

GAC Capacity Development Workshop on DNS Abuse

DNS Security Threats reported to Law Enforcement, and by Law Enforcement

Chris Lewis-Evans (UK National Crime Agency, Co-Chair GAC PSWG)

Gabriel Andrews (US Federal Bureau of Investigation, GAC PSWG member)

ICANN77

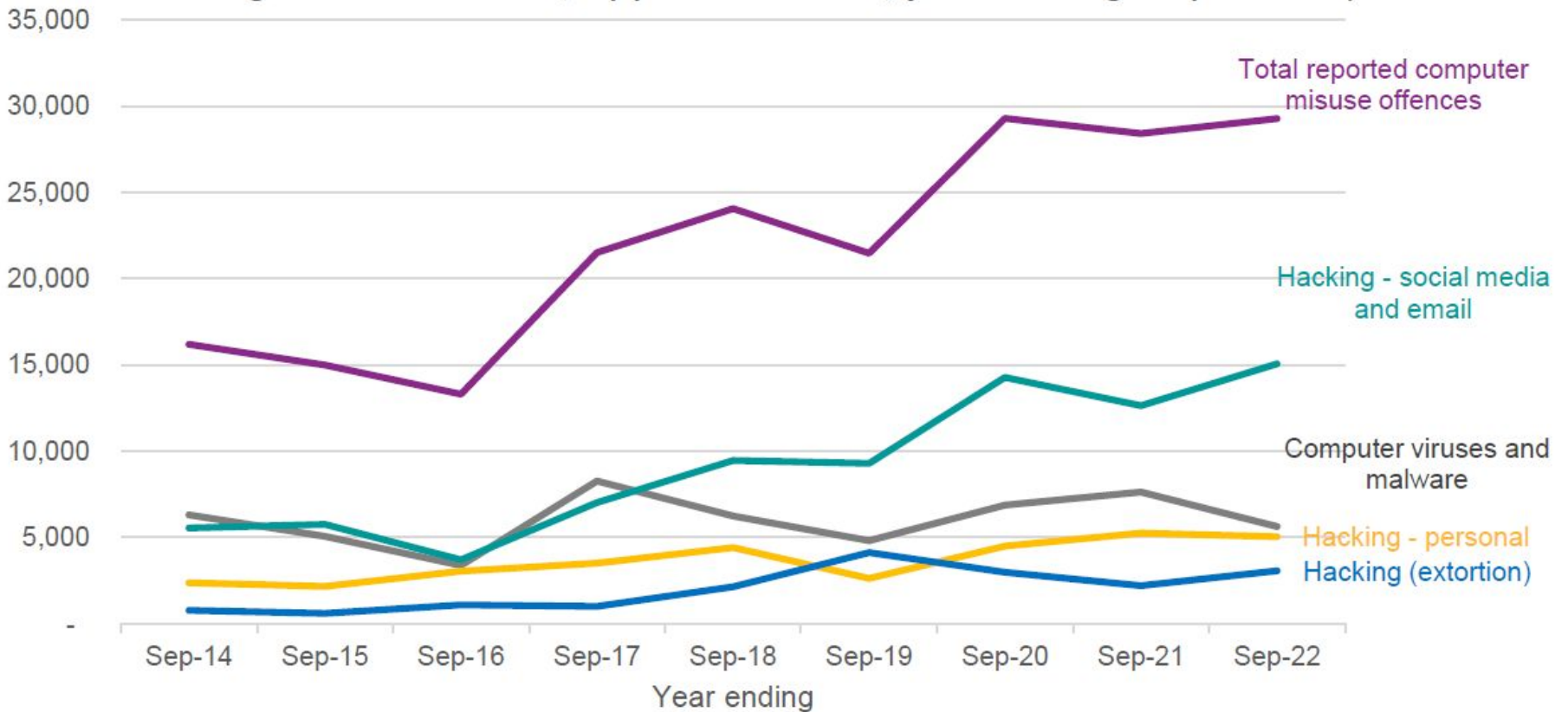
11 June 2023

I C A N N | G A C

Governmental Advisory Committee

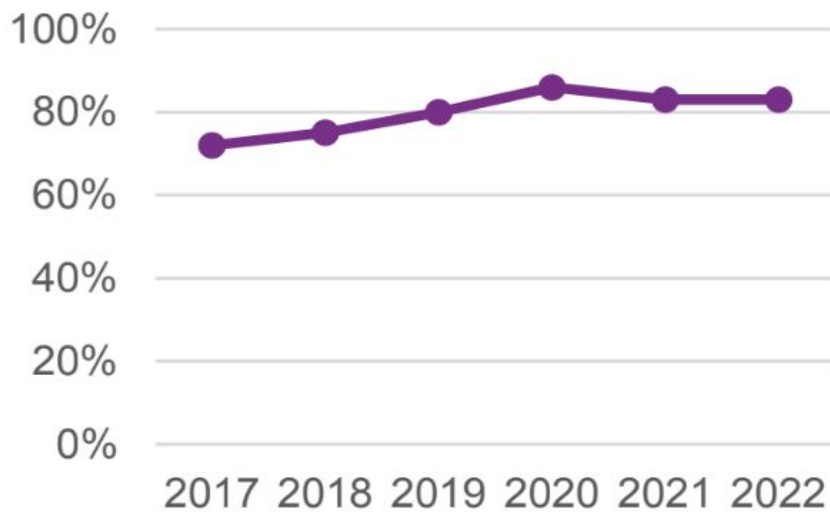
UK - Reporting Volume

Computer misuse offences reported to Action Fraud (Crime in England and Wales, Appendix tables, year ending September)

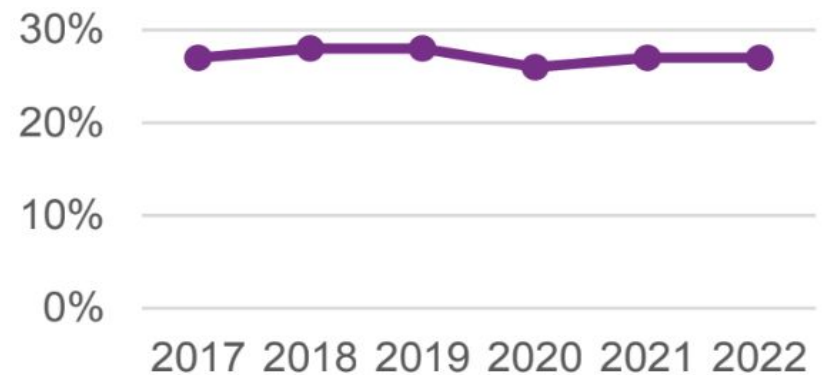


UK - Business breaches

Businesses - % among those who identified a breach who identified an attack vector of phishing



Businesses - % among those who identified a breach who identified an attack vector of others impersonating organisation in emails or online



UK Action Fraud

- Action Fraud is the UK's national reporting centre for fraud and cyber crime.
- In 2020 - 2021 (most recent public report)
 - Action Fraud received 875,622 reports of fraud
 - leading to £2.35bn reported losses.
- 80% of reported fraud was cyber enabled.
- The report identified phishing emails as the key enabler for criminals to initiate cyber attacks and fraud

U.S. Internet Crime & Complaint Center (IC3.gov)

Complaints and Losses over the Last Five Years*

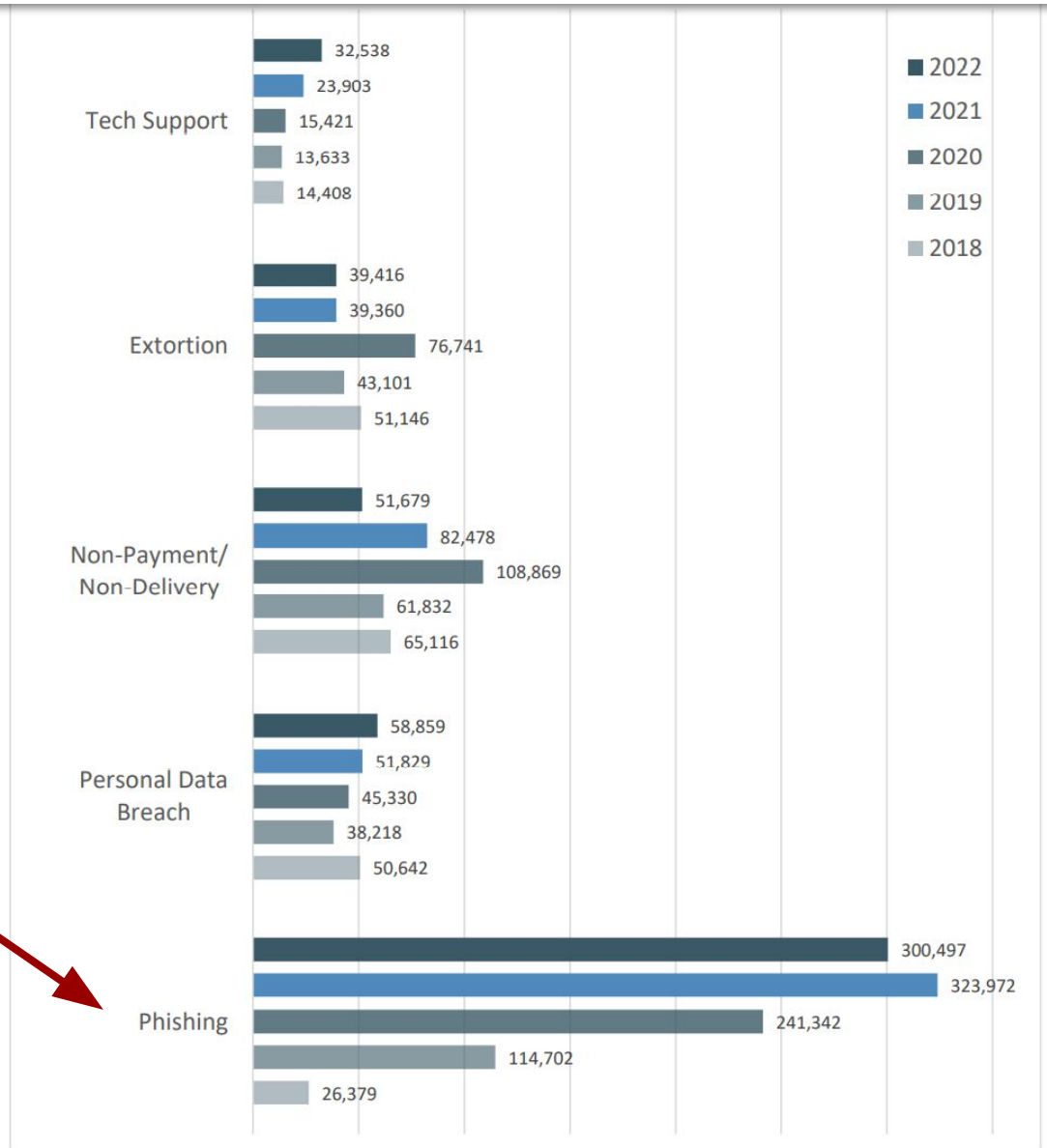


IC3.gov Top 5 Types of Internet Crime (past 5 Years)

“DNS Abuse”
is not tracked as a
category.

BUT...

There are categories of
DNS Abuse which *are*
tracked in IC3 reports:



Case Study - Phishing

- Information received from Police report that a victims social media account had been hacked.
- The victim who was a 17 year old reported that the hacker was asking for more passwords.
- They reported loss of accounts including Snapchat, Instagram, TikTok and their Gmail account.
- Suspect identified
- History of hacking social media
- Warrant at home address finding active phones.
- Evidence on mobile phones of mass phishing.

Case Study - Phishing

The Suspect used the phones to send out hundreds of phishing messages to young girls. The accounts used were hacked accounts of other young girls.

From [REDACTED] rio (owner)

Hi hun, sorry to bother you but I'm not sure if you are aware but theres a website that is posting inappropriate pictures of girls without their permission and one post claimed to be yours, I'm only messaging you about it because it has your socials linked

27/06/2022 10:39:14(UTC+1)

From [REDACTED] Chlo ▼

Can u send me the link?

24/06/2022 05:43:43(UTC+1)

From [REDACTED] rio (owner)

[https://cl\[REDACTED\]m/ZW5\[REDACTED\]N3YxWjQw](https://cl[REDACTED]m/ZW5[REDACTED]N3YxWjQw)

24/06/2022 06:05:11(UTC+1)

Case Study - Phishing

Sign-In

username
password
Remember me
Forgot password
Log In

Don't you have account yet? Click on here
Do you need help? Watch the video to see our guide which helps you to use our site

OUR WEB SITE

- Larvana

SOCIAL MEDIA

- Tutorials
- Telegram

Dashboard / Online Scams

ONLINE SCAMS
FRIENDLY WEBSITE: [LARVANA.COM](#)

- Facebook Home
- FB Color Change (Pwnd)
- Facebook Mobile
- FREE FIRE - GARDIA
- BATTLEGROUND
- Messenger
- NETFLIX
- Facebook Profile Visitors
- Facebook Live Chat
- Clash Of Clans
- FREE FIRE Stone
- FREE FIRE Spin

Log In Snapchat

Username
Password
LOG IN

DASHBOARDS

- Home
- Victims
- Privacy Policy
- Backup Scams
- Chat view
- Change Password

OUR WEB SITE

- Larvana

SOCIAL MEDIA

- Tutorials
- Telegram
- Like us on facebook
- Contact us

VICTIMS

Victims steps only 1 month | Always download your victims |
Show 10 entries

ID	Schema Desc	User name	User Pass	Victime date	Victime Ip	Country	Option
[REDACTED]	Snapchat	test	test	Tue 20 Sep 09:17	[REDACTED]	United Kingdom	0

Showing 1 to 1 of 1 entries

Previous Next

Now 100% Online | Online 100% | Carry 100% Online

Case Study: Reporting Phishing Attacks in the Real World

Here's a real domain (but redacted by me):

usaauth.**VENDOR.TLD**

Case Study: Reporting Phishing Attacks in the Real World

Here's a real domain (but redacted by me):

usaauth.**VENDOR.TLD**



Here's a phishing domain (also redacted):

usaauth-signin**VENDOR.TLD**

Case Study: Reporting Phishing Attacks in the Real World

Whois Record for **UsaAuth-SigniN** **VENDOR.TLD**

— Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	REDACTED FOR PRIVACY
Registrant Country	CH
Registrar	Registrar IANA ID: ### URL: http://www. URL Whois Server: whois. server abuse@ registrar.email (p) + 555-555-5555
Registrar Status	ok
Dates	4 days old Created on 2023-05-11 Expires on 2024-05-11 Updated on 2023-05-11
Name Servers	ARYANNA.NS.CLOUDFLARE.COM (has 26,036,787 domains) DILBERT.NS.CLOUDFLARE.COM (has 26,036,787 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY info@ registrar.email (p) REDACTED FOR PRIVACY xREDACTED FOR PRIVACY (f) REDACTED FOR PRIVACY xREDACTED FOR PRIVACY
IP Address	104.21.31.155 - 739 other sites hosted on this server
IP Location	 - California - San Jose - Cloudflare Inc.
ASN	 AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)



Summary of facts:

1. Domain looks like an important login portal to a federal agency
2. Vendor is target of ongoing phishing attacks
3. Domain is newly created (reported within 1 day of registration by Law Enforcement)

Case Study: Reporting Phishing Attacks in the Real World

Whois Record for **UsaAuth-SigniN** **VENDOR.TLD**

— Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	REDACTED FOR PRIVACY
Registrant Country	CH
Registrar	Registrar IANA ID: ### URL: http://www. URL Whois Server: whois. server abuse@registrar.email (p) +555-555-5555
Registrar Status	ok
Dates	4 days old Created on 2023-05-11 Expires on 2024-05-11 Updated on 2023-05-11
Name Servers	ARYANNA.NS.CLOUDFLARE.COM (has 26,036,787 domains) DILBERT.NS.CLOUDFLARE.COM (has 26,036,787 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY info@registrar.email (p) REDACTED FOR PRIVACY xREDACTED FOR PRIVACY (f) REDACTED FOR PRIVACY xREDACTED FOR PRIVACY
IP Address	104.21.31.155 - 739 other sites hosted on this server
IP Location	 - California - San Jose - Cloudflare Inc.
ASN	 AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)

Presentation Note: Reported to Registrar, Registry, Cloudflare, & Host on 2023-05-12

Desired Action:

Registrar (clientHOLD)
and/or
Registry (serverHOLD)

What happened:

May 12 - **Cloudflare** adds interstitial warning of fraud

May 14 - **Registry**: ‘as we don’t host nor register the domain’, ‘not in position to act’ absent a court order

May 15 - **Registrar** “we are merely the registrar” and don’t control use of the domain, will notify Reseller

May 16 - **Registrar** confirms Reseller deleted domain.

Case Study: Reporting Phishing Attacks in the Real World

>> so why not get a court order?

>> if domain is suspended by the *Registrar* or *Registry*, is the domain still dangerous?

>> if the content *Host* removes the content, is the domain still dangerous?

Taking action “at the DNS Level”...

... vs at “Hosting Level”



<u>DOMAIN NAME</u>	<u>TTL</u>	<u>TYPE</u>	<u>RECORD</u>
RALNBOWBANK.COM.	160	A	101.14.66.2
RALNBOWBANK.COM.	160	A	222.14.10.4
RALNBOWBANK.COM.	160	A	23.124.228.102
RALNBOWBANK.COM.	160	A	101.14.66.22



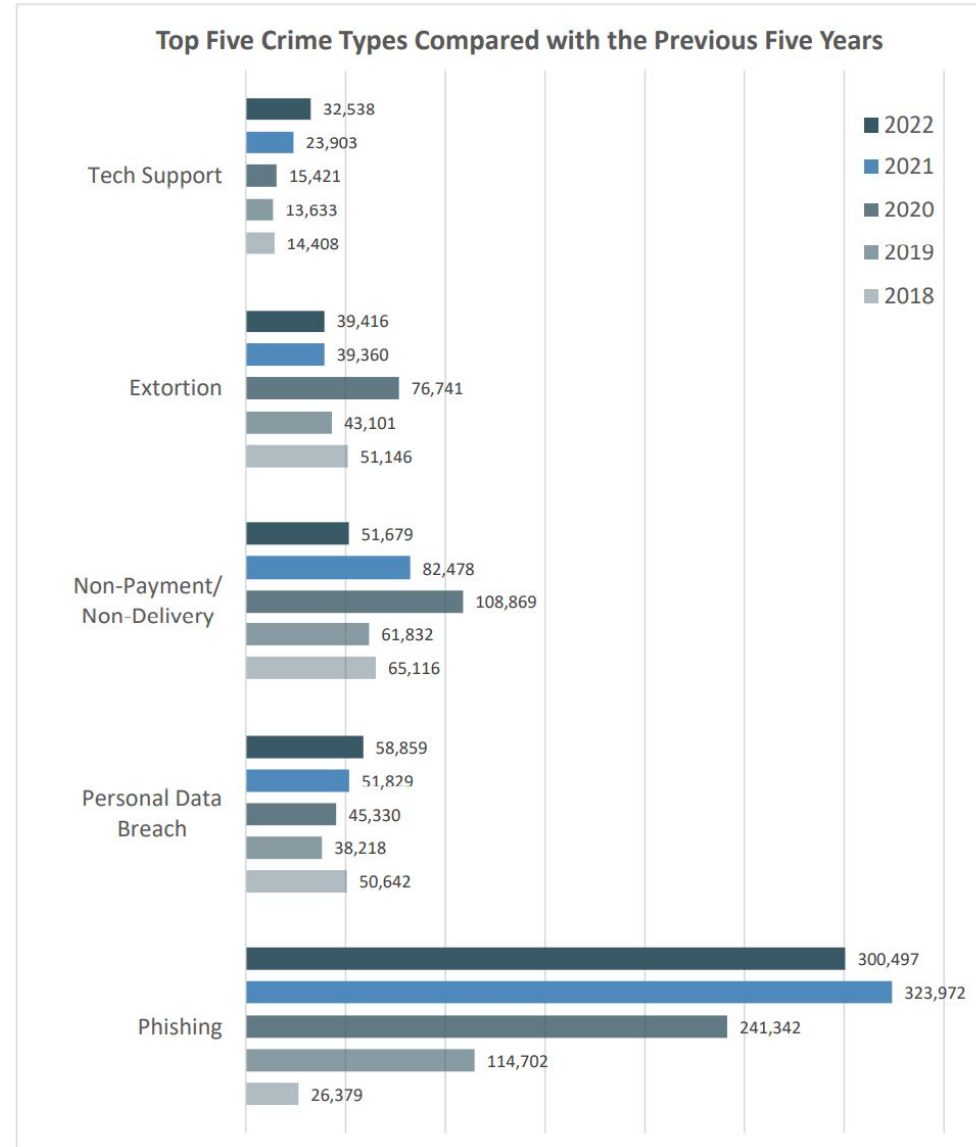
**Registrar &
Registry**
control this



Hosting Provider
controls this

Key Takeaway

- **Phishing** is DNS Abuse
- **Phishing** is top reported Internet crime
- **Phishing** *enables* many other crimes
- Swift action against Maliciously Registered Domains has **BIG IMPACT** on DNS Abuse (and cybercrime)



Prior GAC Contributions on DNS Abuse

- [GAC Statement on DNS Abuse](#) (18 Sep. 2019)
 - *Protecting the public from security threats and DNS Abuse is an important public policy issue.*
 - *If the public is to trust and rely upon the Internet for communications and transactions, those tasked with administering the DNS infrastructure must take steps to ensure that this public resource is safe and secure.*
- Since the GAC's endorsement of the Law Enforcement Due Diligence Recommendations ([Brussels Communiqué](#), June 2010) the GAC has continuously sought to increase the effectiveness of ICANN contracts and their enforcement in mitigating DNS Abuse with Registrars ([Dakar Communiqué](#), Oct 2011) and with New gTLD Registries ([Beijing Communiqué](#) Safeguards Advice, Apr. 2013)
- In the [Beijing Communiqué](#) Safeguards Advice (11 April 2013) the GAC advised that “six safeguards should apply to all new gTLDs and be subject to contractual oversight” including:
 - **Security checks** — *While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate **security threats, such as pharming, phishing, malware, and botnets**. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.*

END

/Questions?