

How Hackers Think

A little bit technical

Daniel Plummer

Registered Care Providers Association

Daniel.plummer@rcpa.org.uk



Hackers – who they are



A conversation with a hacker

Sam Chattel AKA Cyber Sam! Ex Head Chef and...

- ❖ 10+ yrs | Ethical Hacker, Pen Tester, and Cybersecurity Consultant
- ❖ 4 yrs | Advanced Fraud & Cyber Crime Investigator for HSBC UK
- ❖ 3 yrs | Regional Cyber Coordinator for NHS England & UK Lead for Cyber Intelligence
- ❖ 1 yr | Cyber & Data Analyst for Regional Organised Crime Unit
- ❖ Technical Cyber Lead, Digital Care Hub



Dan Plummer

- ❖ 16+ yrs | working in social care
- ❖ 6 yrs | completing the DSPT
- ❖ 3 yrs | local support organisation for DSPT
- ❖ **Tries to communicate data and cyber security**



The Hacker Manifesto

This is our world now... The world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... And you call us criminals. We exist without skin colour, without nationality, without religious bias... And you call us criminals. You build atomic bombs, you wage wars, you murder, you cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all...

*** The Mentor***

Written in 1986 by Loyd Blankenship A.K.A The Mentor.

Belonged to a 2nd generation hacker group called Legion of Doom



“A hacker is an unauthorised user who attempts to gain access to an information system.”



❖ **Black Hat (bad guys)**

- Ignore the law
- No/broken moral compass

❖ **Grey Hat (bad guys, good guys?)**

- Bend the law
- Moral compass / personal code

❖ **White Hat (good guys)**

- Follow the law
- Strong moral compass / code of conduct
- Boring



Hacker's Motivation

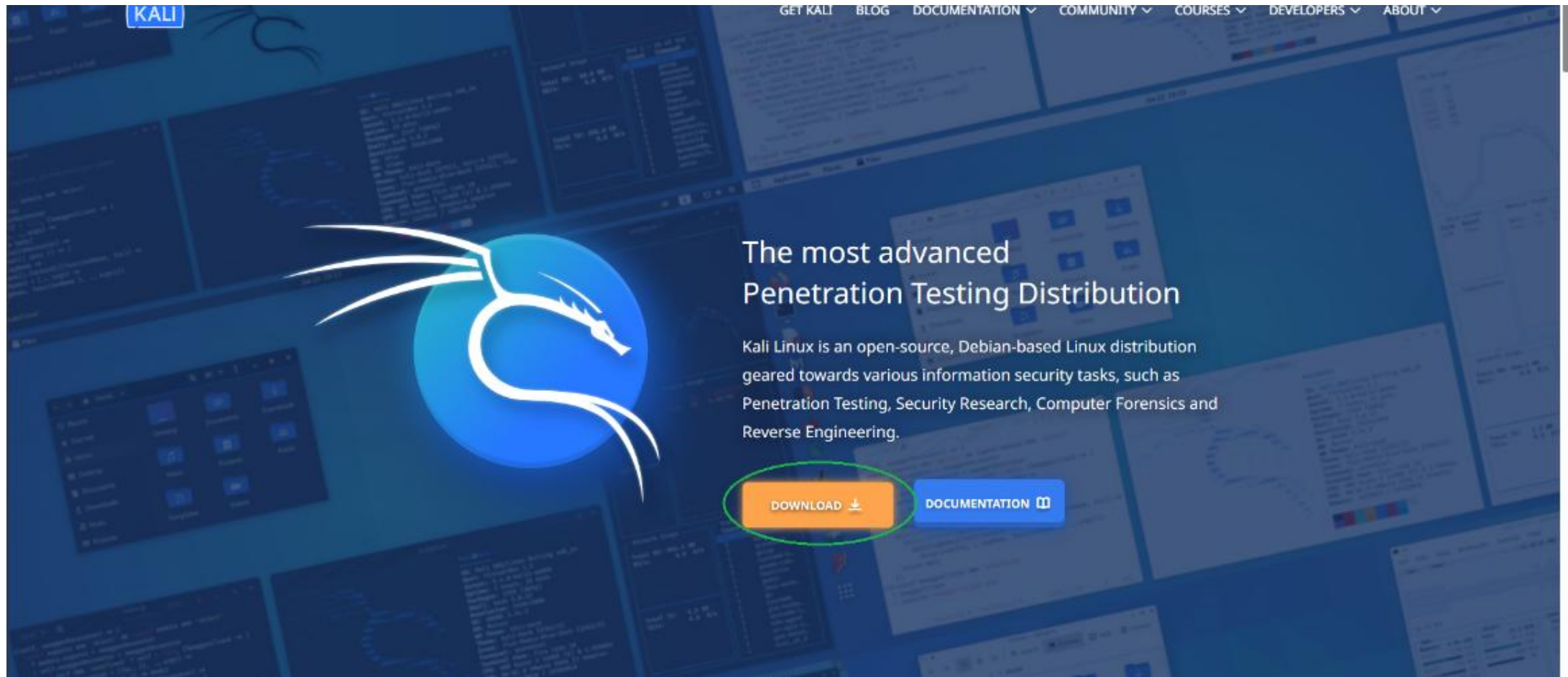
-
- Greed
 - Revenge
 - Curiosity
 - Technical challenge
 - Hacktivism
 - Espionage
 - Cyber terrorism
 - State sponsored
-



How do they do it?



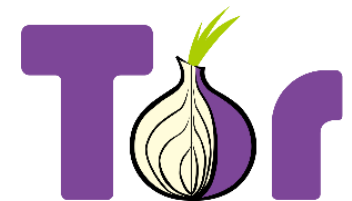
Hacking needs flexibility. They'll use Linux – The flexible operating system



The Dark Web – Encrypted and anonymous.

The screenshot shows a TOR browser window with the address bar displaying a .onion URL. The website is the 'DeepLink Onion Directory'. At the top, there are navigation links: 'Home', 'Add Site', and 'Contact'. Below the header, there are several banners for services like 'PayPal', 'PRIVATE KEYS', 'TORNODE', 'ICEBERG...ONION', 'ESCROW ACCEPT', and 'BOBBY | THE DARKWEB SEARCH ENGINE'. A warning message states: 'We don't send any email asking for money! any email pretend to be from us is SCAM!'. Below this, a yellow box contains the text: 'bookmark the right address! <http://deeeepv4bfndyatwkdzeciebcqwvlvga6mofdtswpon4elfut7lfqd.onion/>'. On the left side, there is a search bar and a list of categories: 'All Onions', 'Market', 'Hacking', 'Hosting', 'Forums', 'Blog', 'Link List / Wiki', 'Communication', 'Social', 'Financial Services', and 'Adult'. The main content area displays four listings:

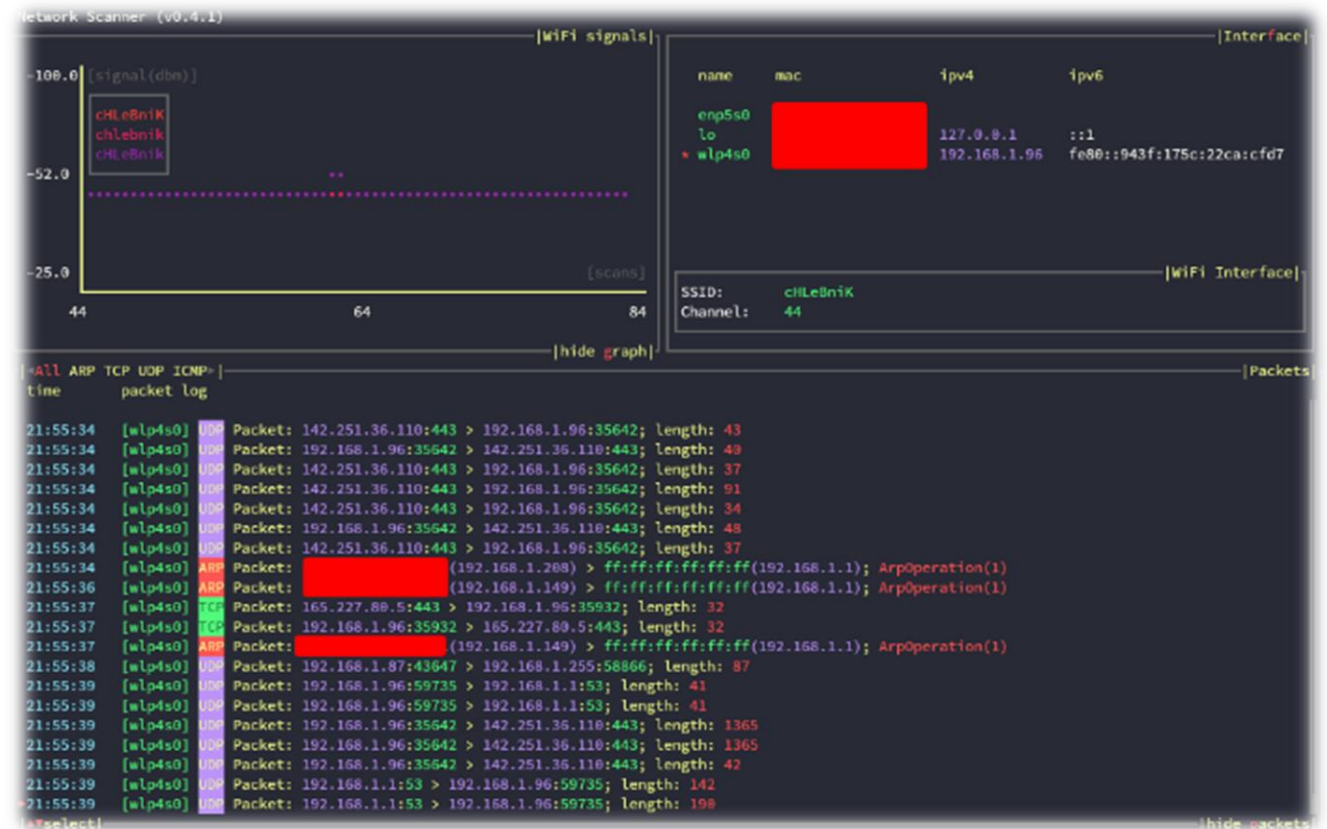
- Best Financial Market ✓**
Prepaid CC (VISA/MasterCard) | Cloned CC | Gift Cards (VISA/Amazon) | PayPal/Western Union Transfers | All our cards come with PINs and instructions!
<http://lthsfilluf5mpybtbud26blpgwou4av7padm4coyepfer5usfjkccyd.onion>
Views: 8,386,620 | Likes: 1,761 | Comments: 7 | Shares: 138 | Verified | Status: Up and Running
- Cash CARDS ✓**
We sell the most demanded products on the deepweb from the US and Europe. We have , specialized and have over 5 years' experience in this field.
<http://whje5cahjivo6s4ox36xrpae5gavgd45uekgaxlkoqjlcxcwkedn2lad.onion>
Views: 7,236,881 | Likes: 1,574 | Comments: 8 | Shares: 118 | Verified | Status: Up and Running
- Hacker Community ✓**
Hire The Most Advanced and Trustable Hackers of the Darknet
<http://ugdbp6mw657tjzmymg2u7xv3uhtmbcpqgiimtsfqc47kicisen7id.onion>
Views: 8,724,428 | Likes: 1,507 | Comments: 7 | Shares: 43 | Verified | Status: Up and Running
- Light Money ✓**
The most Trusted Financial Market Prepaid / Cloned / Gift Cards and Money Transfers via P



Hacking at Scale

Today's criminal groups don't always personalise every attack. They scan broadly and automatically, hunting for the weakest door - things like known software flaws, misconfigured cloud services, or systems that haven't been patched. When they find a gap, they exploit it and then escalate into more focused attacks.

That means even if you're not a 'big target,' a small misconfiguration, unpatched software, or weak password can be enough of an open door to be very tempting...



Social Engineering – The art of making you work for them



Phishing Attacks

Social Engineering Hooks

Phishing | Spear Phishing | Whaling

Scam Letters | Vishing | Smishing | Quishing

The scam changes but the 3 things they want you to do never changes

Click on a link | Open an attachment | Divulge information

Your login details | Deliver malware | Your data

Use tried and tested psychological cues

Authority. Scarcity. Time Pressure.

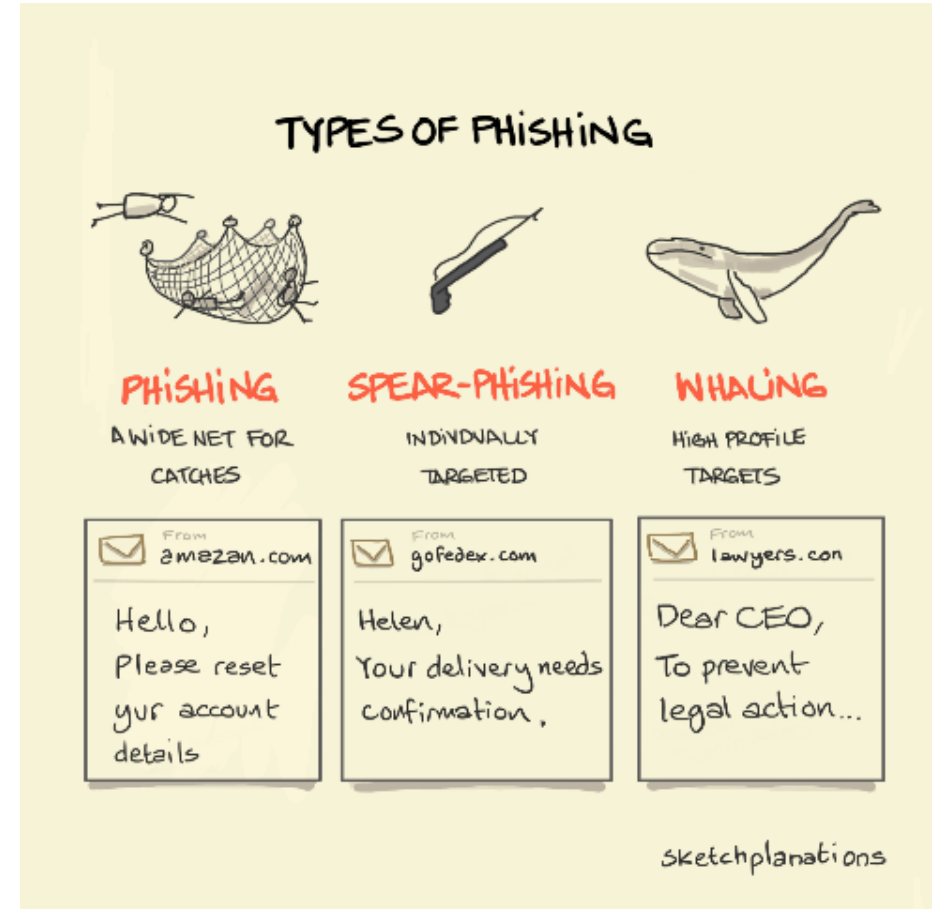


Image: Jono Hey, Big Ideas Little Pictures, Media Lab Books & sketchplanations.com



Open-Source Intelligence Gathering (scouting)

1010 1010 1010
1010 1010 1010



OSINT is the collection and analysis of data gathered from open sources (overt sources and publicly available information) to produce actionable intelligence.

OSINT data collection

- Search Engines (Google, DuckDuckGo, Bing, Yahoo)
- Companies House
- Reverse Image Search (TinEye, Google)
- Social Media (Facebook, LinkedIn, IG)

Have you ever done some Facebook stalking?



Hackers don't do things manually, they're lazy

For Open Source Intelligence (OSINT) Professionals



Social Links Crimewall

- Perform OSINT and SOCMINT across 500+ sources
- Graph, table, and map visualizations for key insights
- ML-driven analysis & real-time monitoring



Usersearch 2.0

- 35+ built-in investigative capabilities, no scripts or coding
- All APIs and services pre-integrated, no API keys
- Video guides and investigation tips in the dashboard



GeoSpy.ai

- Transform images into precise intelligence with AI
- Advanced geospatial AI for city and national monitoring
- From global coverage to street-level precision



OSINT Industries

- Unified profiles by linking emails, phones, usernames, etc.
- Map movements, trace timelines, and flag breaches
- Discover registered accounts across platforms



Maltego Monitor

- Monitor social media, news, and blogs in one interface
- Track specific regions, topics, or crises for tailored insights
- Custom dashboards for events, topics, and regions



Horizon Identity

- Correlate multiple identifiers into unified, reliable profiles
- Instantly resolve identities for subject profiling
- Eliminate manual research with fast identity intelligence



Talkwalker

- Track keywords and mentions across 30 social networks
- Monitor 150+ million websites, forums, blogs, and news
- Discover mentions in videos, images, podcasts, etc.

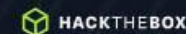


Intelligence X

- Search billions of selectors across emails, domains, IPs...
- Access darknet sources, data leaks, paste sites, archives
- Perform fast OSINT with deep global coverage



Alex Lozano



10 OSINT TOOLS FOR HACKERS

Shodan

Search engine of discoverable network devices on the Internet.

Maltego

View data in graphs to make relationships stand out.

Google Dorks

Advanced Google queries to find exactly what you are looking for.

Recon-ng

Metasploit like interface to run many OSINT tools.

Ahmia.fi

Google for the dark web. Great tool for OSINT forensics.

Wayback Machine

View old versions of websites. Going way back into the 1990s.

theHarvester

Automatically download emails, usernames from a company.

TinEye

A search engine based upon images instead of text.

OSINT Framework

The best way to find information about specific types of OSINT.

Local Library

Not all OSINT tools are online. Check your local library. It has hidden gems!

TIP 1

KEEP YOUR EYES OPEN!

Some things are right here in the target's website/social.

TIP 2

MAKE SURE YOU CHECK ALL DOMAINS AND SUBDOMAINS

One great tool is: <https://github.com/gfek/Lepus>

TIP 3

TIME TO STUDY!

Module: "OSINT: Corporate Recon"

Difficulty: **Hard**

Created by: Cry0l1t3

**OSINT:
Corporate
Recon**



Social-Media: Who cares if someone knows...



"That I went and had a pizza last night?"

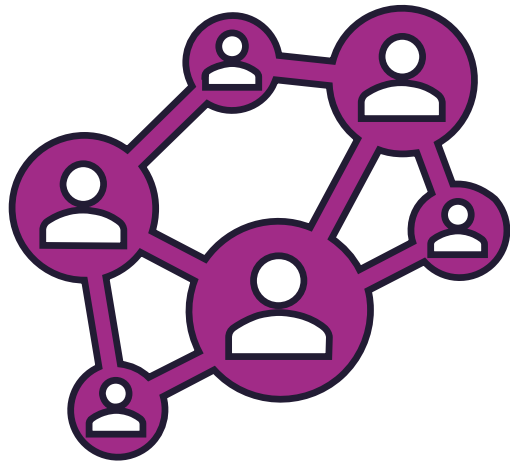
"It's my birthday?"

"What my new car looks like?"

"What the weather is like outside?"



Social Engineering: Using Your Digital Footprints



"That I went and had a pizza last night?"

Find out which restaurant you used, and spear phish with vouchers from that place

"It's my birthday?"

Know your DoB or part of it for identity theft or more believable social engineering

"What my new car looks like?"

With the license plate I now know when your MOT/Tax is due for renewal (spear phish)

"What the weather is like outside?"

Triangulate where you live from the image surroundings. Send official looking letters.



Artificial Intelligence – A game changer?



AI-Powered Social Engineering

The rise of AI tools, such as generative AI, has made social engineering scams more sophisticated and convincing.

Key Risks:

- AI automates at scale, increasing attack volume.
- Emails & messages are harder to detect.
- Traditional anti-phishing defences may struggle to keep up.



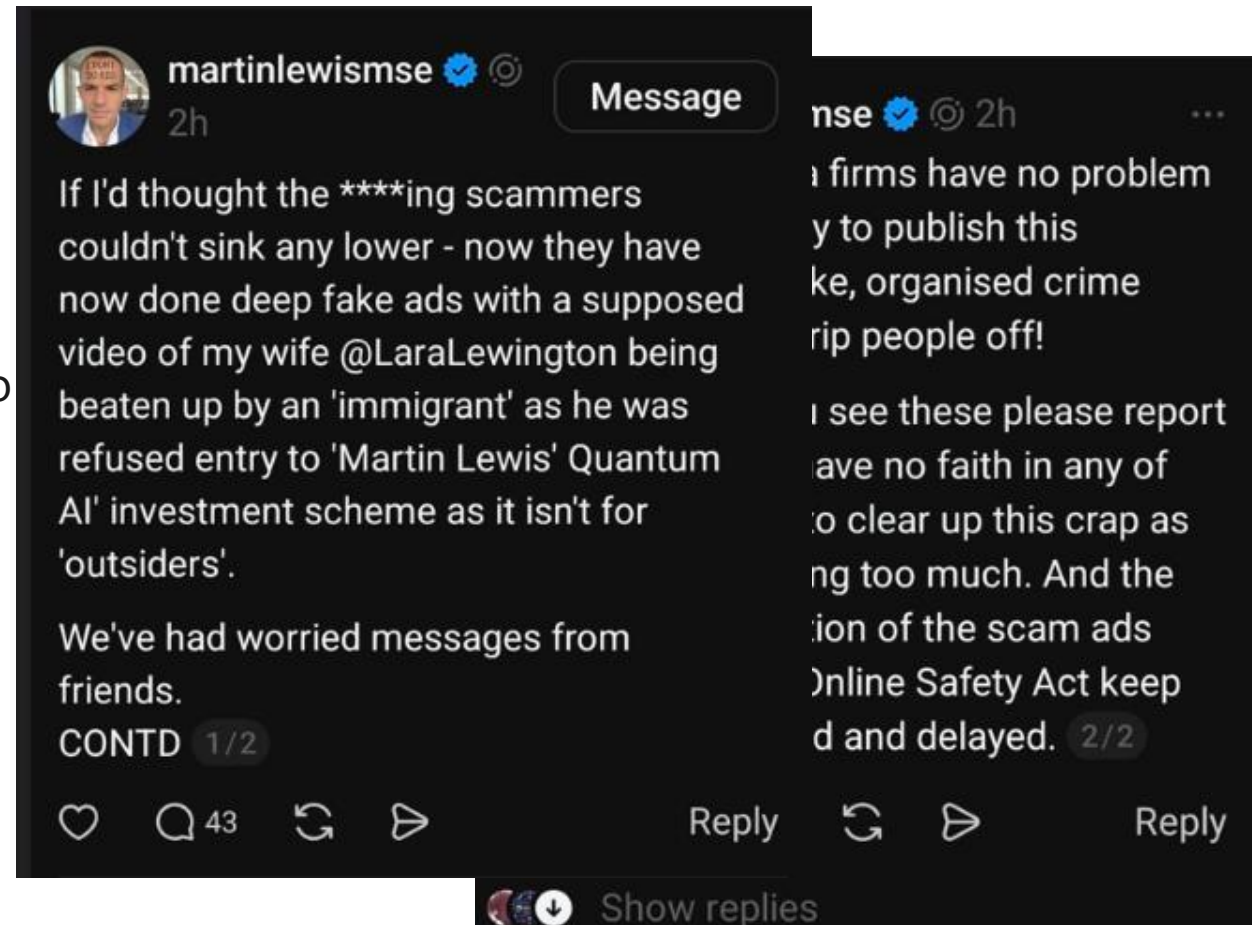
As AI evolves, staying ahead of these threats requires stronger detection strategies and awareness efforts.



AI-Powered Deepfakes

Deepfakes, which are AI-generated synthetic media (pictures, videos, audio), pose significant risks in the realm of hacking.

A finance employee in Hong Kong was tricked into transferring \$25 million using deepfake technology. Scammers created a fake video conference with the company's CFO and other executives, convincing the employee to send the funds. They used past video footage and AI-generated voices and videos to make the deception convincing.



Let's dive into some hacks

Passwords – How to hack a password



Password Attacks

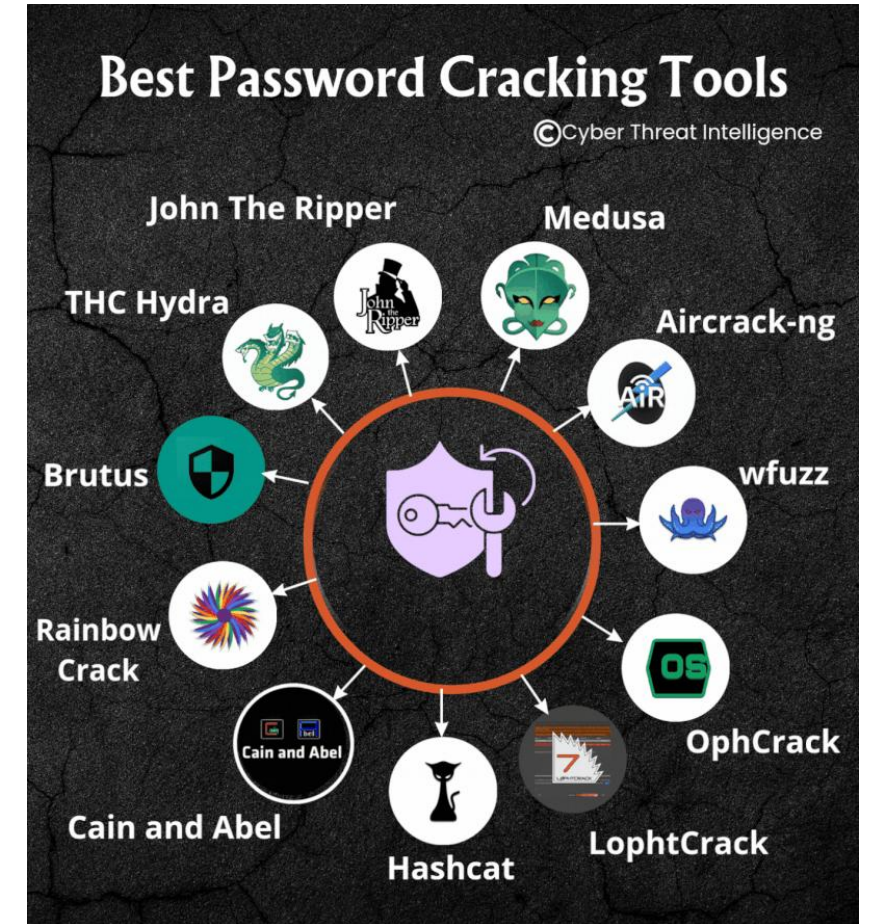
Password Cracking

Hackers don't guess. They *crack*.

How do they do this? (not an exhaustive list)

1 st	Breached passwords* - credential stuffing
2 nd	Most commonly used passwords
3 rd	Dictionary & Rainbow Table attack
4 th	Brute Force - every character possibility

*+Variations . Yes, I know you **CAPITALISED** the first letter and put a "1" & "!" at the end to comply with complexity requirements. *It won't help you.*



Ccompromised data

What Happened

In May 2019, the graphic design tool website [Canva suffered a data breach](#) that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised Data

- Email addresses
- Names
- Usernames
- Geographic locations
- Passwords



Canva

May
2019

In May 2019, the graphic design tool website [Canva suffered a data breach](#) that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data:

- Email addresses
- Geographic locations
- Names
- Passwords
- Usernames

[View Details](#)

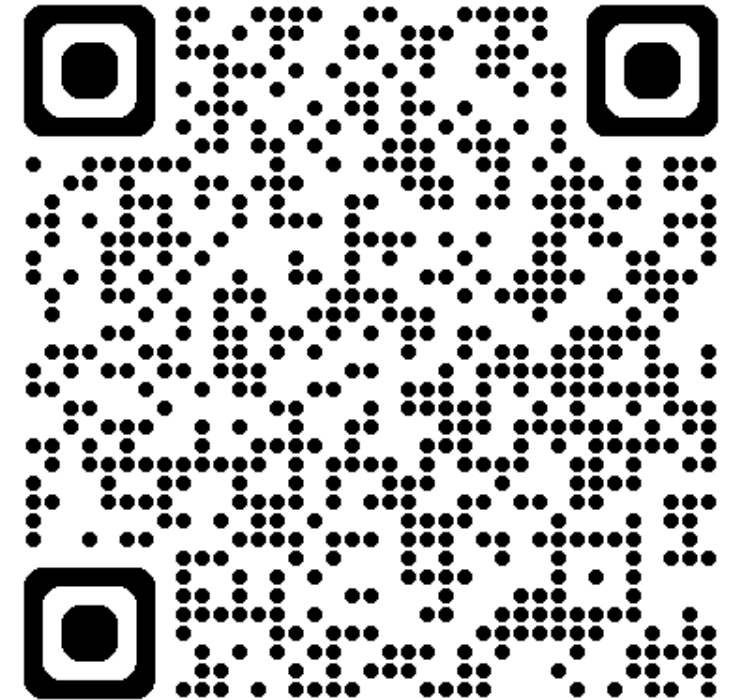


Have I Been Pwned

CHECK FOR BREACHED PASSWORDS NOW



Don't panic if your email is found; monitor for social engineering attempts based on the data leaked, change any breached passwords, and update any recycled passwords.



haveibeenpwned.com



Top 50 Passwords

123456	1234567890	123456a	123abc	zxcvbnm
123456789	123123	654321	1q2w3e4r	1g2w3e4r
qwerty	000000	123321	qwe123	gqwerty
password	iloveyou	666666	7777777	zag12wsx
111111	1234	1qaz2wsx	qwerty123	gqwerty123
12345678	1q2w3e4r5t	myspace1	target123	555555
abc123	qwertyuiop	121212	tinkle	*uckyou
1234567	123	homelesspa	987654321	112233
password1	monkey	123qwe	qwerty1	asdfghjkl
12345	dragon	a123456	222222	1q2w3e

www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt



Password Attacks – TECHNICAL ALERT

Dictionary vs Rainbow Table Attacks

A dictionary attack uses a list of common words, phrases and variants to try and guess passwords.

A rainbow table attack uses tables of password hashes to quickly find matches.

Rainbow tables can be faster than dictionary attacks if the password hash is within the table but take a LOT of computer space.

Dictionary attacks are simpler to execute but often a slow process.

NB: Throttling can thwart these attacks on live systems only (not offline)



password
Password
Password!
Pa55word
p4ssword



"password"

MD5: 5f4dcc3b5aa765d61d8327deb882cf99

SHA-1: 5baa61e4c9b93f3f0682250b6cf83017b16455da

SHA-256: 5e8848994616f1c0f9526c3f21315e2e7e68f26d



Password Attacks

Brute Force

Trying every possible character in every possible combination until the correct password is found.

Number of Characters	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	15 bn 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	100 tn years	7qd years

**TIME IT TAKES
A HACKER TO
BRUTE FORCE
YOUR
PASSWORD**



-Data sourced from [HowSecureismyPassword.net](https://howsecureismypassword.net)



Strong Passwords

Three random words	Make you passwords long and complex. Three random words (plus numbers and symbols), ensure your password is long but easily memorable.
Separate passwords for each account	Reusing passwords, or similar passwords allows hackers to gain access to multiple accounts
Password manager	Dedicated password managers or browser-based password managers are a great tool for remembering passwords.
Write passwords down (yes really)	Writing passwords down helps to remember them. Make sure it is secure and private, no post-it notes!
Check for data breaches	Check Have I Been Pwned regularly and updates accounts as needed.

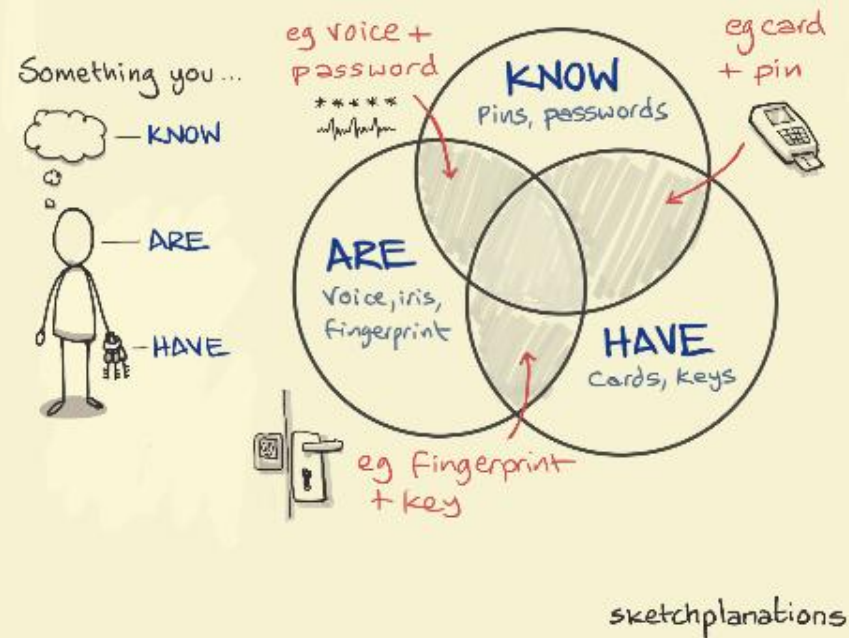


**Multi-factor Authentication – Hackers
can beat this as well**



2 FACTOR AUTHENTICATION

IDENTIFYING USING 2 OF THESE 3 FACTORS



Three threat-paths hackers use to negate MFA

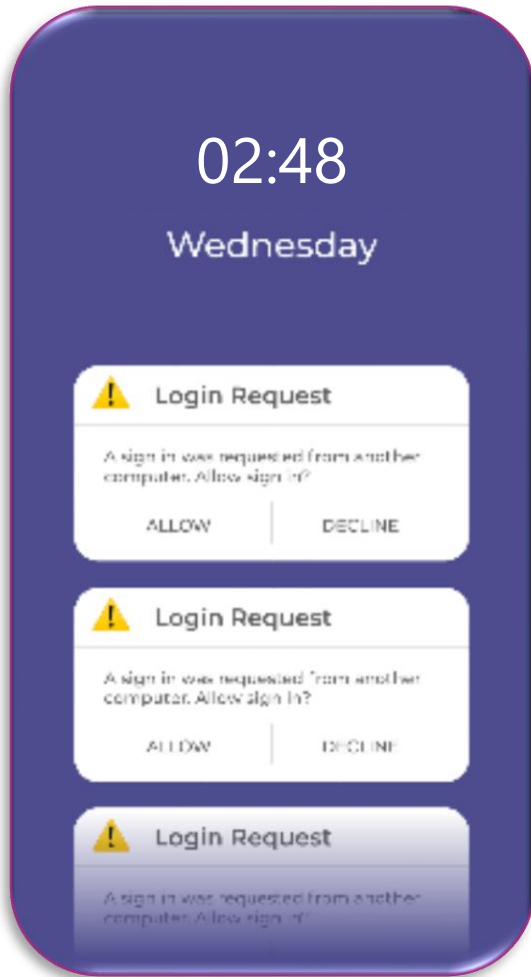
- ❖ Pester Power
- ❖ SIM Swap
- ❖ Token Theft

Image: Jono Hey, Big Ideas Little Pictures, Media Lab Books & sketchplanations.com



❖ Pester Power

British politeness: defeating MFA one “yes, that’s probably me” at a time.



- Hackers just keep sending you MFA prompts until you get fed up and hit “ALLOW”
- You’re busy, distracted, or it’s 3 o’clock in the morning – perfect time for them to strike
- You think it’s a glitch... but it’s a hacker, knocking, over and over and over again.
- Shhh... just tap that little **Allow** button and you can have peace and go back to sleep.



❖ Sim Swap – **TECHNICAL ALERT**

Why hack your phone when they can just be your phone

- They trick your mobile provider into giving *me* control of your number
 - *Steal your credentials*
 - *Social engineer the provider*
- Now your MFA texts goes to *their* phone, not yours
- You won't even know their there – until it's too late

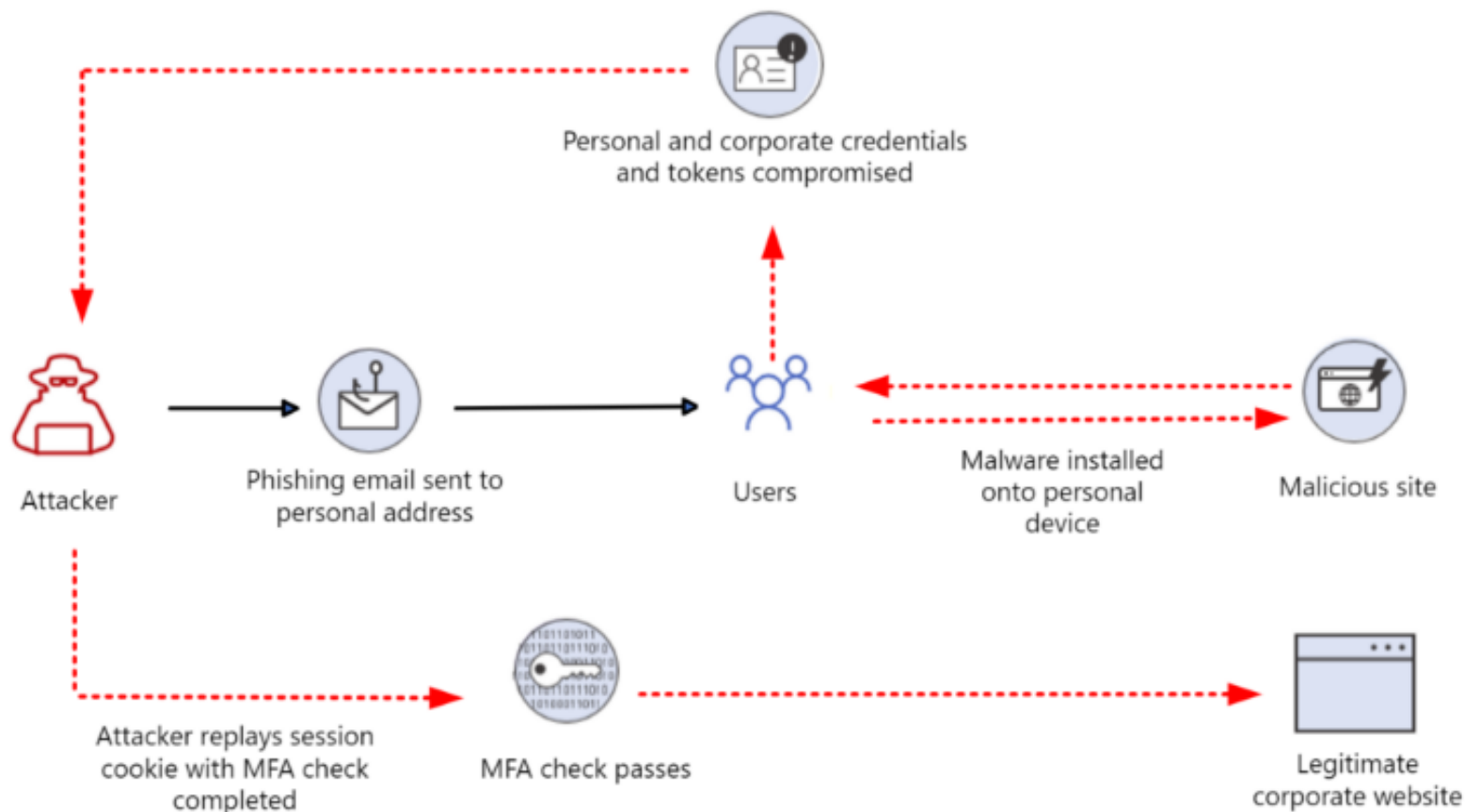


"Hi, is that Vodafone? I'm sorry - this is a bit of an emergency..."
"I work in social care, and I dropped my work phone in the sink during a visit this morning. The SIM's completely dead and I've got safeguarding calls I can't miss."
"I've picked up a new SIM already-I just need my number moved over as soon as possible."
"I can give you the number, my postcode, whatever you need-I'm just really up against it."
*"I've got a call with safeguarding in the next half hour, and if I miss that, it delays care for a really vulnerable adult... **please please can you help me?**"*



**WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES**

❖ Token Theft – TECHNICAL ALERT (NO FOR REAL THIS TIME)



- If a device is “trusted” or remembered, the site issues a session token.
- That token says “yup, still you” - so I can access the account without re-entering credentials or MFA.
- In effect: I don’t need to log in again - the system thinks the legitimate user is still present.



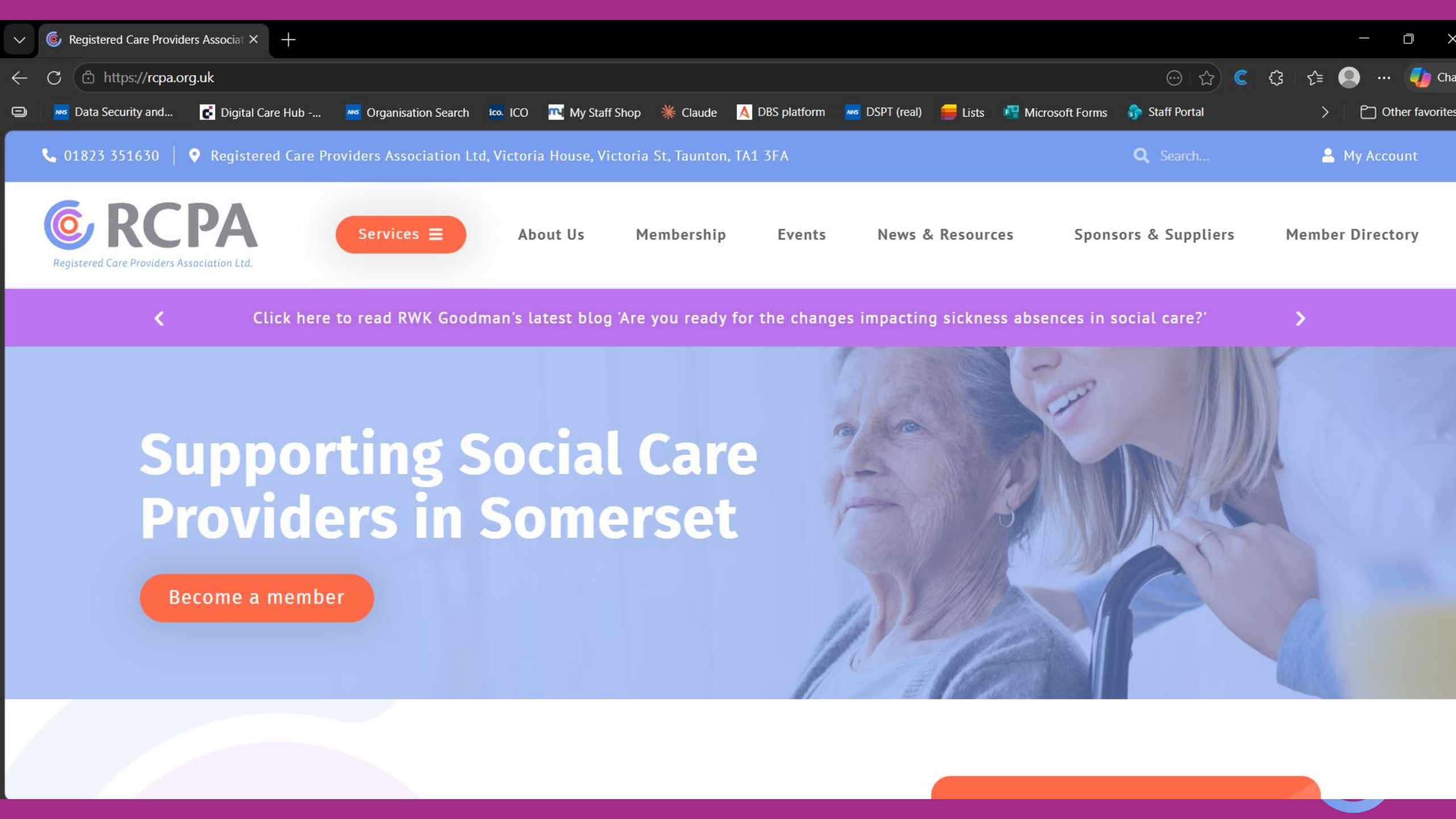
MFA best practice

Pester Power	Avoid MFA which is just a “hit yes it’s you” – go for a number generator. Number generators don’t pester you.
Sim Swap	SMS/text-based based MFA is less secure than authenticator-based versions (Google Authenticator or Microsoft Authenticator) Be wary of social engineering attempts “Hi, to authenticate I’m real, I’m going to send you a code now...”
Token Theft	Always use secure websites (look for HTTPS ) Don’t click dodgy links Avoid public Wi-Fi Log out of important accounts when finished Device updates/passwords/MFA



**Want to see
some hacking?**





Click here to read RWK Goodman's latest blog 'Are you ready for the changes impacting sickness absences in social care?'



Supporting Social Care Providers in Somerset

Become a member

Registered Care Providers Associat X

+

←

↺

https://rcpa.org.uk

AMS Data Security and...

Digital Care Hub -...

AMS Organisation Search

ico. ICO

My Staff Shop

Claud

01823 351630

Registered Care Providers Association Ltd, Victoria House, Victoria St, Taunt



RCPA

Registered Care Providers Association Ltd.

Services

About Us

Membersh

←

RCPA Members Bulletin - 10th April 2026. Please rea

Supporting Social Car

Providers in Somerse

Become a member

https://rcpa.org.uk/#link-popup

Registered Care Providers Associat X

+

←

↺

File C:/Users/DanielPlummer/OneDrive%20-%20Registered%20Care%20Providers%20Association%20L

AMS Data Security and...

Digital Care Hub -...

AMS Organisation Search

ico. ICO

My Staff Shop

Claud

01823 351630

Registered Care Providers Association Ltd, Victoria House, Victoria St, Taunt



RCPA

Registered Care Providers Association Ltd.

Services

About Us

Membersh

Click here to read o

Supporting Social Car

Providers in Somerse

Become a member

file:///C:/become-a-member/

out the RCPA

rcpa

Search Domains

RESULTS

HISTORY

FAVORITES

PREMIUM DOMAINS

DOMAIN TAKEN

rcpa.co.uk

We might be able to help you get it. [See How](#)

Broker Service Fee

£77.99

Hire a Broker

See More

GREAT ALTERNATIVE

rcpa.info

£32.99

£1.84

1st yr only with 2 yr term

Make It Yours

We found 554 domain endings for "rcpa"

View all TLDs

Domains include free Privacy Protection forever.

dd.

Every 7 minutes someone bought a .IO from GoDaddy.

Every 9 minutes someone bought a .ME from GoDaddy.

Every 2 minutes someone bought a .ONLINE

Explore rcpa Endings

See All

DOMAIN TAKEN

.com

Broker Service Fee

£77.99

DOMAIN TAKEN

.net

Broker Service Fee

£77.99

PREMIUM

020 7023 9939 for help

.org

£3,695.15

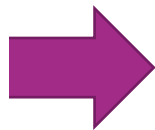
.AI IS TRENDING

.ai

£119.99

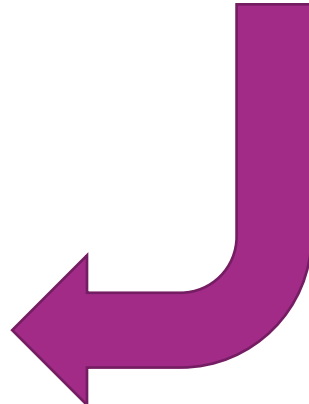
£35.99

1st yr only with 2 yr term



rcpa-ltd.co.uk

~~£12.99~~ £0.01
1st yr only with 3 yr term



←

↺

https://rcpa-ltd.co.uk

< Connection is secure

✕

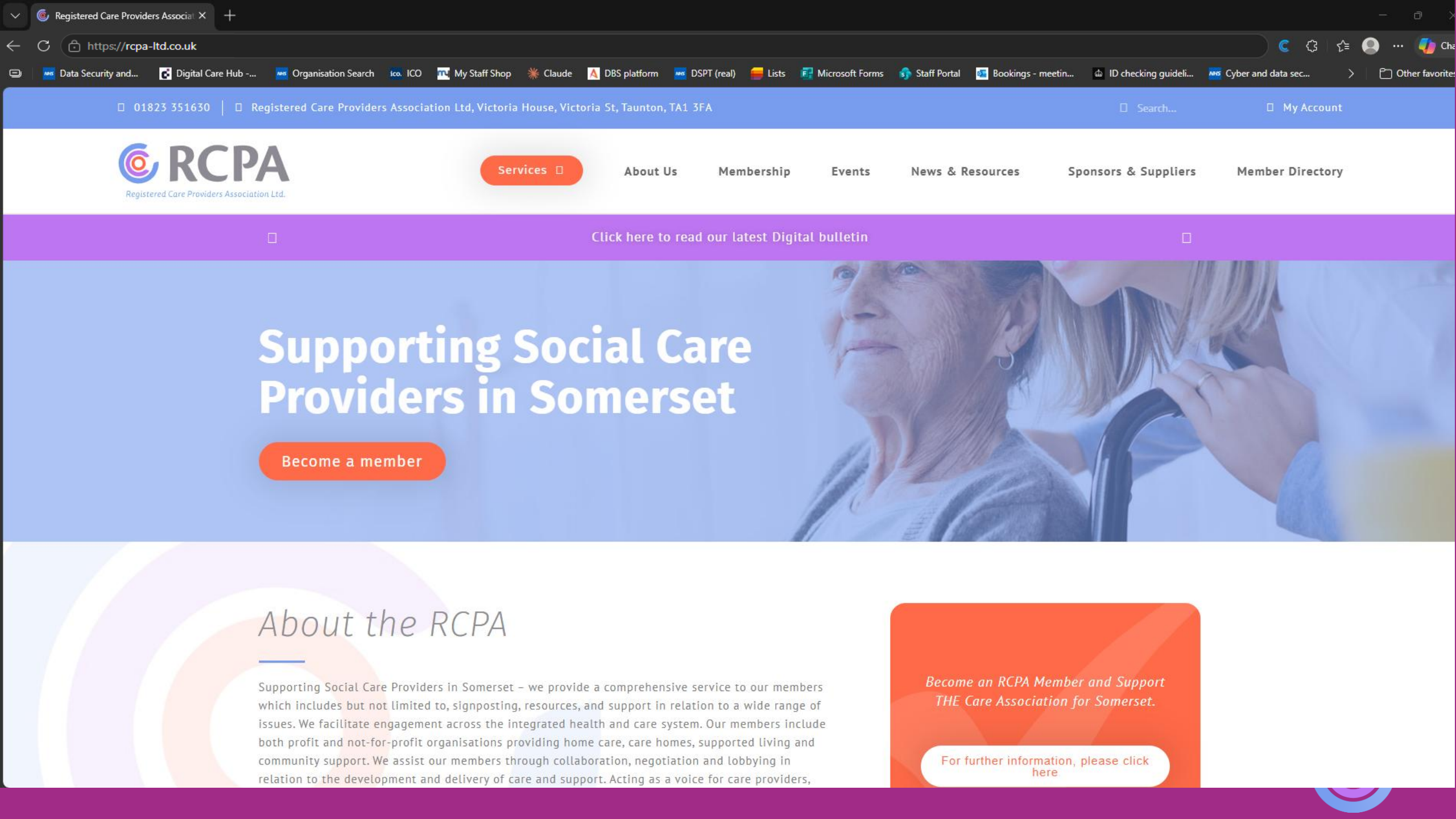
This site has a valid certificate, issued by a trusted authority.

This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.

Always be sure you're on the intended site before entering any information.

[Learn more](#)





Services

About Us

Membership

Events

News & Resources

Sponsors & Suppliers

Member Directory



[Click here to read our latest Digital bulletin](#)



Supporting Social Care Providers in Somerset

[Become a member](#)

About the RCPA

Supporting Social Care Providers in Somerset – we provide a comprehensive service to our members which includes but not limited to, signposting, resources, and support in relation to a wide range of issues. We facilitate engagement across the integrated health and care system. Our members include both profit and not-for-profit organisations providing home care, care homes, supported living and community support. We assist our members through collaboration, negotiation and lobbying in relation to the development and delivery of care and support. Acting as a voice for care providers,

*Become an RCPA Member and Support
THE Care Association for Somerset.*

[For further information, please click
here](#)

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

From Name:

From E-mail:

To:

Subject:

Attachment: No file chosen

Reply-To:

Errors-To:

Cc:

Bcc:

Priority: ☐ Low ☒ Normal ☐ High

X-Mailer:

Confirm delivery:

Confirm reading:

Add Header:

SMTP Server: **Port:**

Date: ☒ Current
☐ Delay sending to the specified time (future only)

Charset:

PGP/GPG Encrypt: ☒ No ☐ Yes ☐ Do not encrypt attachments

Receiver's Public Key:

Technical alert

Email spoofing exploits vulnerabilities in email systems by allowing me to alter fields beyond just the body and “To:” line, including ;

- Mail from:
- Name from:
- Reply-to:
- Errors-to:
- Date:

scammy@scam.scam >
official@official.com



Who will I email? Open-source intelligence

For Open Source Intelligence (OSINT) Professionals



Social Links Crimewall

- Perform OSINT and SOCMINT across 500+ sources
- Graph, table, and map visualizations for key insights
- ML-driven analysis & real-time monitoring



Usersearch 2.0

- 35+ built-in investigative capabilities, no scripts or coding
- All APIs and services pre-integrated, no API keys
- Video guides and investigation tips in the dashboard



GeoSpy.ai

- Transform images into precise intelligence with AI
- Advanced geospatial AI for city and national monitoring
- From global coverage to street-level precision



OSINT Industries

- Unified profiles by linking emails, phones, usernames, etc.
- Map movements, trace timelines, and flag breaches
- Discover registered accounts across platforms



Maltego Monitor

- Monitor social media, news, and blogs in one interface
- Track specific regions, topics, or crises for tailored insights
- Custom dashboards for events, topics, and regions



Horizon Identity

- Correlate multiple identifiers into unified, reliable profiles
- Instantly resolve identities for subject profiling
- Eliminate manual research with fast identity intelligence



Talkwalker

- Track keywords and mentions across 30 social networks
- Monitor 150+ million websites, forums, blogs, and news
- Discover mentions in videos, images, podcasts, etc.

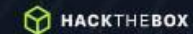


Intelligence X

- Search billions of selectors across emails, domains, IPs...
- Access darknet sources, data leaks, paste sites, archives
- Perform fast OSINT with deep global coverage



Alex Lozano



10 OSINT TOOLS FOR HACKERS

Shodan

Search engine of discoverable network devices on the Internet.

Maltego

View data in graphs to make relationships stand out.

Google Dorks

Advanced Google queries to find exactly what you are looking for.

Recon-ng

Metasploit-like interface to run many OSINT tools.

Ahmia.fi

Google for the dark web. Great tool for OSINT forensics.

Wayback Machine

View old versions of websites. Going way back into the 1990s.

theHarvester

Automatically download emails, usernames from a company.

TinEye

A search engine based upon images instead of text.

OSINT Framework

The best way to find information about specific types of OSINT.

Local Library

Not all OSINT tools are online. Check your local library. It has hidden gems!

TIP 1

KEEP YOUR EYES OPEN!

Some things are right here in the target's website/social.

TIP 2

MAKE SURE YOU CHECK ALL DOMAINS AND SUBDOMAINS

One great tool is: <https://github.com/gfek/Lepus>

TIP 3

TIME TO STUDY!

Module: "OSINT: Corporate Recon"

Difficulty: **Hard**

Created by: Cry0l1t3

**OSINT:
Corporate
Recon**



AI is so clever and willing to help

Here's a realistic example phishing email rendered as it would appear in an inbox — perfect for training purposes. Key red flags are highlighted so you can walk participants through them.

From Security Notifications <noreply@securityalert-notifications.co> suspicious domain
To you@yourcompany.com
Subject [Important] Data breach notification — action required
Date 14 April 2026, 09:12

Dear Customer,

We are writing to inform you that we recently identified unauthorised access to systems associated with our platform. During this incident, some customer data — including email addresses and encrypted passwords — may have been accessed by an unauthorised third party.

We take the security of your data very seriously. In accordance with our obligations under the UK GDPR, we have reported this incident to the Information Commissioner's Office (ICO) and are cooperating fully with their investigation.

To review the full details of this incident, understand what data may have been affected, and access guidance on protective steps you can take, please visit our dedicated security update page:

Link shown in email

<https://security-update-notice.com/breach-notice/verify?token=a9f3d2>

unrelated domain



No connection to any legitimate sender domain — a generic-sounding URL designed to appear official.

Want to be notified when Claude responds?

Notify

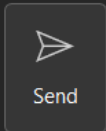


Reply...



Sonnet 4.6





Send

To

Cc

Bcc

Subject

IMPORTANT NOTICE - DATA BREACH

Dear provider,

We are writing to inform you that we recently identified unauthorised access to systems associated with our platform. During this incident, some data; including email addresses and encrypted passwords, may have been accessed by an unauthorised third party.

We take the security of your data very seriously. In accordance with our obligations under the UK GDPR, we have reported this incident to the Information Commissioner's Office (ICO) and are cooperating fully with their investigation.

To review the full details of this incident, understand what data may have been affected, and access guidance on protective steps you can take, please visit our dedicated security update page:

Link shown in email www.rcpa-ltd.co.uk ← THIS IS A LINK TO THE FAKE WEBSITE

For your security, we recommend you change your password.

You may also find advice about protecting yourselves after a data breach from the National Cyber Security Centre. [Cyber security advice for small to medium sized organisations](#) | [National Cyber Security Centre - NCSC.GOV.UK](#)

We sincerely apologise for any concern this may cause.

Kind Regards

Hilary Robinson RGN, LLB (Hons), MSc Adv HCP (Open).

CEO

RCPA Ltd

Tel: 01823 351 630 (central office)



YOU'VE BEEN HACKED!

Worried?

So... how DO YOU defend against Cyber Sam and hackers?



Strong passwords



Use separate password for each account. If you share passwords between accounts, hackers only need one password to access multi accounts.

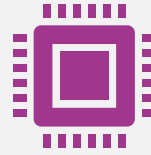


Passwords should be three random words. Three random words are hard to guess and long enough to not be easily cracked while also being simple enough to remember.



Use a password manager (yes even the browser ones)

Multifactor authentication



Turning on MFA is one of the most effective ways to protect your online accounts from hackers.



A PIN or code will be sent via text or email that allows you confirm you're the person trying to access your account. App based authentication is better.



Even if your password is compromised, MFA adds a second layer of defense that stops hackers from getting into your account.

Updates



Installing updates as soon as they become available is key to securing your devices and apps



When a company releases a patch, they also include patch notes. AKA here's the security issue.



What happens the day after a software update is released?

Suppliers



Do they have a cyber security certification such as Cyber Essentials, ISO27001, SOC3 or DSPT?
Get proof, an image can be copied and pasted.



Partnered/supplier or vendor with is jargon.
Partnered with Microsoft or Cisco does not equal cyber certification.



IT support does not equal cyber security. Your IT support company are not necessarily cyber experts.

DSPT & Cyber Resilience *aka The Hacker's Nightmare!*

DSPT Evidence Item	Hacker Nightmare
4.2.4 Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	It's much harder for hackers to use stolen credentials
4.5.4 How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?	It will take hackers forever to breach a strong password; they'll give up and try something else
<u>6.2.1 Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?</u>	Any off-the-shelf malware will be picked up immediately; hackers need to rethink their payload
7.3.4 Are backups routinely tested to make sure that data and information can be restored?	Even if they manage to deploy some malware – they could back up and running in no time
8.3.5 How does your organisation make sure that the latest software updates are downloaded and installed?	None of their software is showing as vulnerable in their scans, NEXT!
9.5.2 Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	The hacker stole this tablet from an exhausted carer on the bus, and they can't do anything with it
10.2.1 Do your organisation's IT system suppliers have cyber security certification?	They've chosen a managed service provider who knows what the hackers are up to – they'll moving on!



Data Security and Protection Toolkit

Deadline to publish and republish is June 30th

Data Security Health Check. A free review of your data and cyber security, includes a technical check for basic cyber security.





Questions?

Daniel.plummer@rcpa.org.uk

07761043433

