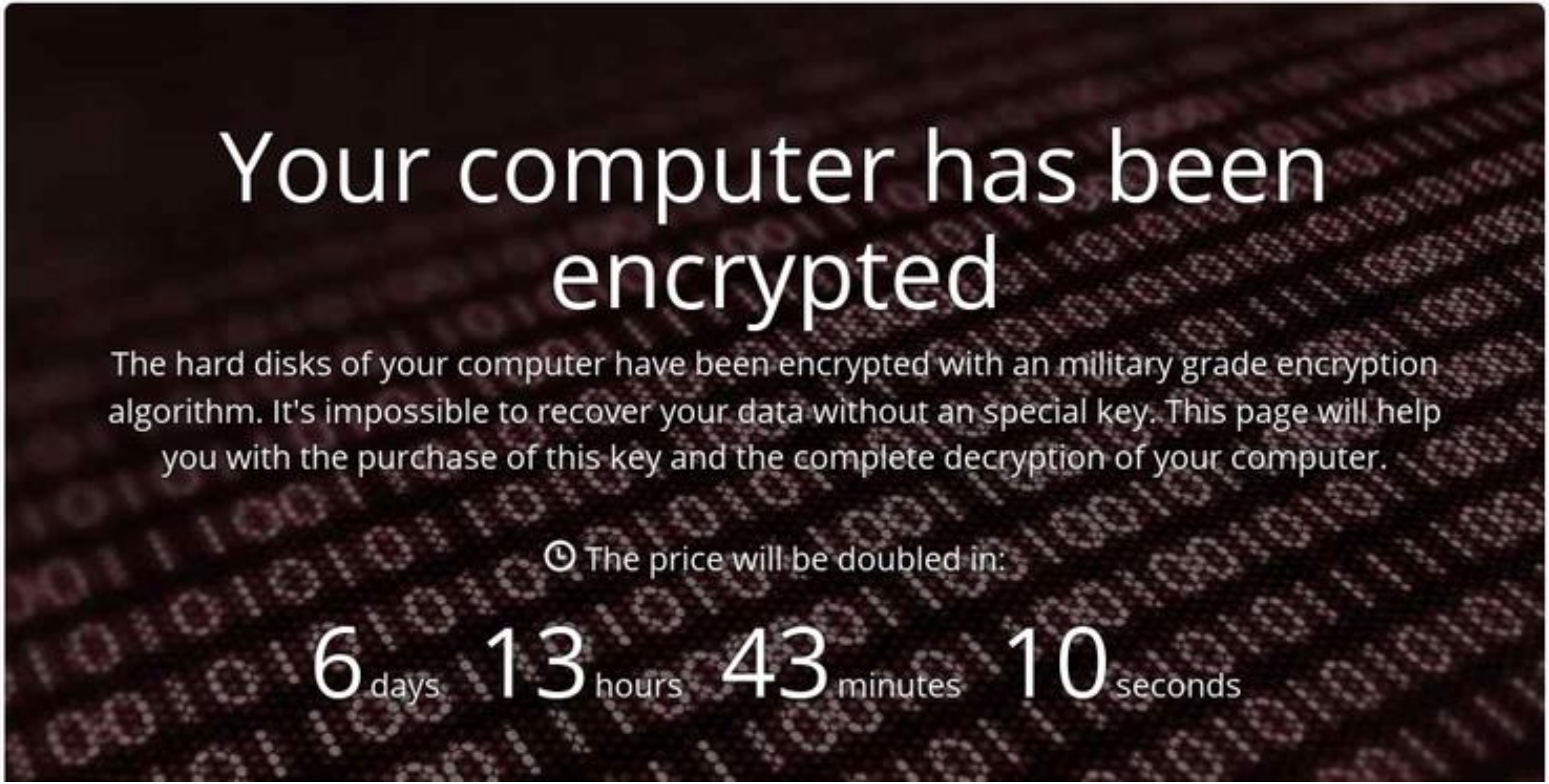
Cyber-crime is already forcing firms out of business



Restarting PC



```
You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://goldenhjnqvc2lld.onion/[redacted]
   http://golden2uqpiqcs6j.onion/[redacted]

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key: _
```



Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

The price will be doubled in:

6 days 13 hours 43 minutes 10 seconds

Ransomware Threats

Encrypting data

Preventing access to some or all data

Demanding a ransom in bitcoins

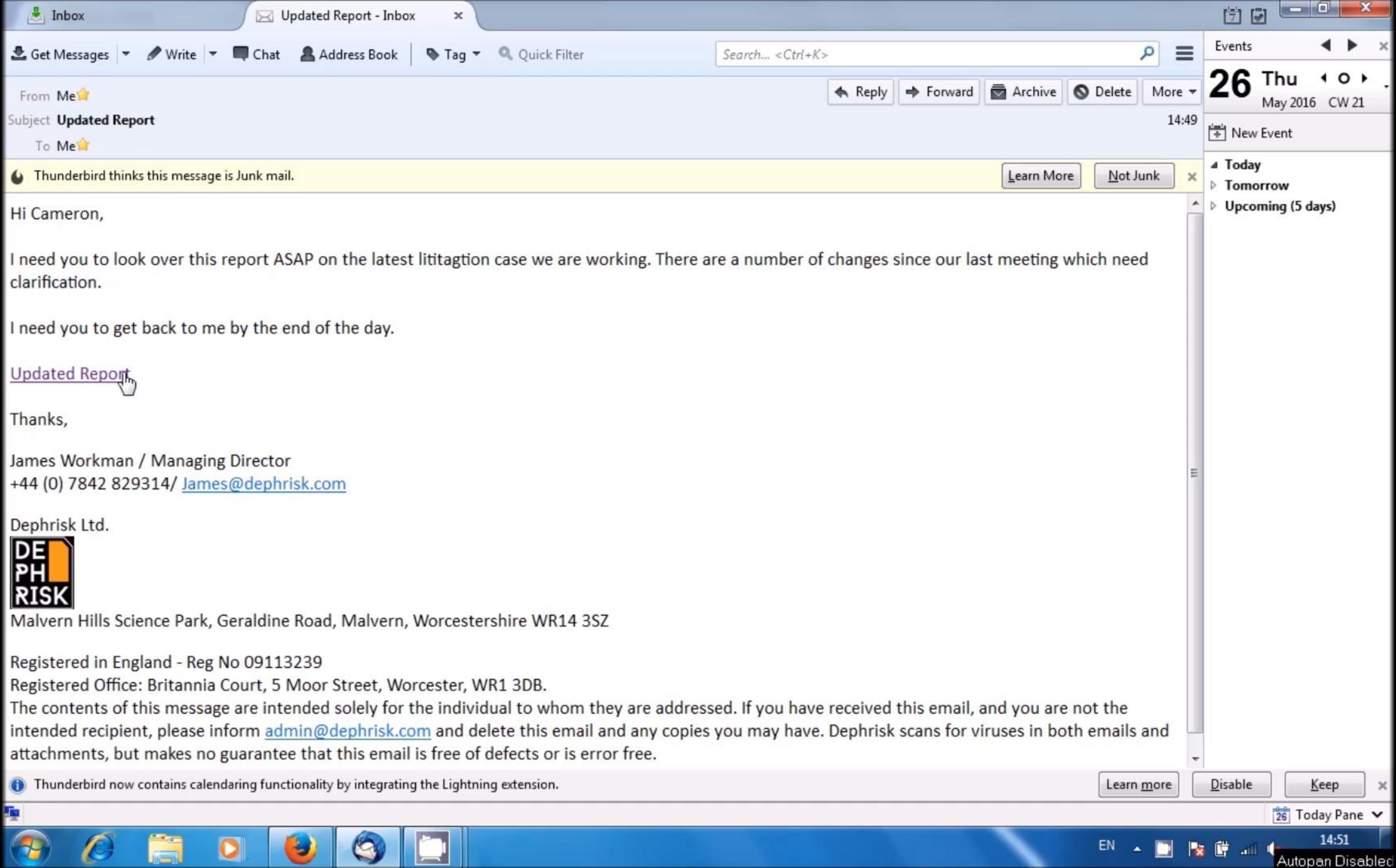
Currently extremely profitable

Hacking

Unauthorised access

Victims will not know…for months!

The Hack



From Me
Subject **Updated Report**
To Me
14:49

Thunderbird thinks this message is Junk mail.

Hi Cameron,

I need you to look over this report ASAP on the latest lititagtion case we are working. There are a number of changes since our last meeting which need clarification.

I need you to get back to me by the end of the day.

Updated Report

Thanks,

James Workman / Managing Director
+44 (0) 7842 829314/ James@dephrisk.com

Dephrisk Ltd.

DE
PH
RISK

Malvern Hills Science Park, Geraldine Road, Malvern, Worcestershire WR14 3SZ

Registered in England - Reg No 09113239
Registered Office: Britannia Court, 5 Moor Street, Worcester, WR1 3DB.
The contents of this message are intended solely for the individual to whom they are addressed. If you have received this email, and you are not the intended recipient, please inform admin@dephrisk.com and delete this email and any copies you may have. Dephrisk scans for viruses in both emails and attachments, but makes no guarantee that this email is free of defects or is error free.

Thunderbird now contains calendaring functionality by integrating the Lightning extension.

It’s Not Personal

Every business will be targeted, sooner or later

It is just a matter of time

Phishing emails are being opened every day

It Is Not Worth The Risk

Data is too valuable to be lost or stolen

The cost of losing data is rising fast

It is management’s responsibility to staff, clients & investors to keep it secure

Time For a New Approach

It is not JUST an IT issue

Firewalls & Anti-virus Software are not enough

Some Statistics

Over 2.5 million cyber-crime incidents in the UK last year

250,000 new viruses published every day with ‘Zero-day’ vulnerabilities last year

One in four UK firms hit by cyber-crime last year by phishing, ransomware & fraud

UK Senior management fraud rising by 20% each year

Cyber-crime attacks on mobile devices in the UK quadrupled last year

Everything Online Is Recorded

Email addresses

News Web pages

Blogs

Social media accounts & postings

Company accounts & director names

Social Engineering

Piecing together bits of data from various sources typically online to identify a target f

Google

Brokerbility

in

FCA
FINANCIAL CONDUCT AUTHORITY

BIBA
Member

t

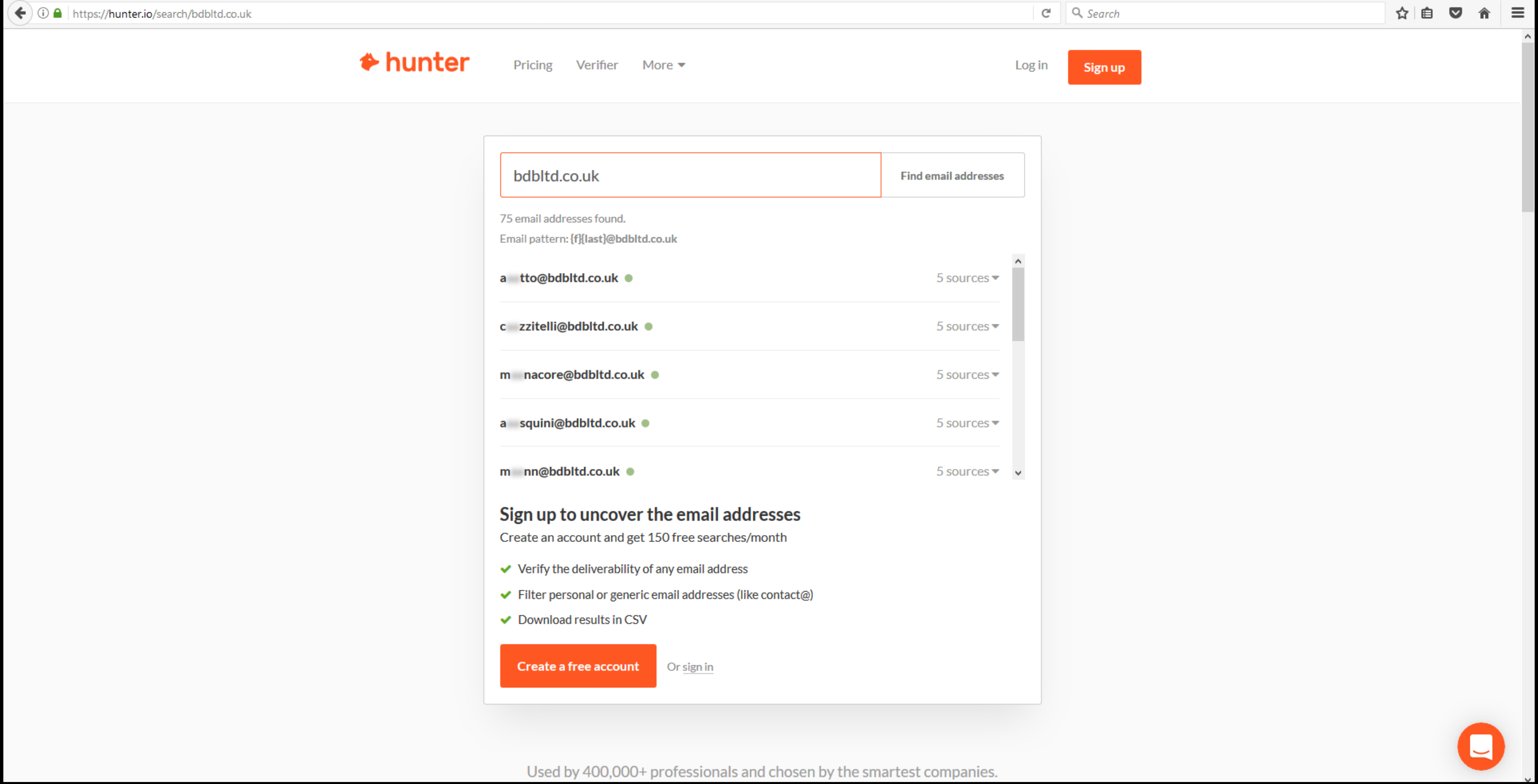
British
Chambers of
Commerce

g+

Solicitors
Regulation
Authority

Companies House

YouTube



75 email addresses found.

Email pattern: {f}{last}@bdbltd.co.uk

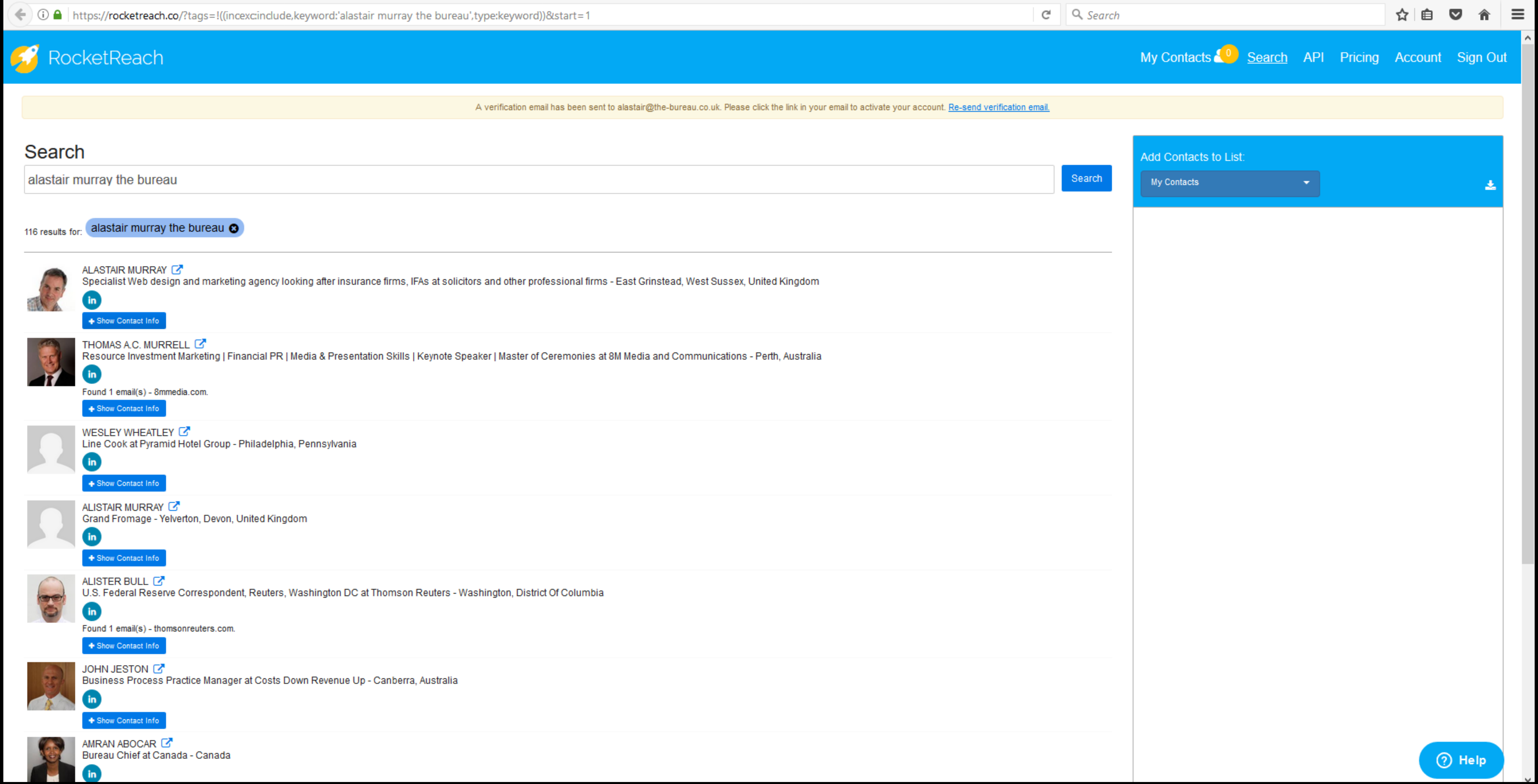
a[redacted]tto@bdbltd.co.uk ●	5 sources
c[redacted]zzitelli@bdbltd.co.uk ●	5 sources
m[redacted]nacore@bdbltd.co.uk ●	5 sources
a[redacted]squini@bdbltd.co.uk ●	5 sources
m[redacted]nn@bdbltd.co.uk ●	5 sources

Sign up to uncover the email addresses

Create an account and get 150 free searches/month

- ✓ Verify the deliverability of any email address
- ✓ Filter personal or generic email addresses (like contact@)
- ✓ Download results in CSV

Used by 400,000+ professionals and chosen by the smartest companies.



https://rocketreach.co/?tags=!((incexc:include,keyword:'alastair murray the bureau',type:keyword))&start=1
Search
RocketReach
My Contacts
0
Search
API
Pricing
Account
Sign Out

A verification email has been sent to alastair@the-bureau.co.uk. Please click the link in your email to activate your account. Re-send verification email.

Search

alastair murray the bureau

Search
Add Contacts to List:
My Contacts
Help

116 results for: alastair murray the bureau

ALASTAIR MURRAY
Specialist Web design and marketing agency looking after insurance firms, IFAs at solicitors and other professional firms - East Grinstead, West Sussex, United Kingdom
in
+ Show Contact Info

THOMAS A.C. MURRELL
Resource Investment Marketing | Financial PR | Media & Presentation Skills | Keynote Speaker | Master of Ceremonies at 8M Media and Communications - Perth, Australia
in
Found 1 email(s) - 8mmedia.com.
+ Show Contact Info

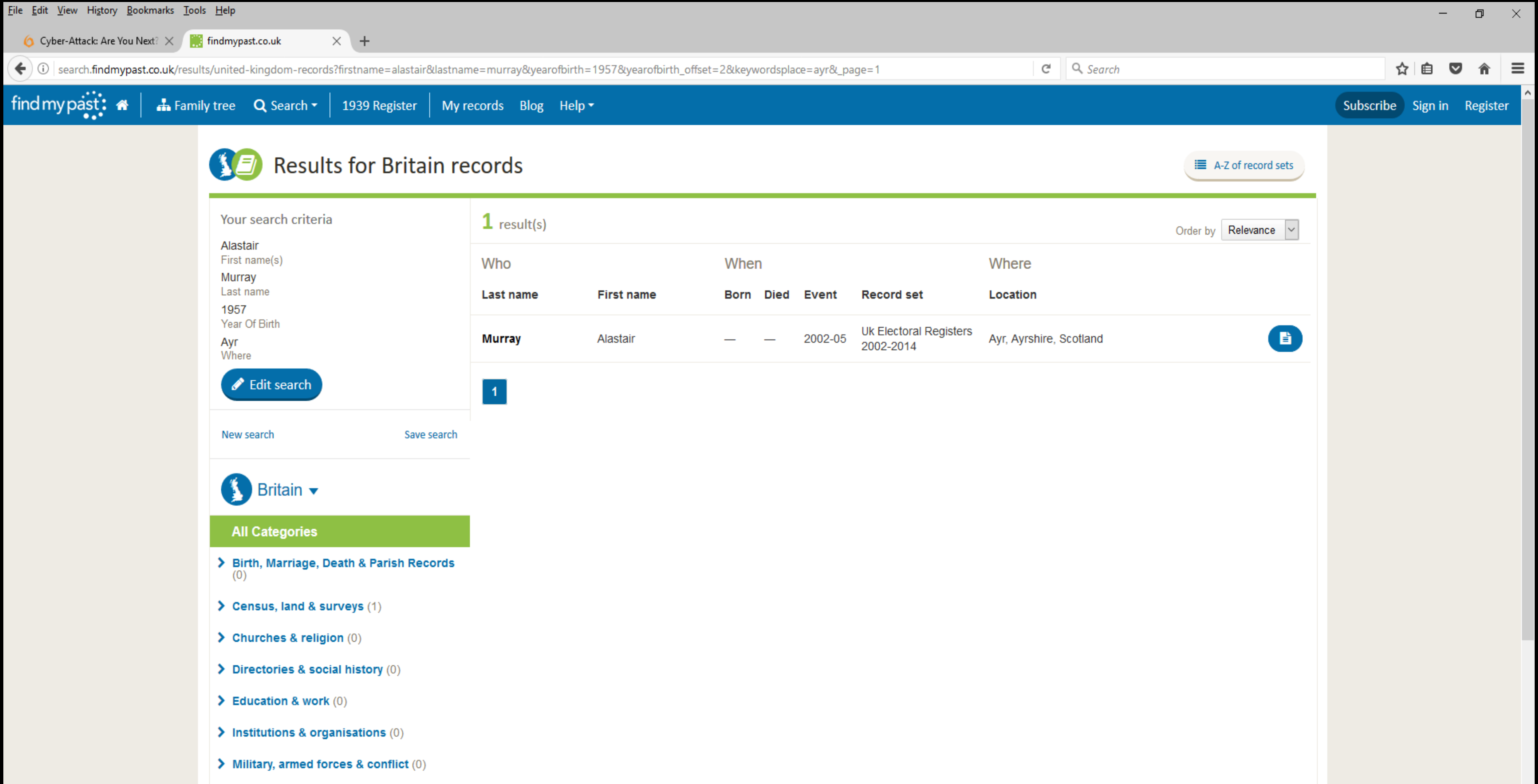
WESLEY WHEATLEY
Line Cook at Pyramid Hotel Group - Philadelphia, Pennsylvania
in
+ Show Contact Info

ALISTAIR MURRAY
Grand Fromage - Yelverton, Devon, United Kingdom
in
+ Show Contact Info

ALISTER BULL
U.S. Federal Reserve Correspondent, Reuters, Washington DC at Thomson Reuters - Washington, District Of Columbia
in
Found 1 email(s) - thomsonreuters.com.
+ Show Contact Info

JOHN JESTON
Business Process Practice Manager at Costs Down Revenue Up - Canberra, Australia
in
+ Show Contact Info

AMRAN ABOCAR
Bureau Chief at Canada - Canada
in



search.findmypast.co.uk/results/united-kingdom-records?firstname=alastair&lastname=murray&yearofbirth=1957&yearofbirth_offset=2&keywordsplace=ayr&_page=1

Results for Britain records

Your search criteria

Alastair
First name(s)

Murray
Last name

1957
Year Of Birth

Ayr
Where

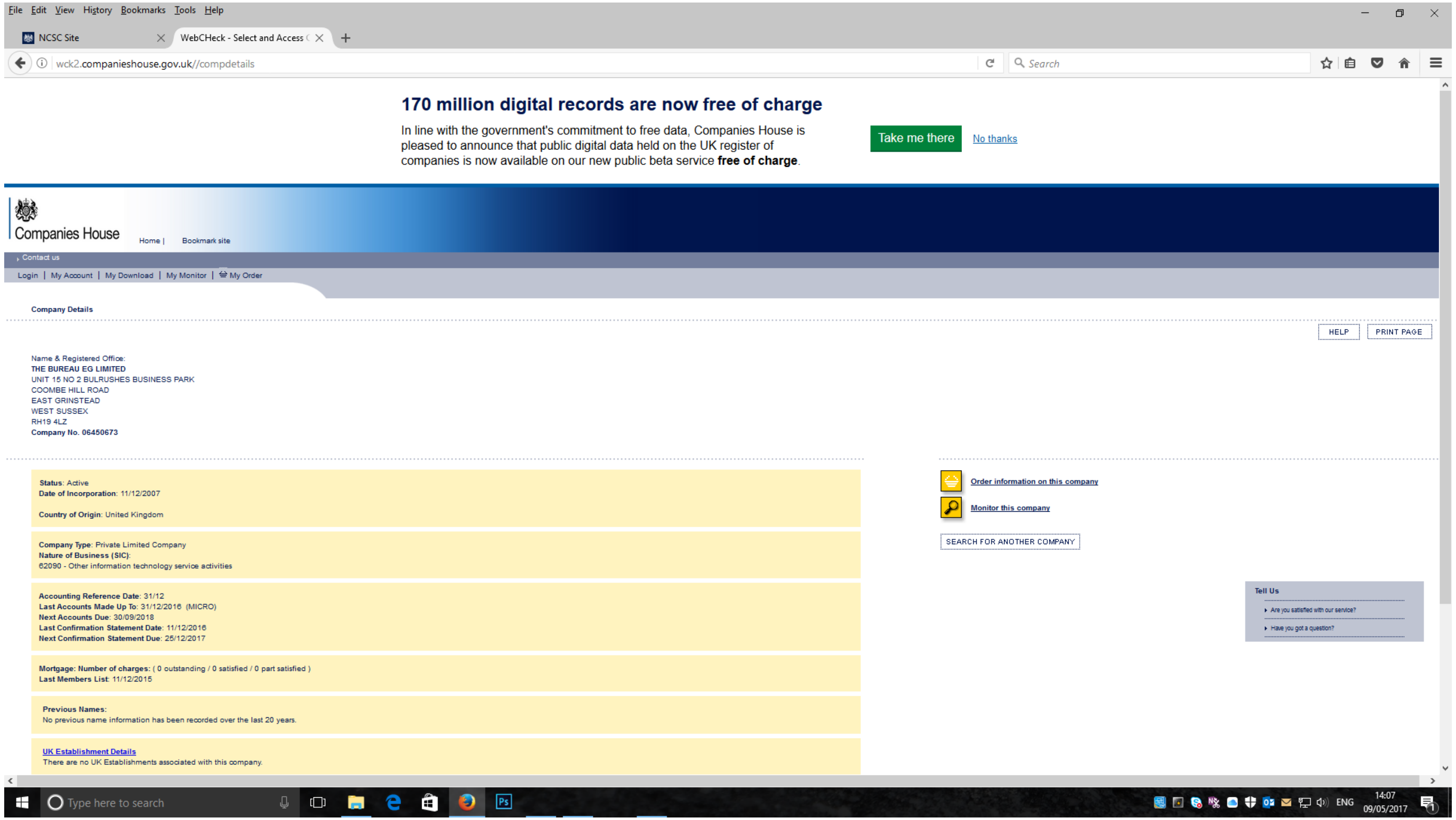
1 result(s)

Who		When				Where
Last name	First name	Born	Died	Event	Record set	Location
Murray	Alastair	—	—	2002-05	Uk Electoral Registers 2002-2014	Ayr, Ayrshire, Scotland

Britain

All Categories

- **Birth, Marriage, Death & Parish Records** (0)
- **Census, land & surveys** (1)
- **Churches & religion** (0)
- **Directories & social history** (0)
- **Education & work** (0)
- **Institutions & organisations** (0)
- **Military, armed forces & conflict** (0)


File Edit View History Bookmarks Tools Help
NCSC Site
WebCHeck - Select and Access (
wck2.companieshouse.gov.uk//compdetails
Search
Take me there
No thanks
Companies House
Home |
Bookmark site
Contact us
Login | My Account | My Download | My Monitor | My Order
HELP
PRINT PAGE
Order information on this company
Monitor this company
SEARCH FOR ANOTHER COMPANY
Tell Us
Are you satisfied with our service?
Have you got a question?
Type here to search
ENG
14:07
09/05/2017

170 million digital records are now free of charge

In line with the government's commitment to free data, Companies House is pleased to announce that public digital data held on the UK register of companies is now available on our new public beta service **free of charge**.

Company Details

Name & Registered Office:
THE BUREAU EG LIMITED
UNIT 15 NO 2 BULRUSHES BUSINESS PARK
COOMBE HILL ROAD
EAST GRINSTEAD
WEST SUSSEX
RH19 4LZ
Company No. 06450673

Status: Active
Date of Incorporation: 11/12/2007

Country of Origin: United Kingdom

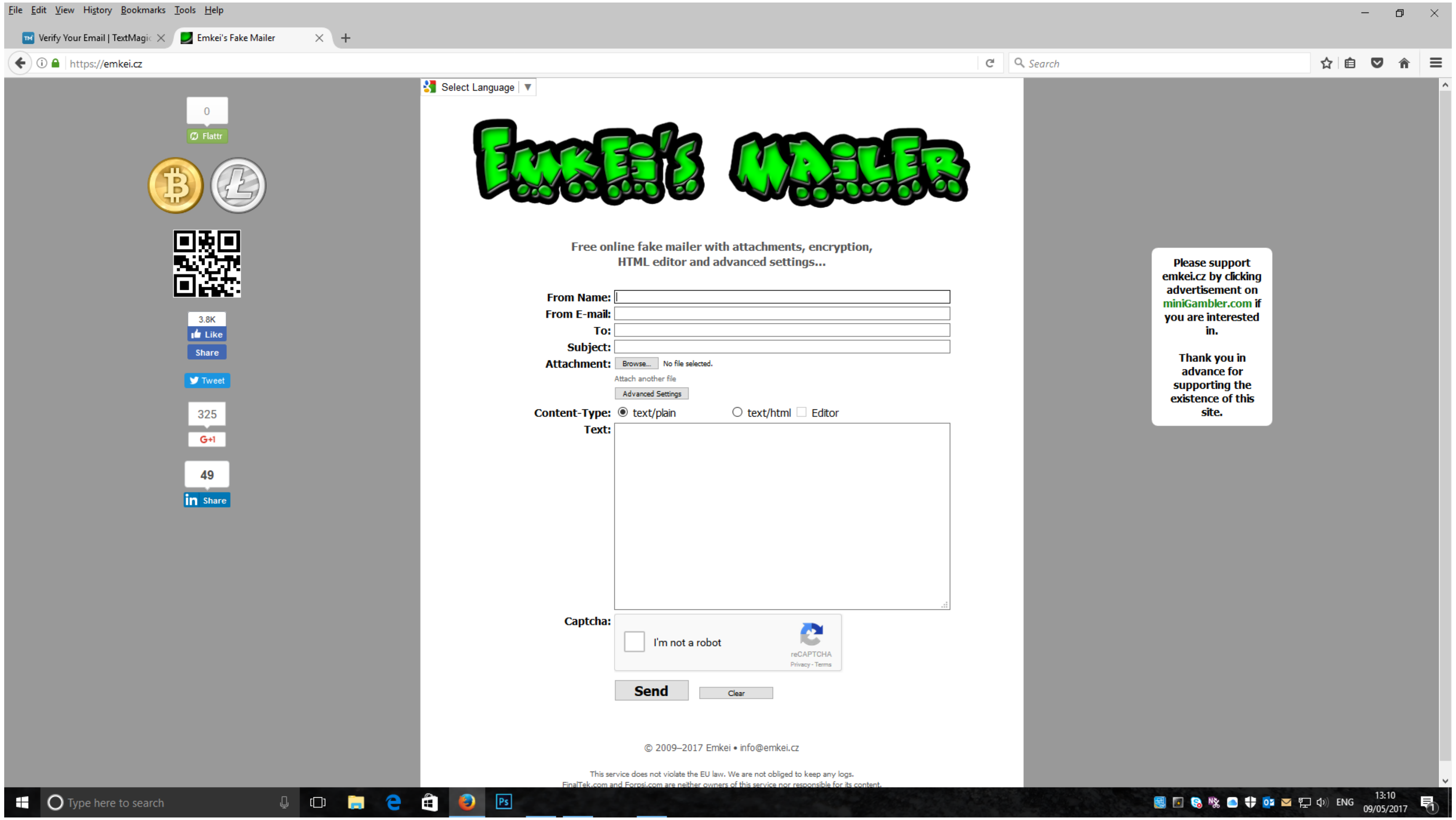
Company Type: Private Limited Company
Nature of Business (SIC):
62090 - Other information technology service activities

Accounting Reference Date: 31/12
Last Accounts Made Up To: 31/12/2016 (MICRO)
Next Accounts Due: 30/09/2018
Last Confirmation Statement Date: 11/12/2016
Next Confirmation Statement Due: 25/12/2017

Mortgage: Number of charges: (0 outstanding / 0 satisfied / 0 part satisfied)
Last Members List: 11/12/2015

Previous Names:
No previous name information has been recorded over the last 20 years.

UK Establishment Details
There are no UK Establishments associated with this company.



Free online fake mailer with attachments, encryption,
HTML editor and advanced settings...

From Name:

From E-mail:

To:

Subject:

Attachment: Browse... No file selected.

Attach another file

Advanced Settings

Content-Type: ● text/plain ○ text/html □ Editor

Text:

Captcha: □ I'm not a robot reCAPTCHA Privacy - Terms

Send Clear

© 2009–2017 Emkei • info@emkei.cz

This service does not violate the EU law. We are not obliged to keep any logs.
FinalTek.com and Forpsi.com are neither owners of this service nor responsible for its content.

Please support emkei.cz by clicking advertisement on miniGambler.com if you are interested in.

Thank you in advance for supporting the existence of this site.

How Much Will Its Cost?

SME firms do NOT know how much a breach will cost

They are keeping their fingers crossed

The average cost of the worst breach for a SME is £75k to £310K

- Forensics
- Post breach audits & data restoration
- Communications to clients & suppliers & Regulatory Authorities
- Client loyalty re-building
- Market standing & goodwill re-building

UK consumers say they would avoid firms that had been hacked

www.

GDPR May 25th 2018

Data Responsibilities

Who Should Be Concerned?

Organisations of ALL sizes in every sector

There are 5.5 million SMEs in UK representing 99% of ALL businesses
5.1 million micro businesses with 1 to 9 employees representing 95% of all businesses
Accounting for 33% of all UK employees and 18% of annual turnover

Over a quarter of them suffered a security breach last year

Almost all were caused by human error

Lock It Up!

Data records were physically locked-up in the past by one or a few keyholders

Office Networks should do the same swapping physical cabinets & keys for secure logins & encryption

A lot of standard office software offers this type of security Microsoft 365 a good example & used by many SMEs

Where to Start

By assuming you are a target

Today every business is a potential target

Review Current Security

What Cyber Security is currently in place?

Visit Government’s cyber security Website

https://www.gov.uk/government/policies/cyber-security

www.

ecsc
more secure

CiSP
A CATALYST FOR COLLABORATION

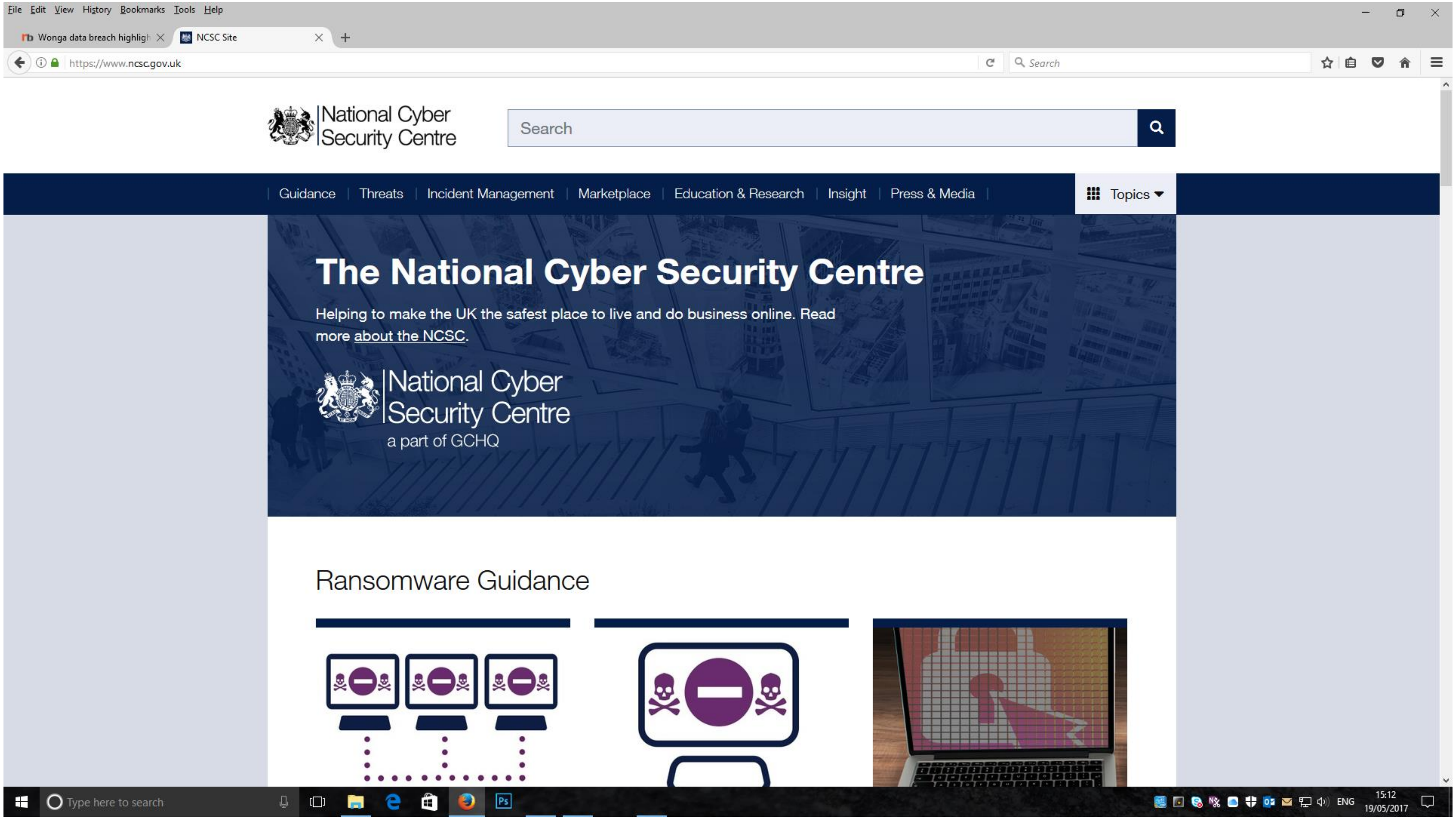
IASME
Consortium ®

CREST

ncsc
NATIONAL CYBER SKILLS CENTRE

National Cyber
Security Centre
a part of GCHQ

CYBER
MANAGEMENT
ALLIANCE

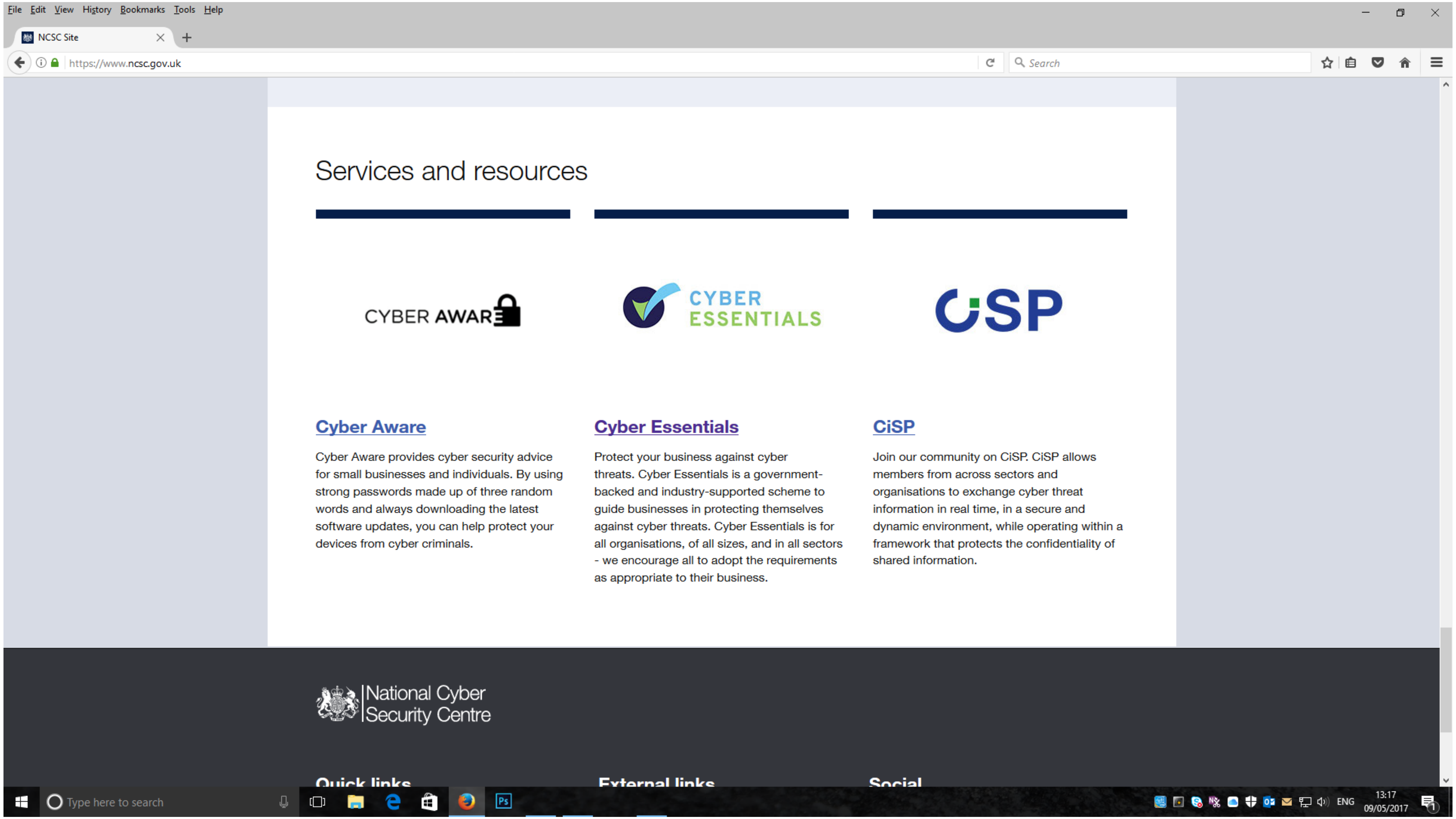


The National Cyber Security Centre

Helping to make the UK the safest place to live and do business online. Read more about the NCSC.

National Cyber Security Centre
a part of GCHQ

Ransomware Guidance



Services and resources

Cyber Aware

Cyber Aware provides cyber security advice for small businesses and individuals. By using strong passwords made up of three random words and always downloading the latest software updates, you can help protect your devices from cyber criminals.

Cyber Essentials

Protect your business against cyber threats. Cyber Essentials is a government-backed and industry-supported scheme to guide businesses in protecting themselves against cyber threats. Cyber Essentials is for all organisations, of all sizes, and in all sectors - we encourage all to adopt the requirements as appropriate to their business.

CiSP

Join our community on CiSP. CiSP allows members from across sectors and organisations to exchange cyber threat information in real time, in a secure and dynamic environment, while operating within a framework that protects the confidentiality of shared information.

National Cyber Security Centre

Quick links

External links

Social

Start Building Your Defences

Adopt the Government backed scheme

The Cyber Essentials

Offering a cyber security template for SME organisations

A security map for your IT & office network

desktop PCs – laptops – mobile phones – tablets – portable hard drives

Apply for **Cyber Essentials Accreditation** & steal a march on your rivals

Earn the Cyber Essentials Accreditation

The Cyber Essentials

Check & update firewall IP passwords

Check & update user login passwords

Install ALL operating system patches & updates

Run regular anti-virus updates – auto & manual

Run regular back-up checks & ‘Restores’

The Cyber Essentials

Adopt a Cyber Security Policy

Write an Assets Register

Promote & refresh the importance of Cyber Security

Appoint a cyber contact in the office

The Cyber Essentials

Adopt a cyber security policy

To clarify the safe use of office IT
(staff rules the do’s and don’ts when used in the office & away from the office)

To set a standard for password updating

To set a standard for software patching / updating

To set a standard for back-ups and restore testing

To set a standard for social media, the Web, mobile phones

Who to contact when something bad is suspected

The Cyber Essentials

Write an Assets Register

To know what you have & what to protect

(Property, IT & Computers, Websites, software & versions, brands, copyrights, patents, etc)

The Cyber Essentials

Promote & refresh the importance of Cyber Security

Terms of Employment

Terms of Business

Staff Memos & Meetings

Notice Boards

Screen Savers

www.

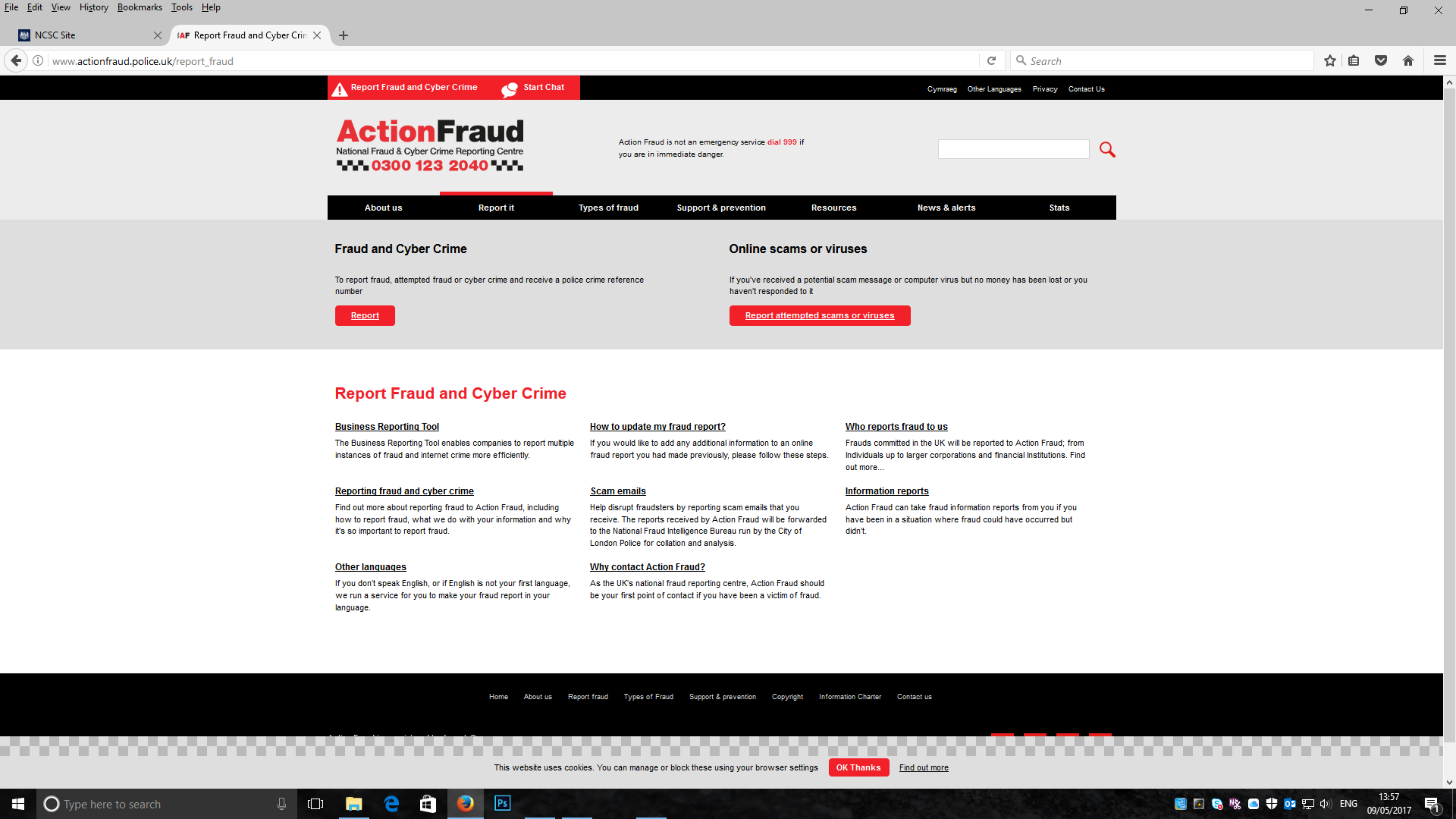
The Cyber Essentials

Appoint a cyber contact in the office…a point of contact

An office manager, compliance or fire officer, health and safety officer

To report any suspicious phone calls, emails, slowness of office network

strange pop-ups… even a ransomware screen!



Action Fraud is not an emergency service dial 999 if you are in immediate danger.

Fraud and Cyber Crime

To report fraud, attempted fraud or cyber crime and receive a police crime reference number

Report

Online scams or viruses

If you've received a potential scam message or computer virus but no money has been lost or you haven't responded to it

Report attempted scams or viruses

Report Fraud and Cyber Crime

Business Reporting Tool

The Business Reporting Tool enables companies to report multiple instances of fraud and internet crime more efficiently.

Reporting fraud and cyber crime

Find out more about reporting fraud to Action Fraud, including how to report fraud, what we do with your information and why it's so important to report fraud.

Other languages

If you don't speak English, or if English is not your first language, we run a service for you to make your fraud report in your language.

How to update my fraud report?

If you would like to add any additional information to an online fraud report you had made previously, please follow these steps.

Scam emails

Help disrupt fraudsters by reporting scam emails that you receive. The reports received by Action Fraud will be forwarded to the National Fraud Intelligence Bureau run by the City of London Police for collation and analysis.

Why contact Action Fraud?

As the UK's national fraud reporting centre, Action Fraud should be your first point of contact if you have been a victim of fraud.

Who reports fraud to us

Frauds committed in the UK will be reported to Action Fraud; from Individuals up to larger corporations and financial Institutions. Find out more...

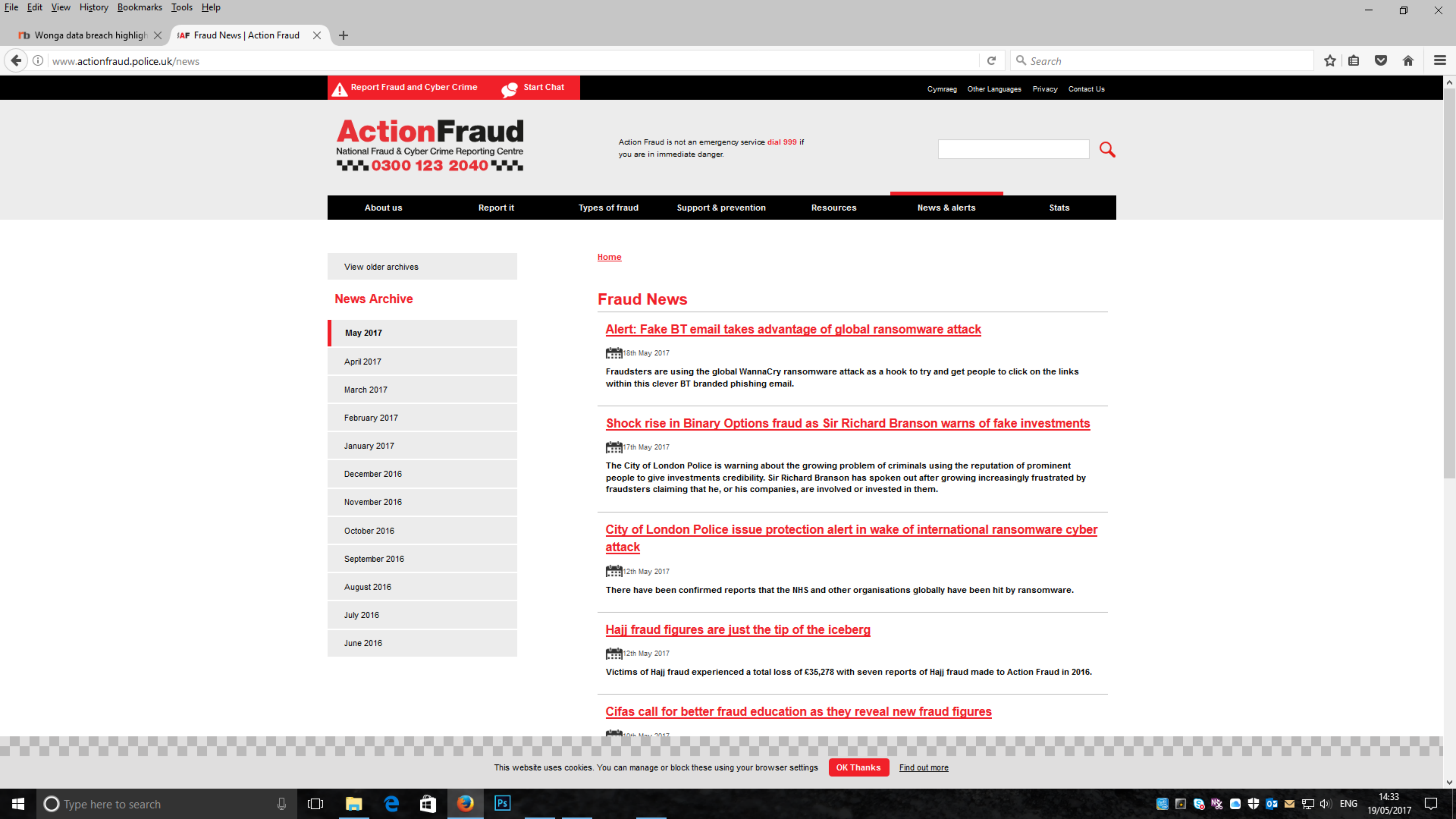
Information reports

Action Fraud can take fraud information reports from you if you have been in a situation where fraud could have occurred but didn't.

This website uses cookies. You can manage or block these using your browser settings

OK Thanks

Find out more



ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Action Fraud is not an emergency service dial 999 if you are in immediate danger.

View older archives

News Archive

- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- December 2016
- November 2016
- October 2016
- September 2016
- August 2016
- July 2016
- June 2016

Home

Fraud News

Alert: Fake BT email takes advantage of global ransomware attack

18th May 2017

Fraudsters are using the global WannaCry ransomware attack as a hook to try and get people to click on the links within this clever BT branded phishing email.

Shock rise in Binary Options fraud as Sir Richard Branson warns of fake investments

17th May 2017

The City of London Police is warning about the growing problem of criminals using the reputation of prominent people to give investments credibility. Sir Richard Branson has spoken out after growing increasingly frustrated by fraudsters claiming that he, or his companies, are involved or invested in them.

City of London Police issue protection alert in wake of international ransomware cyber attack

12th May 2017

There have been confirmed reports that the NHS and other organisations globally have been hit by ransomware.

Hajj fraud figures are just the tip of the iceberg

12th May 2017

Victims of Hajj fraud experienced a total loss of £35,278 with seven reports of Hajj fraud made to Action Fraud in 2016.

Cifas call for better fraud education as they reveal new fraud figures

10th May 2017

This website uses cookies. You can manage or block these using your browser settings OK Thanks Find out more

Protecting Staff

Most cyber breaches are caused by human error

Arrange cyber awareness & intelligence training

Explanations of the threats, vulnerabilities, common phishing ploys, approach to social media, cyber security tactics, reporting procedures, reconnaissance, cues & detection

Protecting Staff

Cyber Security induction training for existing staff

Cyber Security induction training for all new staff

Include Cyber Security responsibilities in Terms of Employment

Regular review of management & staff login permissions

(who gets access to what)

Add Cyber Security to staff meetings agenda

Appoint a Cyber Security Officer

Create A Cyber Security Culture

We have it for regulatory compliance

We have it for professional conduct

We have it for health and safety

Cyber Insurance

Most organisations do NOT have cyber insurance

It is widely available

Find a specialist to arrange adequate protection

Cyber Insurance

Covering

The loss of data from IT systems & networks

Assistance with Cyber incident management

– help with reputational damage – regulatory enforcement - legal

The loss or damage of equipment & software costs

Business interruption cost

Extortion costs

Client & supplier notification costs

Post incident investigation/audits & legal dispute costs

Defamation, privacy breaches, negligence, civil actions costs

Loss of data compensation costs

AXA

Allianz

AVIVA

BRIT

AIG

HISCOX

RSA

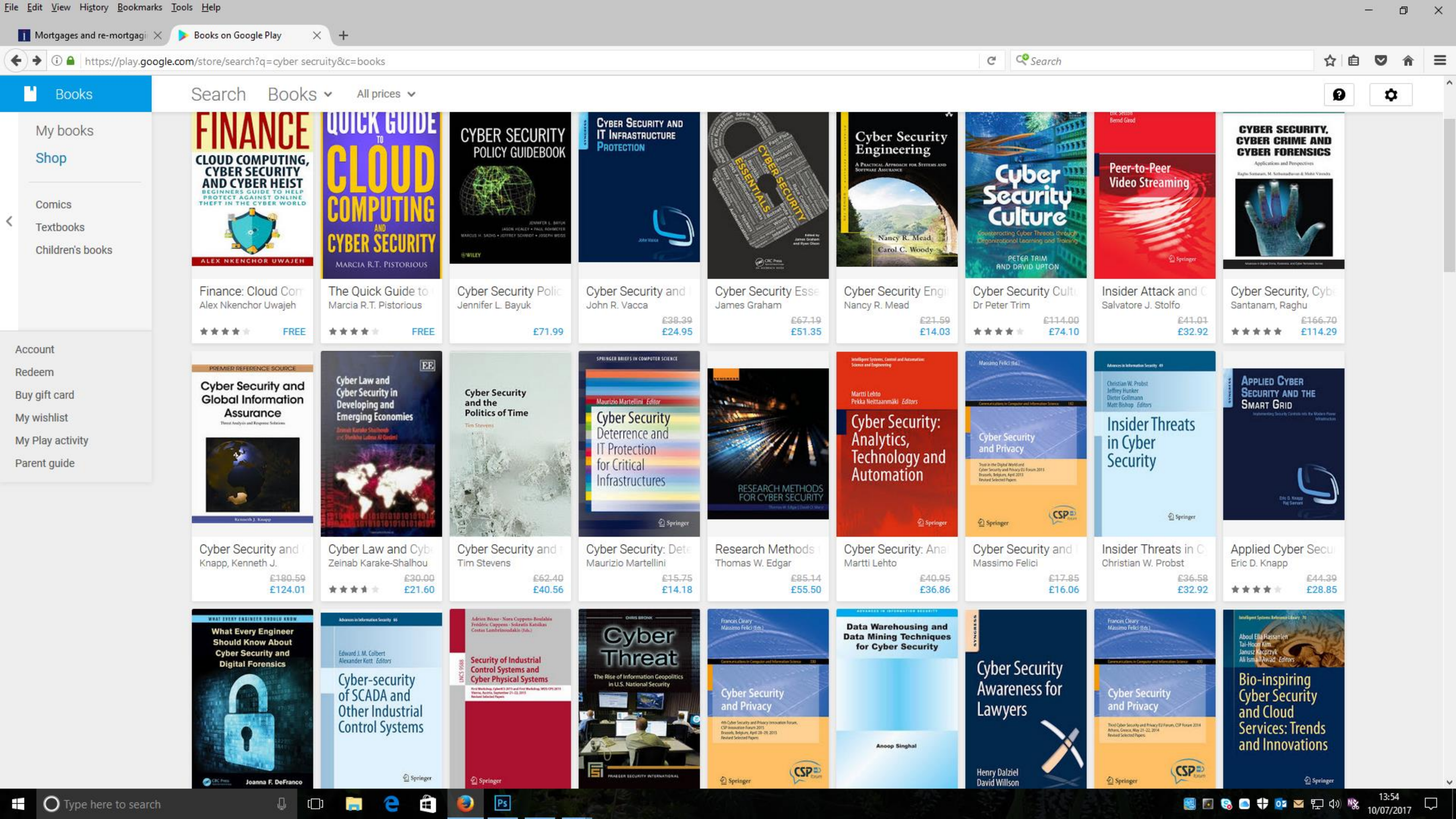
CHUBB®

cfc Underwriting

LLOYD'S
LLOYDS OF LONDON

ZURICH

QBE



Finance: Cloud Com	Alex Nkenchor Uwajeh	FREE
The Quick Guide to	Marcia R.T. Pistorious	FREE
Cyber Security Polic	Jennifer L. Bayuk	£71.99
Cyber Security and	John R. Vacca	~~£38.39~~ £24.95
Cyber Security Esse	James Graham	~~£67.19~~ £51.35
Cyber Security Engi	Nancy R. Mead	~~£21.59~~ £14.03
Cyber Security Cult	Dr Peter Trim	~~£114.00~~ £74.10
Insider Attack and	Salvatore J. Stolfo	~~£41.01~~ £32.92
Cyber Security, Cyb	Santanam, Raghu	~~£166.70~~ £114.29
Cyber Security and	Knapp, Kenneth J.	~~£180.59~~ £124.01
Cyber Law and Cyb	Zeinab Karake-Shalhou	~~£30.00~~ £21.60
Cyber Security and	Tim Stevens	~~£62.40~~ £40.56
Cyber Security: Dete	Maurizio Martellini	~~£15.75~~ £14.18
Research Methods	Thomas W. Edgar	~~£85.14~~ £55.50
Cyber Security: Ana	Martti Lehto	~~£40.95~~ £36.86
Cyber Security and	Massimo Felici	~~£17.85~~ £16.06
Insider Threats in C	Christian W. Probst	~~£36.58~~ £32.92
Applied Cyber Secu	Eric D. Knapp	~~£44.39~~ £28.85

For These Presentation slides
Cyber Security Training Courses
Discuss Your Cyber Security Needs

Contact The Bureau

Ignorance Is No Defence

Thank you for Listening

Cyber Security Courses

Cyber Awareness

Understanding the threats:

Even with the best security software that your IT budget permits your office network will be penetrated. One click of a rogue email by an employee to infect one or more workstation, allow hackers in, cause a data breach or even a cyber ransom.

This is a 4 hour, half day course suitable for pre or post incident that addresses the same fundamentals.

Definitions of threats, vulnerabilities, risks and assets whilst reviewing the many steps organisations can take to address them.

Social engineering receives plenty of attention with discussions about the pre-requisites, reconnaissance, types of attacks and avoidance methods, cues and detection as well as the myths and misconceptions.

Cyber Essentials

Step by Step Cyber Essentials:

This is a one day classroom based course that teaches an organisation the minimum level of Cyber Security and how to achieve it. It will also prepare organisations wishing to apply for and earn the Cyber Essentials Accreditation.

This is currently the only UK Government-backed, industry supported scheme to encourage awareness of and protection from the escalating risk of cyber attacks.

It promotes what are termed the 5 Key technical controls that every organisation should have in place as a minimum level of protection.

Cyber Security & Privacy Essentials

Cyber Security & Privacy Essentials:

This course (CSPE) will both broaden and deepen your understanding of cyber security. With attacks becoming more common and the complexity ever increasing, security awareness at all levels in an organisation is key.

This course gives your team the opportunity to learn from experienced professionals who operate at the sharp end of Cyber Security. The course is reviewed on a regular basis and delivers training and support on the very latest Cyber Security Threats.

The CSPE course has also been given **GCHQ approval** through the **CESG Certification.** (Communications-electronics Security Group – located within GCHQ)

Cyber Bytes

Cyber Bytes: Keep Your Humans Safe:

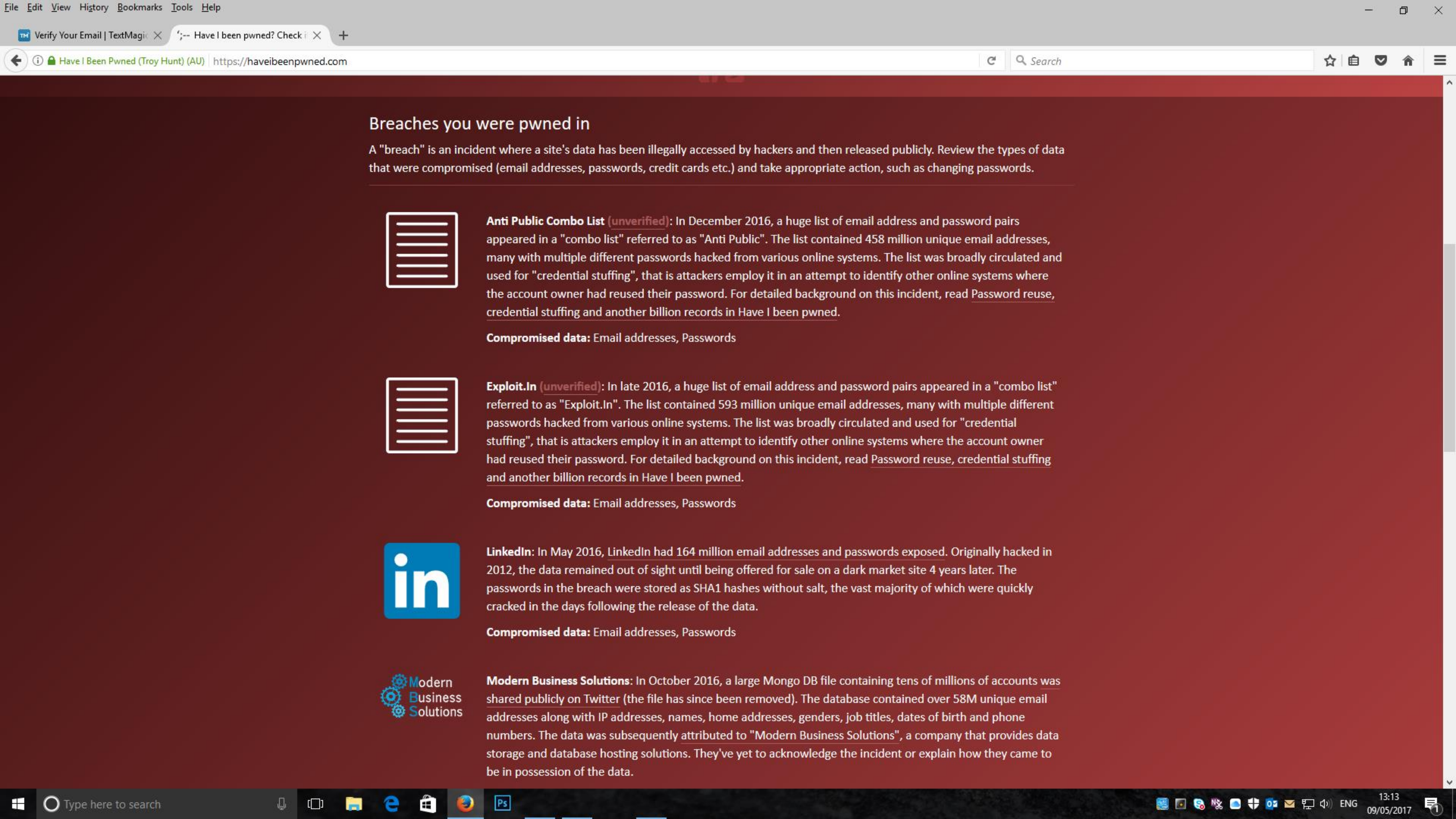
This is a 2 to 3 hour course suitable and recommended for all people in an organisation to encourage greater cyber security awareness in both private and business life.

A delegate will learn about the human element of Cyber Security and understand how the majority of attacks occur because of human error or through insider malicious activity.

At the end of the session a delegate will understand:

- Cyber Attacks – How they Happen
- What they Want – Why your business is a target?
- Social Engineering – What is it and how to spot it?
- Accidents happen with data and how to prevent them
- Social Media Safety – Basic Awareness
- Safety at Work, Home, and In-between – What should and shouldn’t you and your staff do?

www.


File Edit View History Bookmarks Tools Help
Verify Your Email | TextMagic
';-- Have I been pwned? Check i
Have I Been Pwned (Troy Hunt) (AU)
https://haveibeenpwned.com
Search
Type here to search
ENG
13:13
09/05/2017

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

Anti Public Combo List (unverified): In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I been pwned.

Compromised data: Email addresses, Passwords

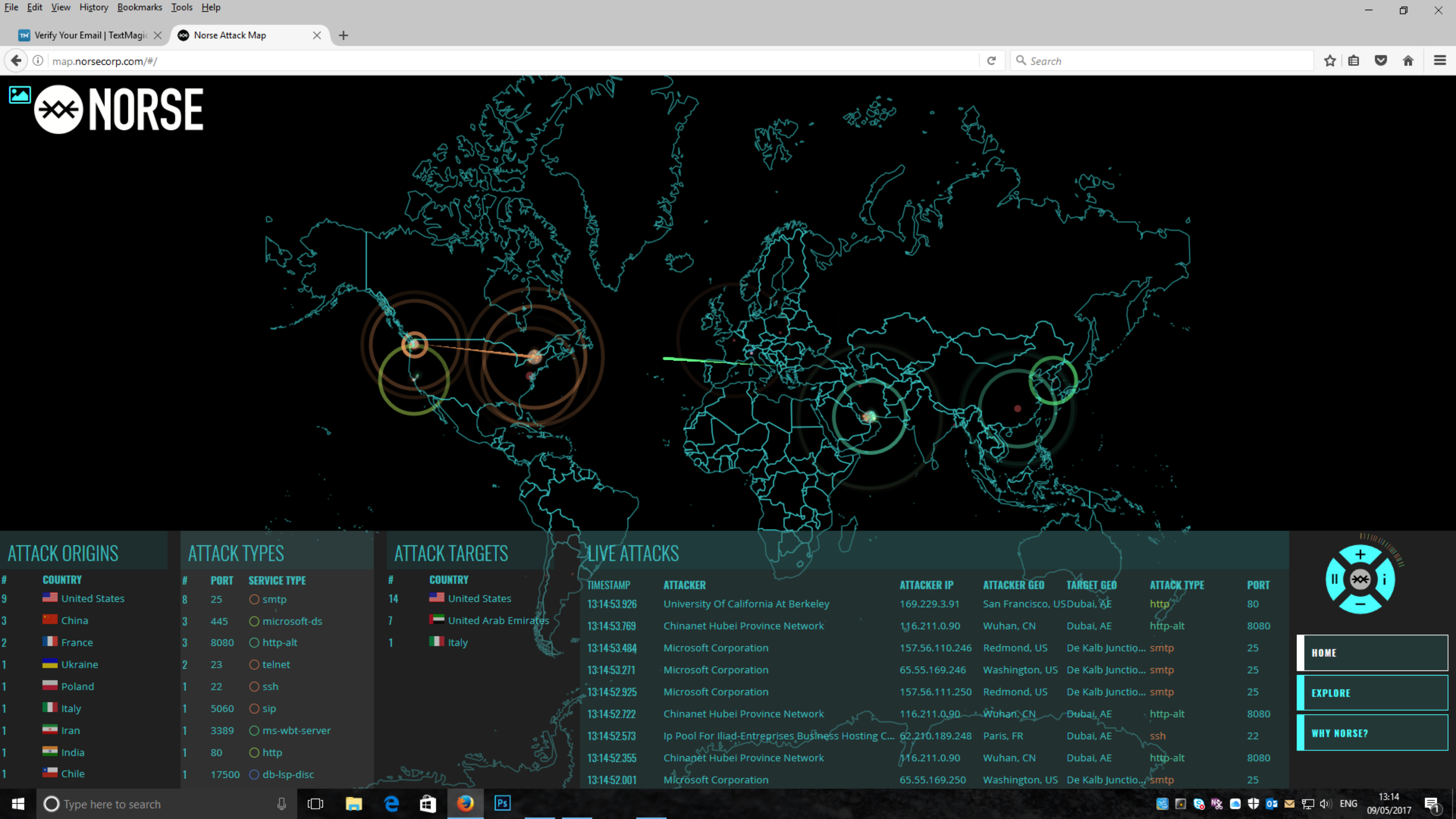
Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I been pwned.

Compromised data: Email addresses, Passwords

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

Modern Business Solutions: In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.



ATTACK ORIGINS

#	COUNTRY
9	United States
3	China
2	France
1	Ukraine
1	Poland
1	Italy
1	Iran
1	India
1	Chile

ATTACK TYPES

#	PORT	SERVICE TYPE
8	25	○ smtp
3	445	○ microsoft-ds
3	8080	○ http-alt
2	23	○ telnet
1	22	○ ssh
1	5060	○ sip
1	3389	○ ms-wbt-server
1	80	○ http
1	17500	○ db-lsp-disc

ATTACK TARGETS

#	COUNTRY
14	United States
7	United Arab Emirates
1	Italy

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
13:14:53.926	University Of California At Berkeley	169.229.3.91	San Francisco, US	Dubai, AE	http	80
13:14:53.769	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
13:14:53.484	Microsoft Corporation	157.56.110.246	Redmond, US	De Kalb Junctio...	smtp	25
13:14:53.271	Microsoft Corporation	65.55.169.246	Washington, US	De Kalb Junctio...	smtp	25
13:14:52.925	Microsoft Corporation	157.56.111.250	Redmond, US	De Kalb Junctio...	smtp	25
13:14:52.722	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
13:14:52.573	Ip Pool For Iliad-Entreprises Business Hosting C...	62.210.189.248	Paris, FR	Dubai, AE	ssh	22
13:14:52.355	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
13:14:52.001	Microsoft Corporation	65.55.169.250	Washington, US	De Kalb Junctio...	smtp	25