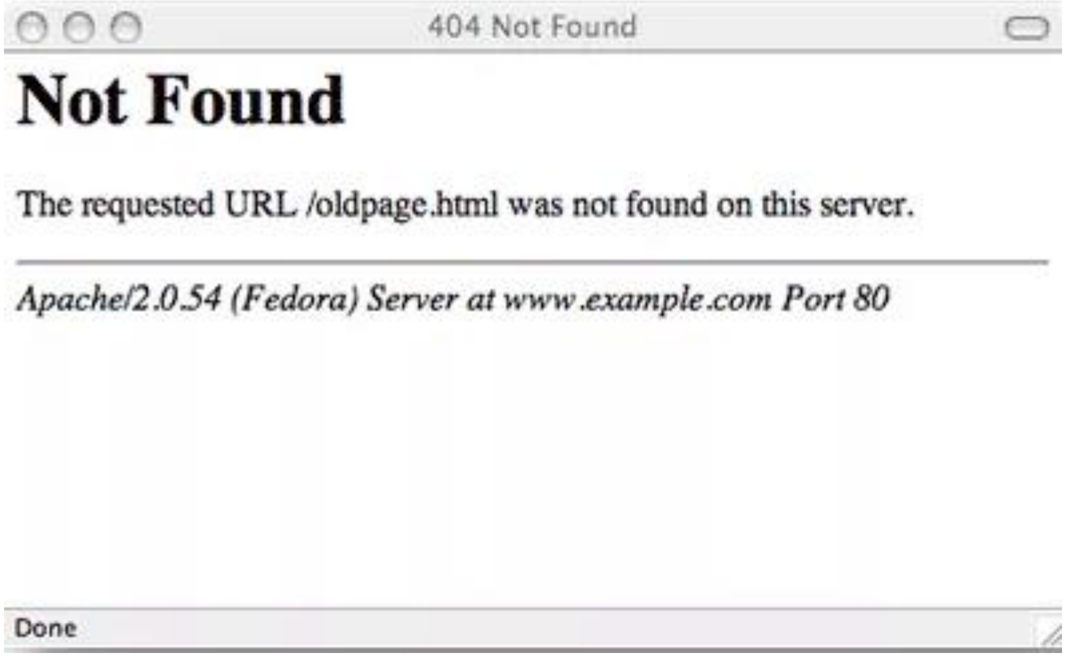
Cybersecurity and user awareness

Jean-Jacques Sahel

Conference Circle of Digital Life
Prague, 20 September 2018

ICANN’s role

Without ICANN



Not Found

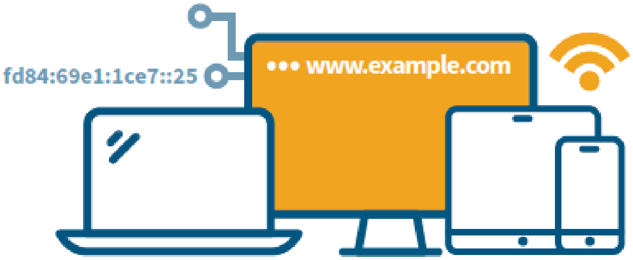
The requested URL /oldpage.html was not found on this server.

Apache/2.0.54 (Fedora) Server at www.example.com Port 80

Coordinating with our technical partners, we help make the Internet work.

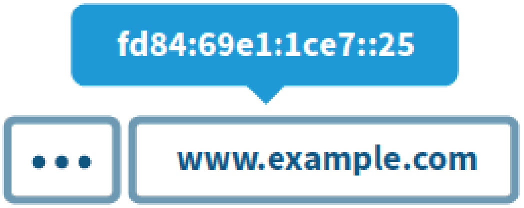
ICANN’s focus: Unique Names and Numbers

Anything connected to the Internet – including computers, mobile phones and other devices – **has a unique number called its IP address**. IP stands for Internet Protocol.



This address is like a postal address. It allows messages, videos and other packets of data to be sent from anywhere on the Internet to the device that has been uniquely identified by its IP address.

IP addresses can be difficult to remember, so instead of numbers, **the Internet’s domain name system (DNS) uses letters, numbers and hyphens, to form a name that is easier to remember**.

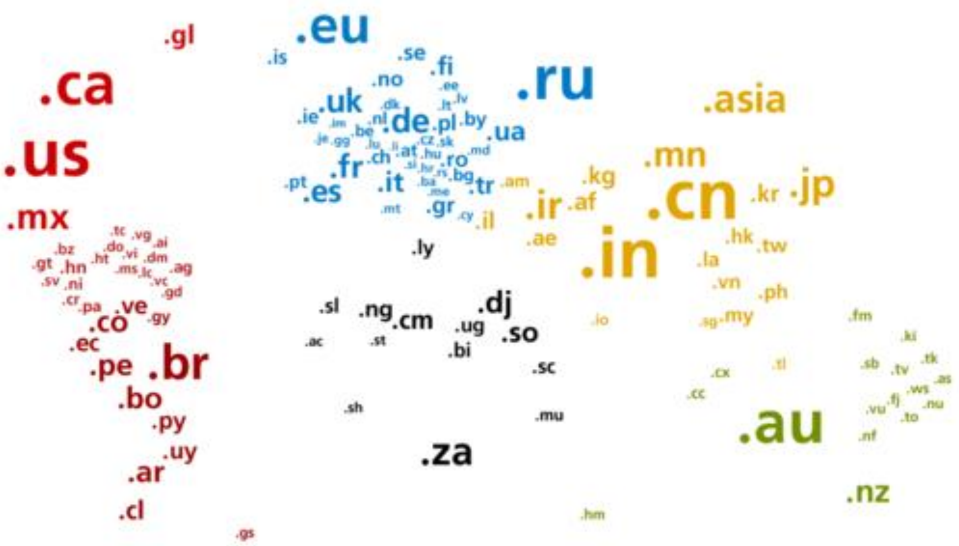


ICANN's Mission

The mission of the Internet Corporation for Assigned Names and Numbers (ICANN) is to **ensure the stable and secure operation of the Internet's unique identifier systems**

ICANN is (primarily) involved in the top-most levels of the domain name system:

- Create/change new TLDs
  - **.EXAMPLE**
- Enforce contractual obligations on (non-country code) registries and registrars that operate and sell 2nd level names
  - **CTU**.EXAMPLE



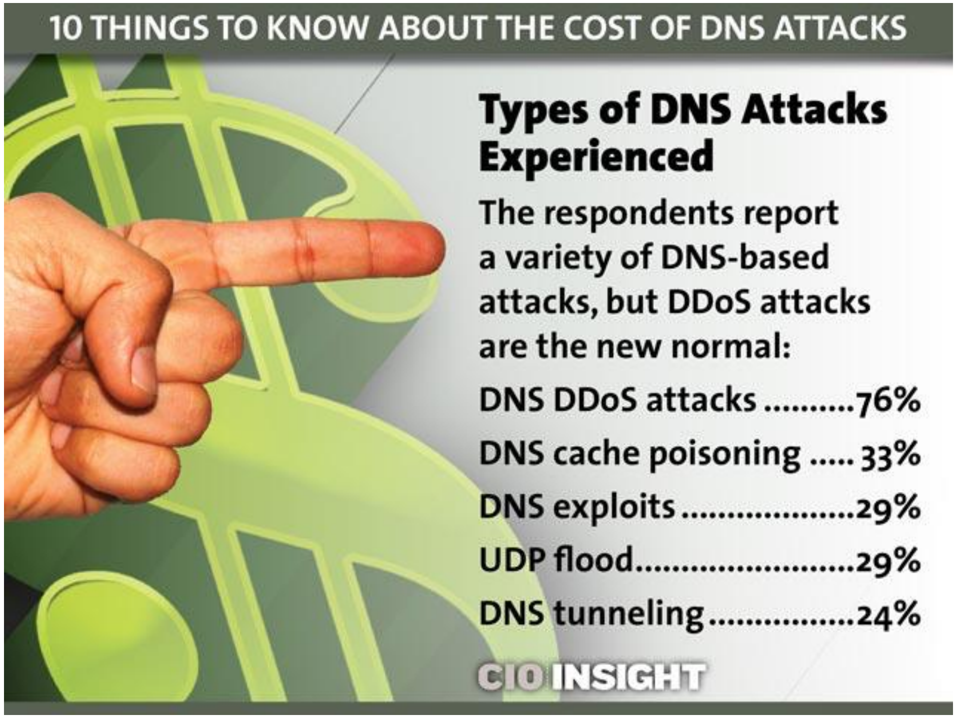
Cybersecurity threats at the DNS level

DNS Abuse

- Using the Internet’s naming system for malicious purposes.

Examples:

- Denial of service via DNS protocol
- Botnet command/control synchronization
- Spam-vectored threats:
  - Phishing for distribution of malware or fraud
- Infrastructure-vectored threats:
  - Cache poisoning
  - Resolver Redirection
  - DNS tunneling



10 THINGS TO KNOW ABOUT THE COST OF DNS ATTACKS

Types of DNS Attacks Experienced

The respondents report a variety of DNS-based attacks, but DDoS attacks are the new normal:

DNS DDoS attacks	76%
DNS cache poisoning	33%
DNS exploits	29%
UDP flood	29%
DNS tunneling	24%

CIO INSIGHT

http://www.cioinsight.com/security/slideshows/10-things-to-know-about-the-cost-of-dns-attacks.html

Why? A (Very) Recent Example...

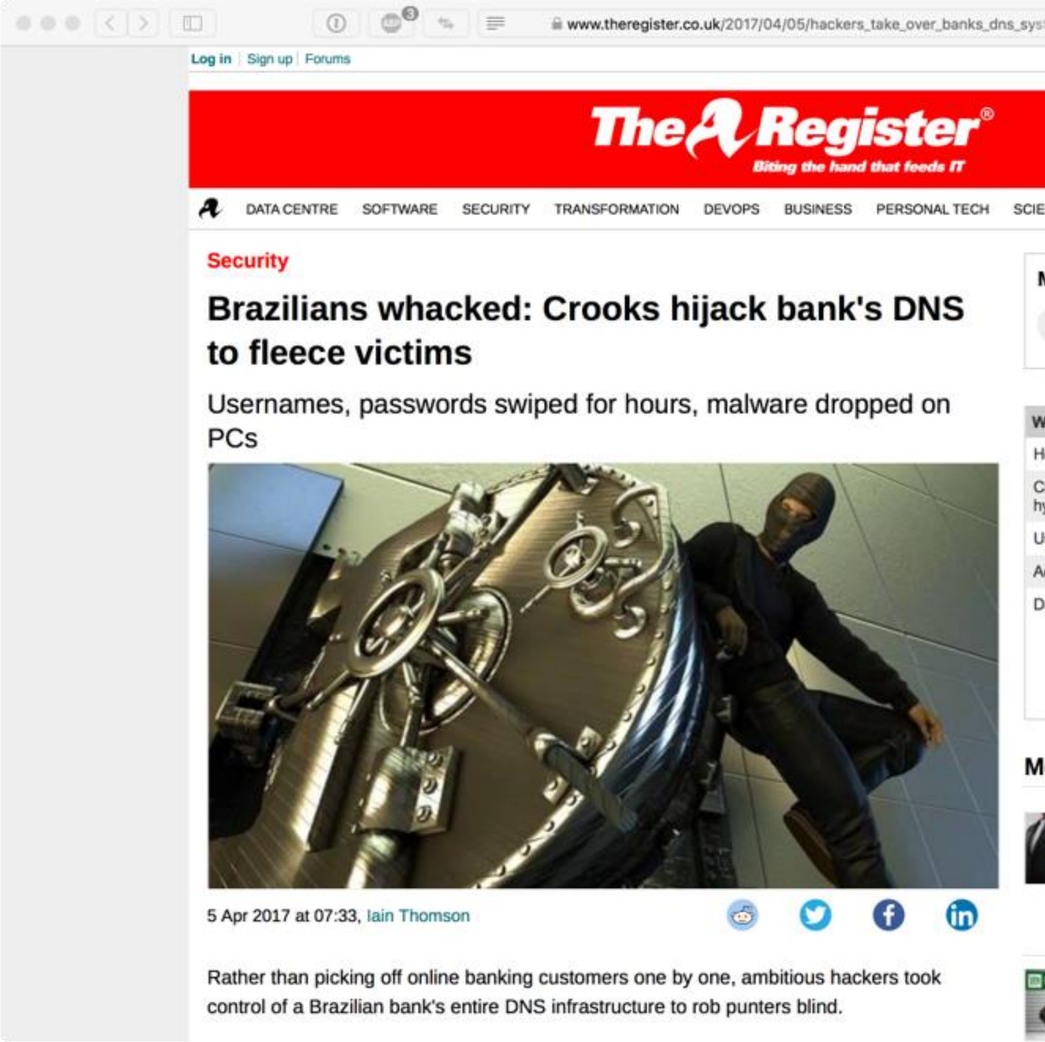
- “[A] major Brazilian financial company with hundreds of branches, operations in the US and the Cayman Islands, 5 million customers, and more than $27 billion in assets.”

  https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/

- “[A]ccording to security researchers at Kaspersky, **the bank is just one of ten** around the world that has been almost **totally compromised** in a comprehensive cyber attack.”

- **“If DNS was under control of the criminals, you're screwed**.”

  http://www.computing.co.uk/ctg/news/3007938/brazilian-bank-customers-targeted-after-hackers-transfer-all-of-the-banks-domains-to-phony-websites



www.theregister.co.uk/2017/04/05/hackers_take_over_banks_dns_sys
Log in | Sign up | Forums
The Register®
Biting the hand that feeds IT
DATA CENTRE
SOFTWARE
SECURITY
TRANSFORMATION
DEVOPS
BUSINESS
PERSONAL TECH
SCIE

Security

Brazilians whacked: Crooks hijack bank's DNS to fleece victims

Usernames, passwords swiped for hours, malware dropped on PCs

5 Apr 2017 at 07:33, Iain Thomson

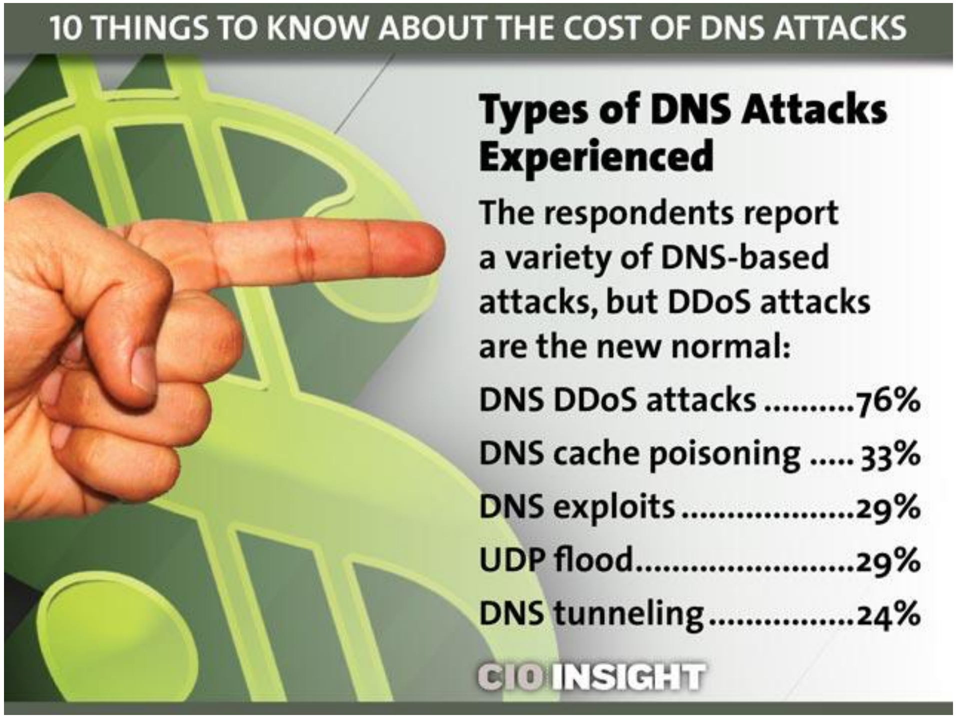
Rather than picking off online banking customers one by one, ambitious hackers took control of a Brazilian bank's entire DNS infrastructure to rob punters blind.

Cybersecurity: DNS Abuse

- Using the Internet's naming system for malicious purposes.

Examples:

- Denial of service via DNS protocol
- Botnet command/control synchronization
- Spam-vectored threats:
  - Phishing for distribution of malware or fraud
- Infrastructure-vectored threats:
  - Cache poisoning
  - Resolver Redirection
  - DNS tunneling



10 THINGS TO KNOW ABOUT THE COST OF DNS ATTACKS

Types of DNS Attacks Experienced

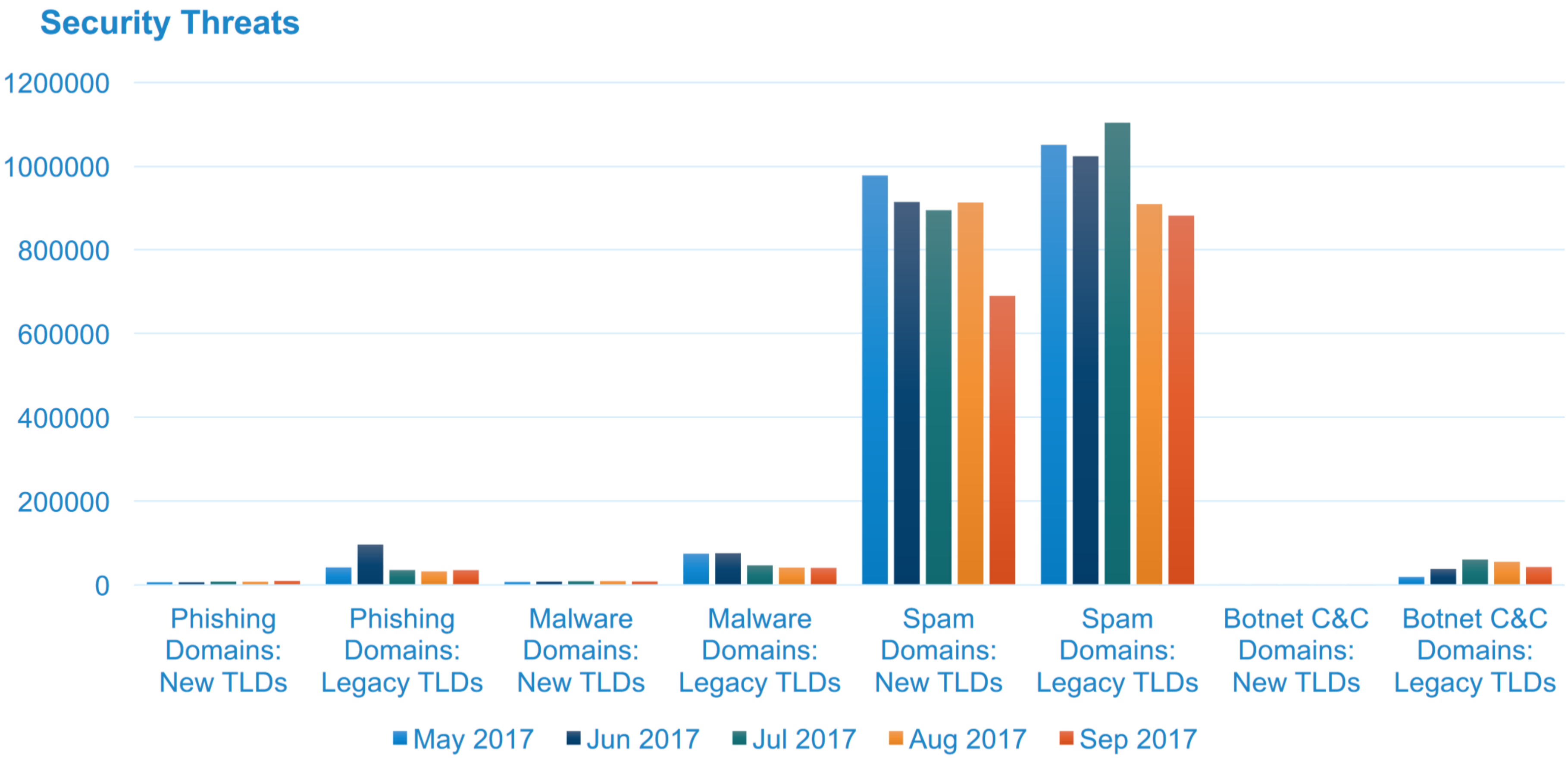
The respondents report a variety of DNS-based attacks, but DDoS attacks are the new normal:

DNS DDoS attacks	76%
DNS cache poisoning	33%
DNS exploits	29%
UDP flood	29%
DNS tunneling	24%

CIO INSIGHT

http://www.cioinsight.com/security/slideshows/10-things-to-know-about-the-cost-of-dns-attacks.html

Data Set: All gTLDs having at least 1 reported abuse domain



ICANN’s role and activities in Internet security and safety

6 April 2017

ICANN’s Role in Cybersecurity & Cybersafety

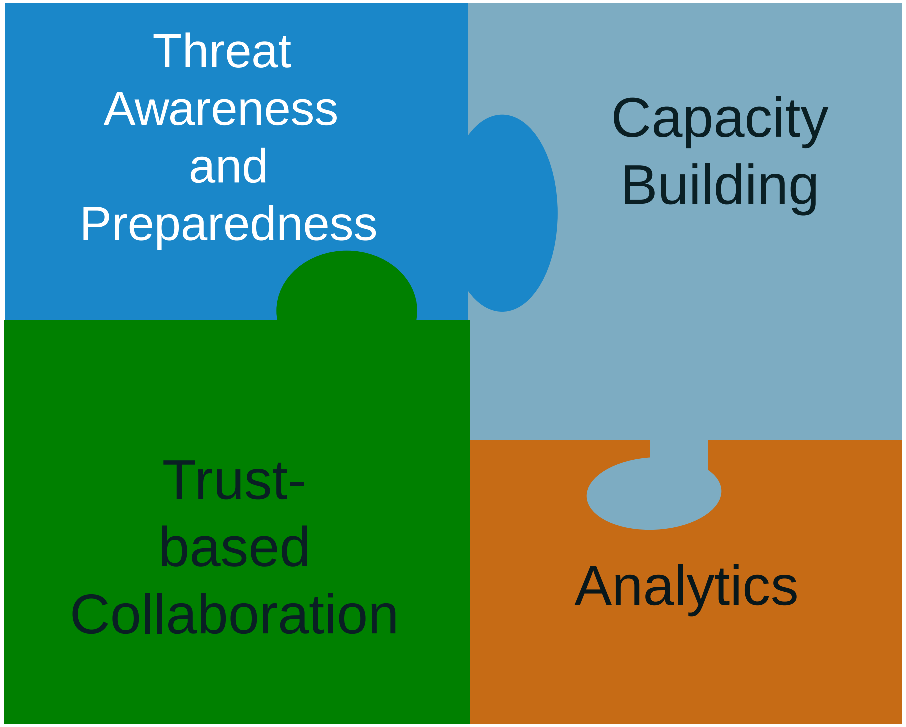
- **Preparedness:** Identifying and helping the community be prepared for identifier-based threats
  - DNS, IP addresses, and similar technologies
  - Encouraging use of DNSSEC

- Threat **awareness**:
  - Data reporting on DNS (Domain name) Abuse
  - Data sharing to assist operations or security activities
  - Collaboration with public safety community (investigations, training)
  - Security knowledge transfer

- **Capacity building**, training, information sharing

- **Collaboration:** Working with the operational security community via trust networks

- **Contractual obligations on generic top-level domain registries and registrars:**
  - Require contact details of registrants;
  - Force compliance with IETF standards;
  - “Public Interest Commitments”, e.g. against malware, maintaining safe & secure systems)



- **Analytics:** Providing neutral and unbiased data-backed analysis

What Can You Do at the DNS level?

Regulators/Governments

- Participate in ICANN
  - Government Advisory Committee
  - GAC's Public Safety Working Group
  - Engage in capacity building workshops
- Enquire about DNSSEC plans with your network operators
  - Ready for root key update?
- Support a national Computer Emergency Response Team (CERT)

Network Operators and businesses

- Participate in ICANN
  - Internet Service Providers and Connectivity Providers & Business Constituencies
  - Technical Experts Group
  - RSSAC Caucus
- Enable DNSSEC validation
  - Prepare for root key update
- Deploy DNSSEC
  - Sign all your zones
  - Encourage your customers to sign their zones
- Mirror the root zone
  - RFC 7706 is easiest

What you can (must?) do generally

- **Cooperation** to prevent and to stop abuse

  Ongoing exchange of information and enforcement cooperation (rapid when needed!)

- **Organisational preparedness**
  - In government as in ALL businesses / organisations
  - Government MUST work with business, esp. for critical infrastructure
  - Audit, data protection processes in place
  - Not just about hardware and software, but also people…

- **Awareness raising:** User education is the key
  - Human often the weak link (social engineering, response to phishing)
  - For employees
  - For individual users
  - A culture of cyber-security, from school onwards!

- **Smart legislation: collaborative policy and legislation**
  - Informed by reality including the technology; dialogue with all relevant stakeholders
  - Supporting swift and robust enforcement, including across (multiple) borders
  - Balance different legislative aspects (privacy vs. security; ensuring consistency between frameworks for a global Internet vs. local / regional legislative approaches)

- **Think ahead about emerging technologies**
  - Internet of Things ? Blockchain ? AI ?
  - ‘Secure by design’

THE INTERNET IS GOOD !

Thank you and questions

ICANN

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann