

# DNS Abuse Mitigation

Gabriel Andrews (US Federal Bureau of Investigation)

Lauren Kapin (US Federal Trade Commission, Co-Chair GAC PSWG)

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

ICANN76

14 March 2023

**ICANN | GAC**

Governmental Advisory Committee

# Agenda

---

- 1. Introduction and overview by GAC Topic Leads**
- 2. Presentation by Internet & Jurisdiction Policy Network**
- 3. Presentation on Cybercrime Statistics**
- 4. Ongoing Activities in the ICANN Community**
- 5. Considerations for Cancún Communiqué**

# DNS Abuse Mitigation: Importance

## Why this is important for the GAC

- **Existing definitions of Abuse of the DNS** include Security Threats such as *Phishing, Malware, Botnets* ([GAC Beijing Safeguard Advice](#)) and as *“intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names”* (CCT Review definition quoted in the [GAC Statement on DNS Abuse](#), 18 September 2019) **constitute**:
  - **A threat to consumers and Internet users** (individual and commercial) and their trust in the DNS
  - **A threat to the security, stability and resiliency of DNS Infrastructure**
- **The GAC established a Public Safety Working Group (PSWG)** in the [ICANN52 Singapore Communiqué](#) (11 February 2015)
  - to focus aspects of ICANN’s policies and procedures that implicate the safety of the Public (see [ToR](#))
  - As part of its strategic objectives, as reflected in its 2023-2024 Work Plan, the PSWG seeks to:  
**Support and develop capabilities of the ICANN and Law Enforcement communities to prevent and mitigate abuse involving the DNS as a key resource**
- The GAC, the GAC Public Safety Working Group and **many ICANN stakeholder groups prioritize curbing DNS Abuse**, recognizing in particular that **current ICANN contracts do not provide sufficiently clear and enforceable obligations** to mitigate DNS Abuse and need to be improved. This has been evidenced in:
  - Community discussions
  - Board correspondence (in particular [with the Business Constituency in 2020/2019](#), see 12 Feb. 2020)
  - GAC Inputs in Reviews (CCT, RDS-WHOIS2, SSR2) and in GNSO PDPs (New gTLD Subsequent Procedures)
  - Ongoing Contract Negotiations between ICANN org and Contracted Parties

# Presentation by I&JPN

---

Presentation by Internet & Jurisdiction Policy Network (30 min)

# Presentation on Cybercrime Trends from 2022

Without the understanding of multiple perspectives, you can never fully understand the impact or level of threat from Cybercrime.

## DNS centric Reporting:

- DNS Abuse Institute ([Compass](#))
- ICANN Domain Abuse Activity Reporting ([DAAR](#))
- European Commission [Study on Domain Name System \(DNS\) abuse](#)
- Interisle Phishing and Malware Reports

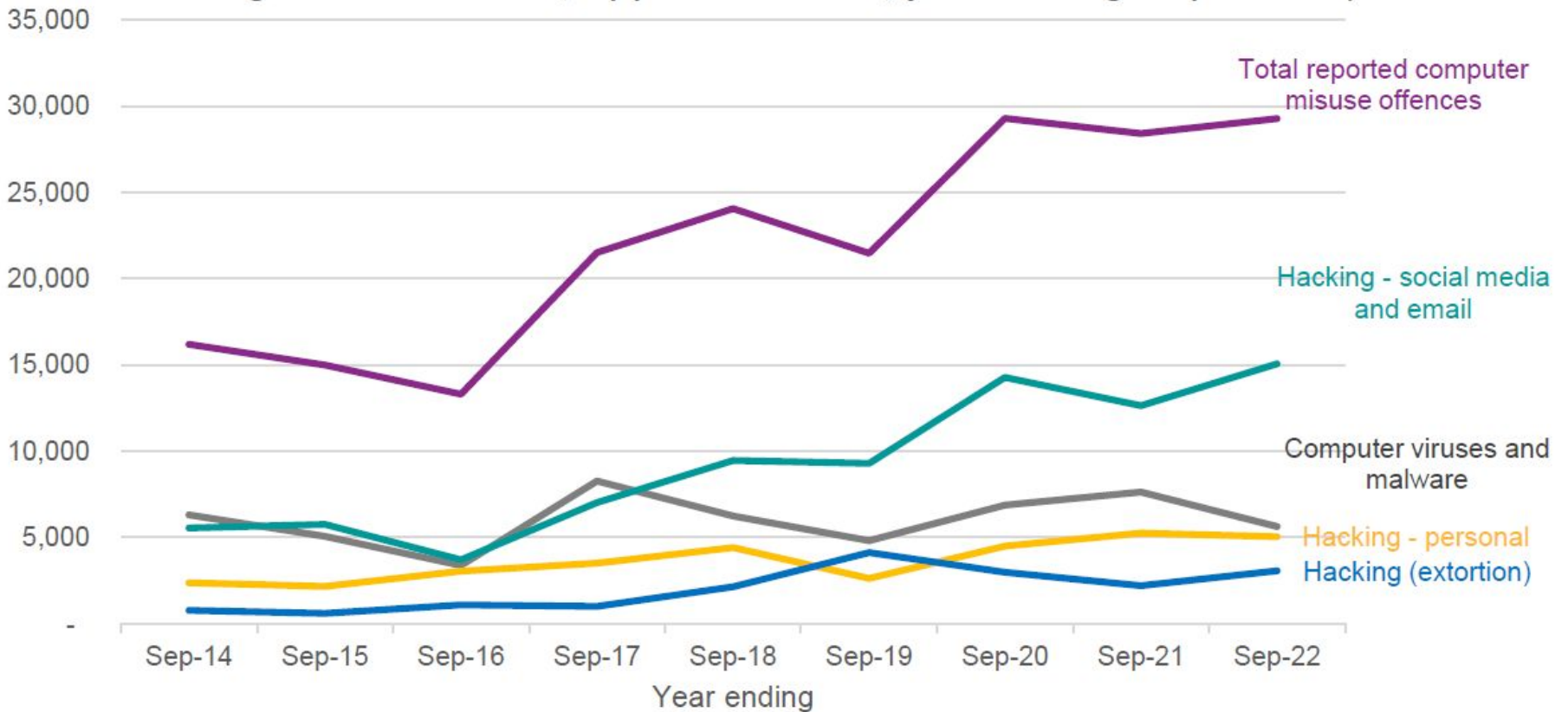
## Perspectives from PSWG Members:

- FBI Internet Crime Report 2022
- UK Cybercrime Research and Analysis 2022



# UK - Reporting Volume

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



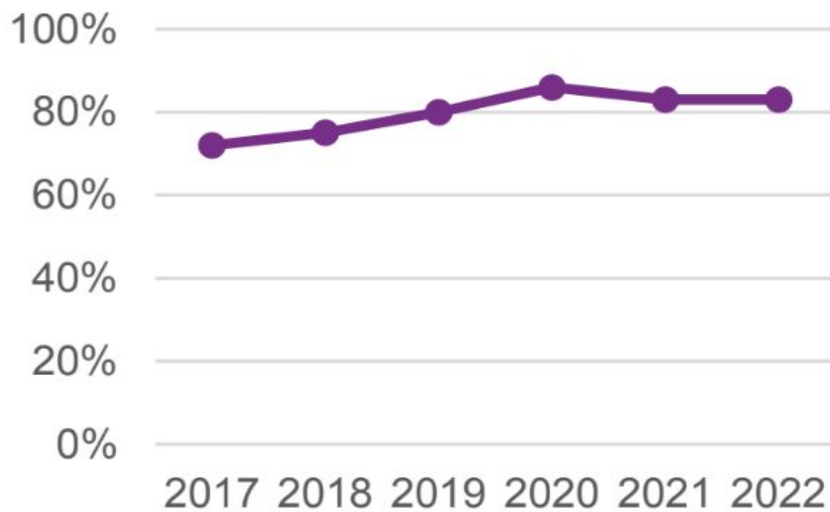
# UK - Breaches or attacks over time

Percentage of organisations surveyed over time identifying any breaches or attacks

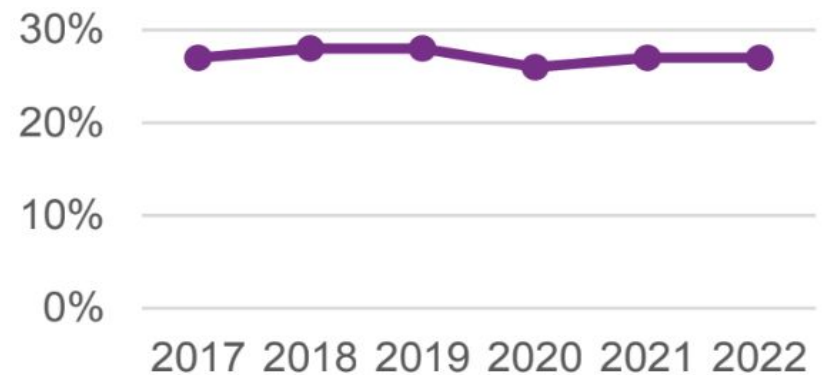


# UK - Business and Charities breaches

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



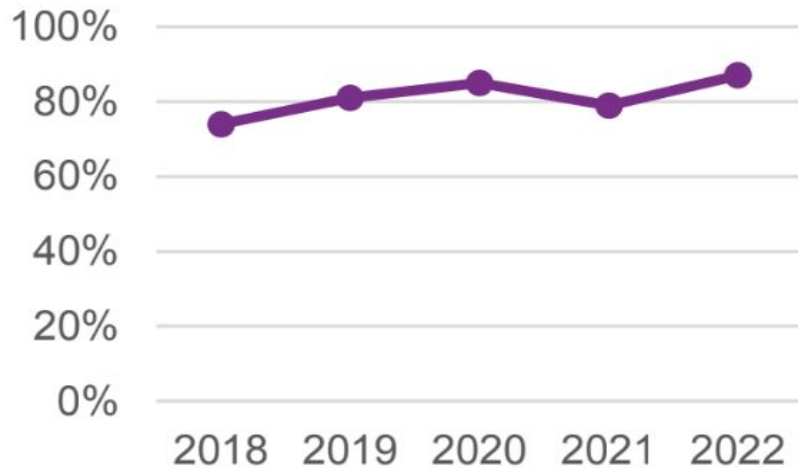
Businesses - % among those who identified a breach who identified an attack vector of others impersonating organisation in emails or online



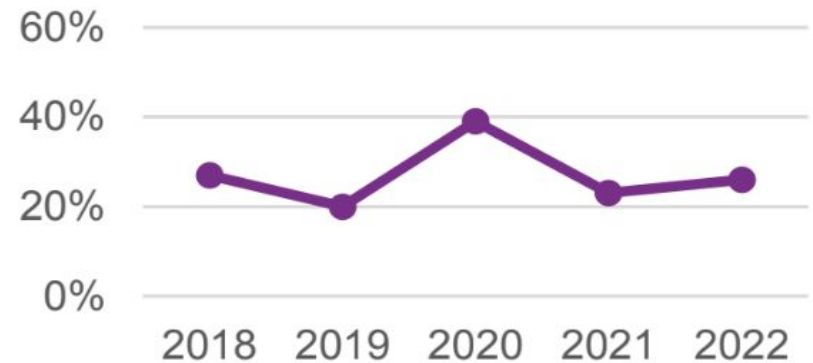


# UK - Business and Charities breaches

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



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



# UK - Suspicious email reporting service (SERS)

---

The public are encouraged to forward suspect emails to the UK's [Suspicious Email Reporting Service](#) (SERS) at [report@phishing.gov.uk](mailto:report@phishing.gov.uk), while suspicious texts should be forwarded to 7726.

SERS received 6.4 million reports during 2022. This brings the total number of reports since its launch in 2020 to 15.8m.

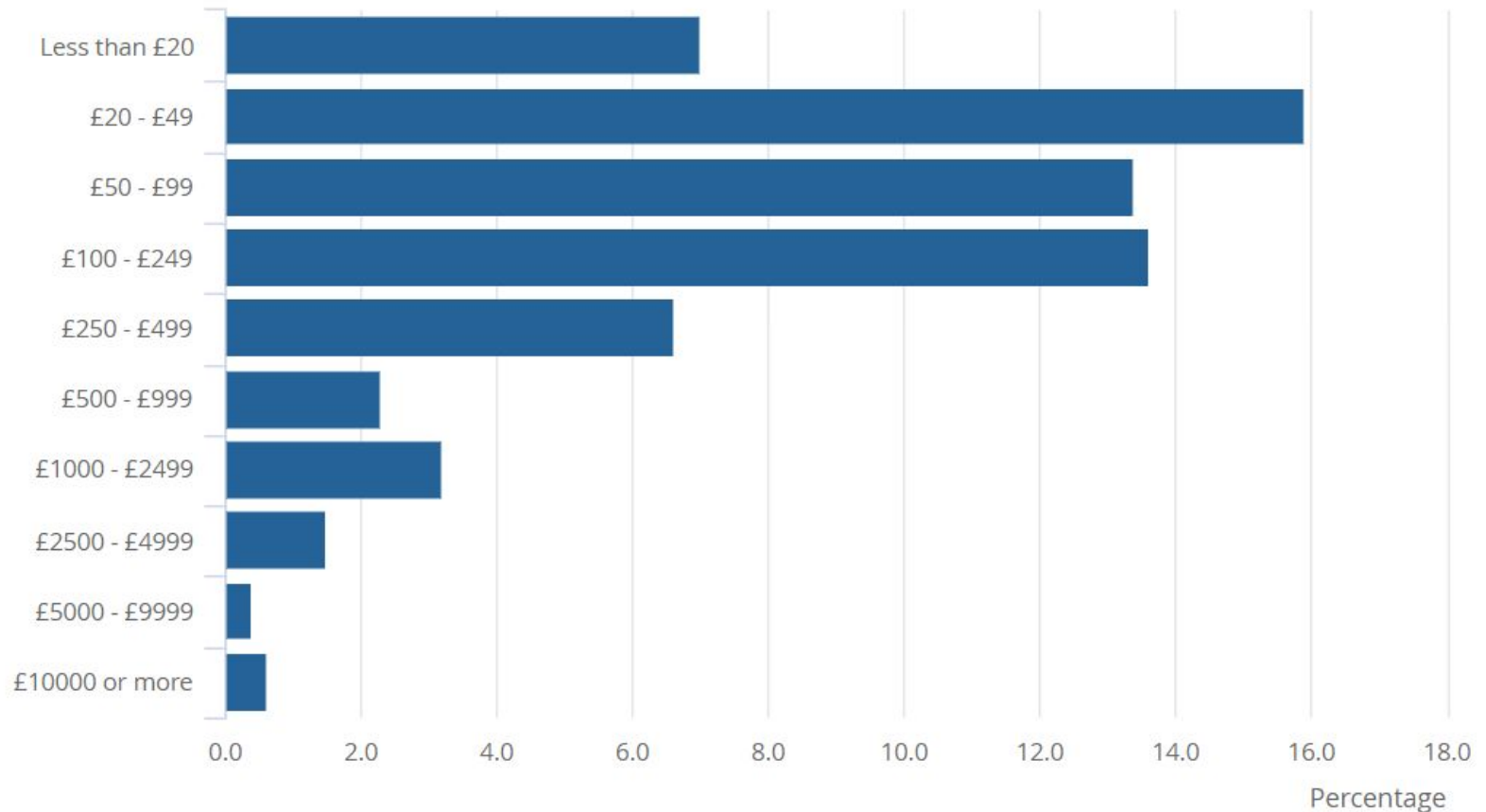
The top Government branded attacks that have been reported to SERS that have resulted in takedowns are:

1. National Health Service (NHS)
2. TV Licensing
3. HM Revenue & Customs
4. Gov.uk
5. Driver and Vehicle Licensing Agency

# UK - Impact on individuals

**Figure 4: Losses incurred by victims of fraud, TCSEW year ending March 2022**

## England and Wales



# UK - Impact on individuals

---

- 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.

# UK - Impact on individuals

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)

# UK - Impact on individuals

The image displays several screenshots from a website, likely related to online scams. The main screenshot shows a dashboard with a grid of scam offers, including Facebook Home, Facebook Mobile, Messenger, Free Fire, and Netflix. A sidebar on the left lists navigation options like 'OUR WEB SITE', 'SOCIAL MEDIA', and 'Telegram'. A 'Log In Snapchat' form is overlaid on the bottom left. A 'VICTIMS' table is shown in the bottom right, listing scam details and victim information.

**Log In Snapchat**

Username:

Password:

**LOG IN**

**OUR WEB SITE**

- Lartana

**SOCIAL MEDIA**

- Tutorials
- Telegram

**Facebook**

Facebook Home

EN AR FR IL

**Facebook**

FB Color Change (Piev)

EN AR FR IL

**Facebook**

Facebook Mobile

EN AR FR IL

**Messenger**

Messenger

EN AR FR IL

**Facebook**

Profile Visitors

EN AR FR IL

**Facebook**

Live Chat

EN AR FR IL

**FREE FIRE**

FREE FIRE - GARDIA

EN AR FR IL

**BATLEGROUND**

BATLEGROUND KNOWS

PUBG - MOBILE

EN AR FR IL

**NETFLIX**

Netflix

EN AR FR IL

**FREE FIRE**

Clash Of Clans

EN AR FR IL

**FREE FIRE**

FREE FIRE Slava

EN AR FR IL

**FREE FIRE**

FREE FIRE Spin

EN AR FR IL

**DASHBOARDS**

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

**OUR WEB SITE**

- Lartana

**SOCIAL MEDIA**

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

**VICTIMS**

Victims stop only 1 month! Always download your victims!

Show 10 entries

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

Showing 1 to 1 of 1 entries

Previous Next

Now 100% FREE! | Update 10.9 | Copy 100% FREE

# 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

# FBI Internet Crime Report for 2022



## FEDERAL BUREAU of INVESTIGATION Internet Crime Report 2022



INTERNET CRIME COMPLAINT CENTER

The Internet Crime Complaint Center (ic3.gov) is the primary intake portal for reporting Internet crimes to the FBI.

### IC3 BY THE NUMBERS<sup>16</sup>



**\$10.3 Billion**

Victim losses in 2022



**2,175+**

Average complaints received daily

2021  
2019  
2018  
2017  
2016

**651,800+**

Average complaints received per year (last 5 years)

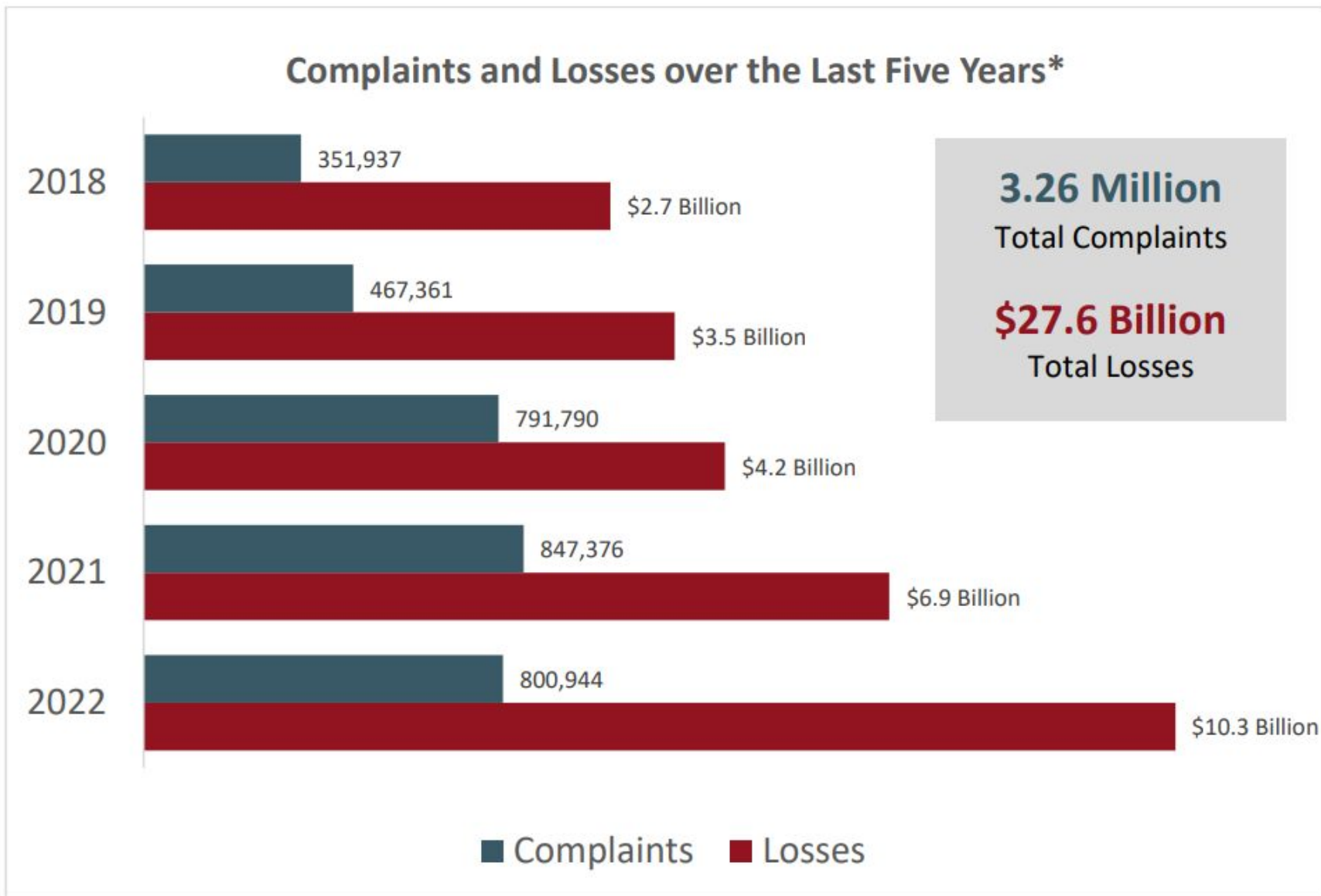


**Over 7.3 Million**

Complaints reported since inception



# Measured not by # of domains, but # of victims, \$

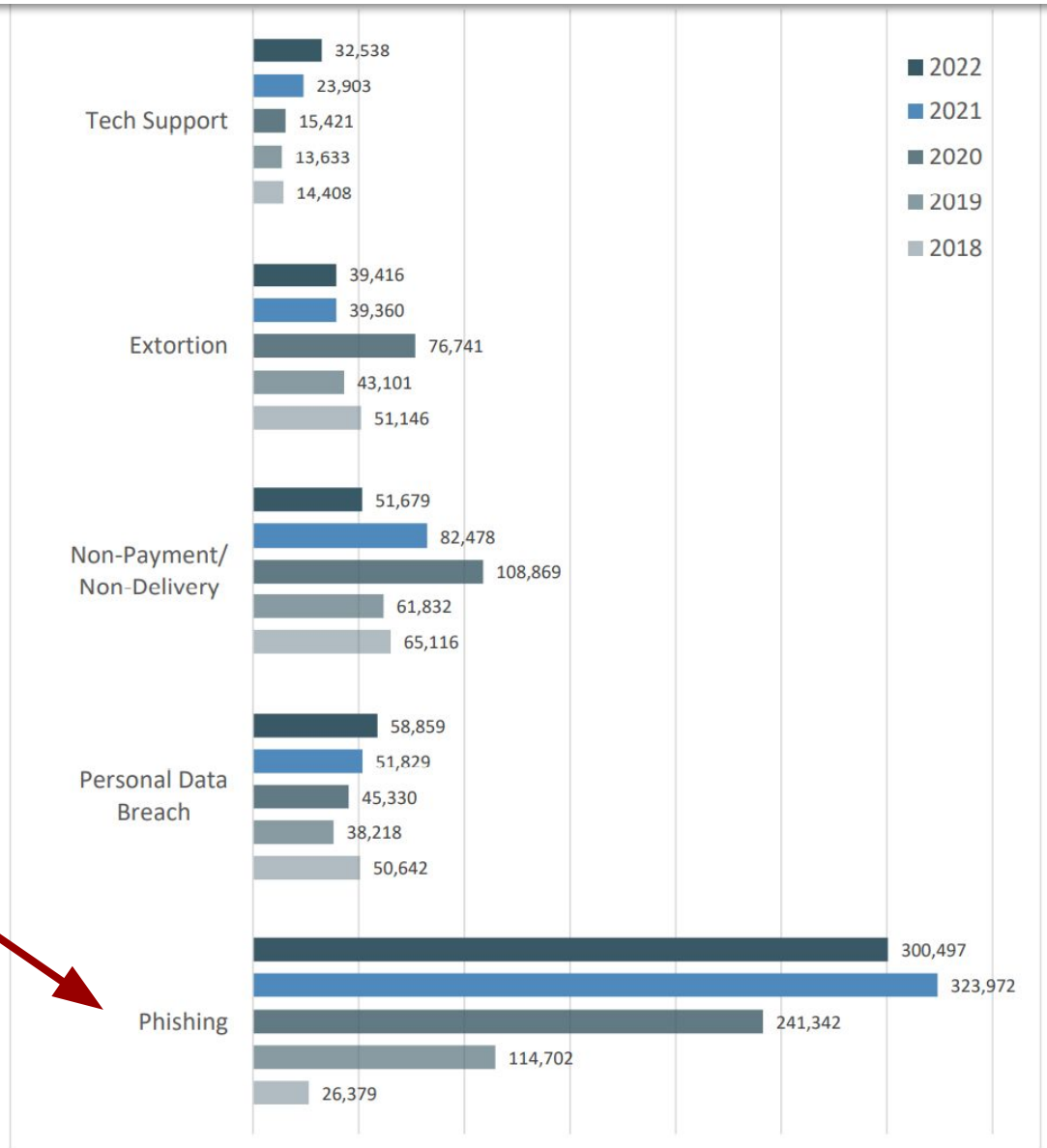


# Top 5 Crime Types Compared, over past 5 Years

“DNS Abuse”  
is not tracked as a  
category.

BUT...

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



# Count of Complaints - by category of scheme

## 2022 CRIME TYPES

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		
<i>Descriptors*</i>			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

# And the very newest trends...

thunderbird - Google Search

https://www.google.com/search?q=thunderbird&gl=us&hl=en&location=United+States&uule=w+CAIQICINW5pd...


Google thunderbird

About 104,000,000 results (0.51 seconds)

**Ad** · <https://www.tthunderbir.space/>

**Thunderbird - Easier Easy to Set Up**

Thunderbird is a email application that's easy to set up and customize - great features! Many more features you can change the look and feel in an instant.

 IcedID

<https://www.thunderbird.net>

**Thunderbird — Make Email Easier. — Thunderbird**

Thunderbird is a free email application that's easy to set up and customize - and it's loaded with great features!

**Download Thunderbird**

Download Thunderbird. Your download should begin ...

**Features**

Thunderbird is a free email application that's easy to set up ...

**Add-ons**

Most Popular Extensions - Themes - Featured Extensions - ...

**Make Email Easier.**

Thunderbird is a free email application that's easy to set up ...

More results from [thunderbird.net](https://www.thunderbird.net) »

**Public Service Announcement**

FEDERAL BUREAU OF INVESTIGATION

**December 21, 2022**

**Alert Number**  
**I-122122-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:  
[www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices)

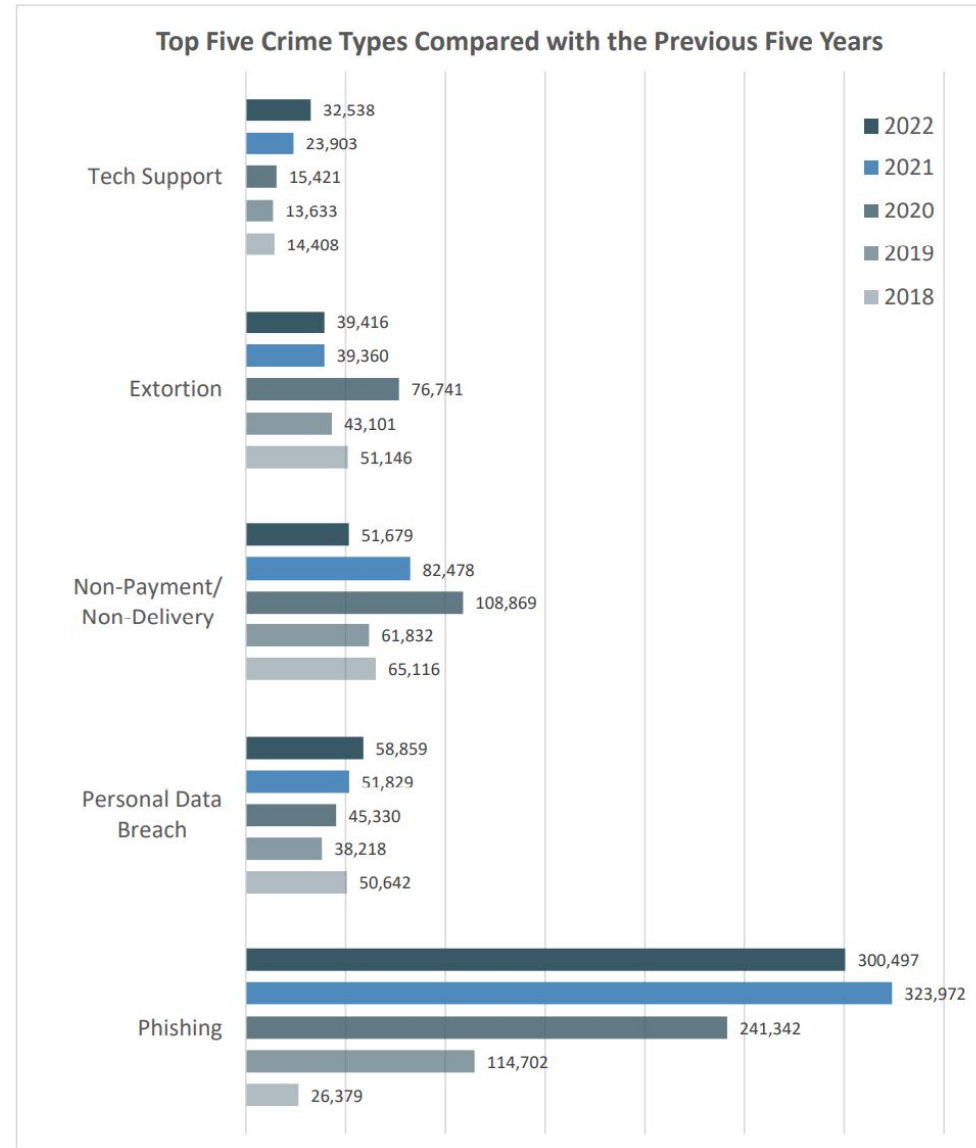
**Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users**

The FBI is warning the public that cyber criminals are using search engine advertisement services to impersonate brands and direct users to malicious sites that host ransomware and steal login credentials and other financial information.

^ img from abuse.ch twitter @abuse\_ch

# Key Takeaway

- **Phishing** is DNS Abuse
- **Phishing** is top reported Internet crime
- **Phishing** *enables* many other crimes
- Swift action against Maliciously Registered Domains is key



# Community Activities on DNS Abuse Mitigation

---

## Contracted Parties (ICANN76 Outreach on DNS Abuse)

- Registries are working on **voluntary sharing of statistics** relating to “evidenced and escalated” instances of DNS Abuse, as part of their obligation to monitor Security Threats (RA Specification 11 3b)  
*Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. [...]*
- The Registrar Stakeholder Group developed [acidtool.com](https://acidtool.com) (Abuse Contact IDentifier) to provide contact information of relevant parties to whom to direct **DNS Abuse reports**, including: hosting and email service providers, registrar and registrant.
- During ICANN76 the DNS Abuse Institute discussed with the PSWG the continued use of [netbeacon.org](https://netbeacon.org), a free **centralized reporting tool** (for phishing, malware, botnets and spam) which standardizes and enriches reports and distributes them automatically to registrars (currently only for gTLDs). This was presented to the GAC during ICANN74 and is consistent with the recommendation in SSAC 115.
- The DNS Abuse Institute shared its **continued measurement, and analysis of DNS Abuse data**, measuring phishing and malware, including levels of mitigation, time to mitigation, and distribution between compromised and malicious domains.

# Community Activities on DNS Abuse Mitigation

---

## GNSO Small Team on DNS Abuse

- On 31 January 2022 the GNSO Council [formed](#) a GNSO Small Team on DNS Abuse expected to determine “***what policy efforts, if any, the GNSO Council should consider undertaking to support the efforts already underway in the different parts of the community to tackle DNS abuse***”.
- In the [The Hague Communiqué](#) (20 June 2022), the GAC stated that “***any PDP on DNS Abuse should be narrowly tailored to produce a timely and workable outcome***” to which the ICANN Board responded that it shares this view and is prepared to support the ICANN community in such pursuits.
- The GNSO Small Team recommended in a [Report to the GNSO Council](#) (7 October 2022): **the initiation of a tightly scoped policy development on malicious registrations** (Rec. 1), further **exploration of the role of bulk registrations** play in DNS Abuse and measures already in place to address it (Rec. 2), **encouraging further work towards easier, better and actionable reporting of DNS Abuse** (Rec. 3), and possible work between Contracted Parties and ICANN Compliance regarding its findings on **potential gaps in interpretation and/or enforcement of the current ICANN contracts** (Rec. 4)

# Community Activities on DNS Abuse Mitigation

---

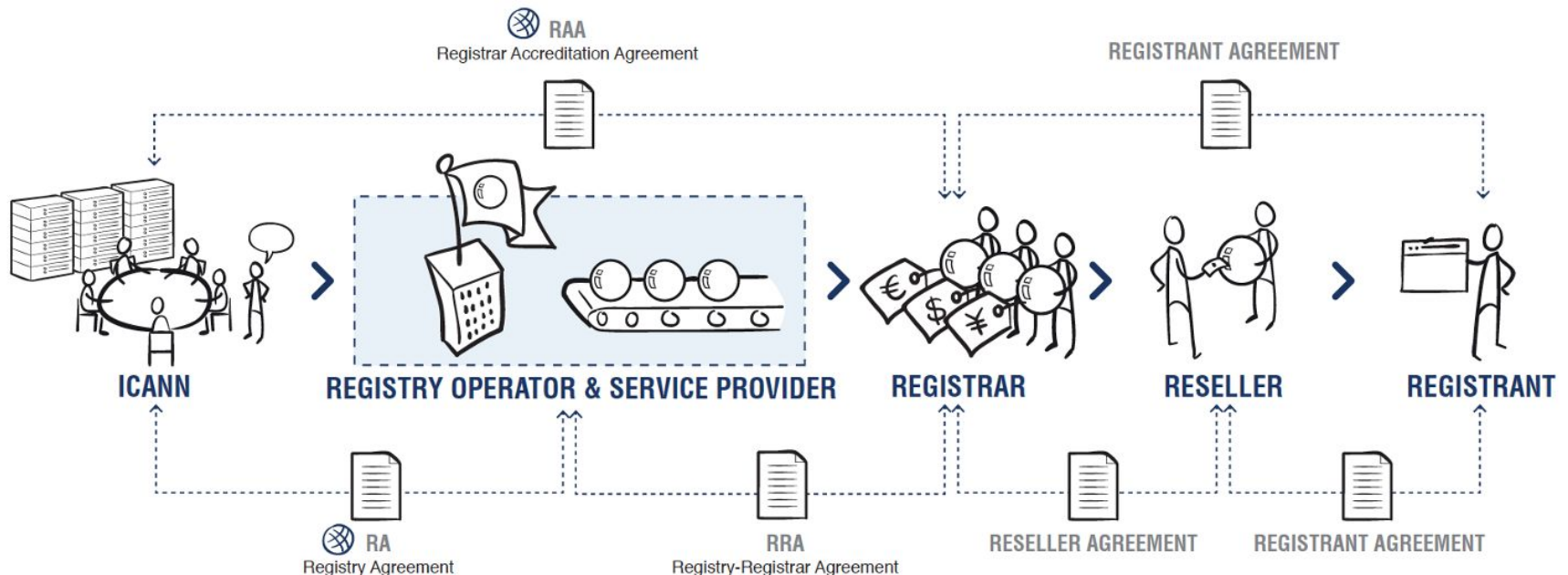
## ICANN Domain Abuse Activity Reporting (DAAR)

- The ICANN DAAR tool continues to analyse data related to 1145 gTLD's (and 21 [participating ccTLDs](#)) to produce reports on trends of reported abuse on domains from a number of sources.
- They continue to produce [monthly reports](#) available to the community and track trends.
- The GAC [welcomed](#) (21 Feb. 2022) the agreement between ICANN and the Registry Stakeholder Group (RySG) to expand data collection to enable registrar-level reporting in DAAR for gTLDs.
- In its [response](#) (29 March 2022), ICANN org stated that expanding DAAR's access to registrar-level data is a priority for ICANN org. A [proposed amendment](#) of the Registry Agreement to this effect (Sep. 2022) is undergoing a 60-day voting period for registries approval



# ICANN's Contracting Model (Reminder)

- ICANN and Registrars contract via the Registrar Registration Agreement (RAA)
- ICANN and Registry Operators contract via the Registry Agreement (RA)
- ICANN is not a party to agreements between:
  - Registries and Registrars (Registry-Registrar Agreements)
  - Registrars and Resellers
  - Registrars/Resellers and Registrants



# Community Activities on DNS Abuse Mitigation

**Ongoing Issues: Resellers** (intermediaries between registrants and ICANN-accredited registrars)

- Phase 1 Proposed Implementation– [GAC Comment on the Draft Registration Data Consensus Policy for gTLDs](#) (21 November 2022)
  - Re: “6.4 Registrar *MAY* generate the Reseller data element value. “ . . .  
**GAC suggests the following text:**  
  
***6.4 Registrar SHOULD generate the Reseller data element value, for the Reseller with a direct relationship with the Registrant.***
  - GAC supports the inclusion of corporate entities inherent to the registrar’s distribution channel as this would prove as **a benefit in highlighting the best point of contact to deal with notifications of abuse or compromise** to the party with the ability to act the quickest or most appropriately.
- This is consistent with Recommendation 17 of the [CCT Review Team](#) (8 Sep. 2018):  
*ICANN should collect data about and publicize the chain of parties responsible for gTLD domain name registrations.*
  - ICANN Board “accepted” this recommendation and noted this was already being done but. . . this was an optional ,not mandatory collection and publication

# Potential Issues for Communiqué (1/2)

---

- **Contract Negotiations** - Contracted parties have signaled that their current negotiations:
  - Seek to raise the floor on contract obligations with regard to taking action against DNS Abuse
  - First of many steps (may include targeted PDPS, more negotiations)
  - Upcoming opportunity for public comments
  - GAC role in next steps

# Potential Issues for Communiqué (2/2)

---

- **Resellers** - Prior GAC Input regarding Identifying Resellers
  - [GAC Comments on CCT Review Final Report](#) (Dec. 2018)
  - [GAC Comments on Plan for Implementation](#) (Oct. 2019)
  - [GAC Comment on the Draft Registration Data Consensus Policy for gTLDs](#) (Nov. 2022)

# Considerations for Cancun Communiqué

---

- Statement of Support for the Contract Negotiations
- Follow-up on prior GAC input on issues of resellers
- Are there any other topics GAC Members would like to see reflected in the Communiqué ?