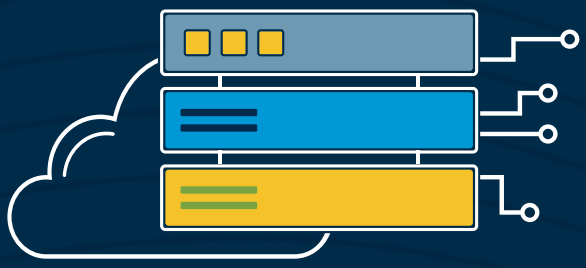
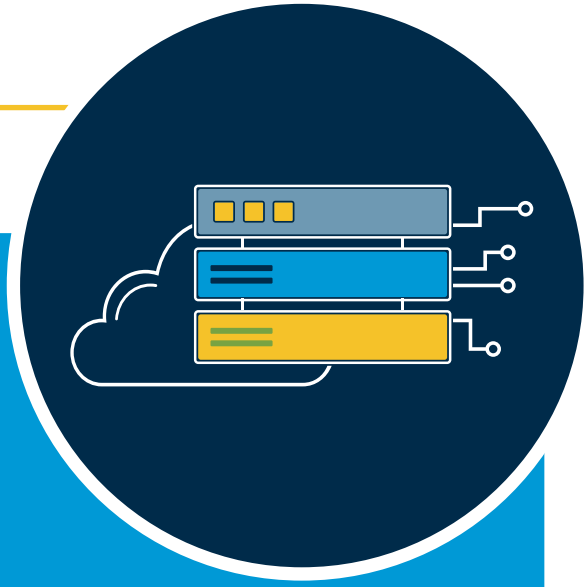


Domain Name Security Threat Information Collection and Reporting (DNSTICR)

January 2022

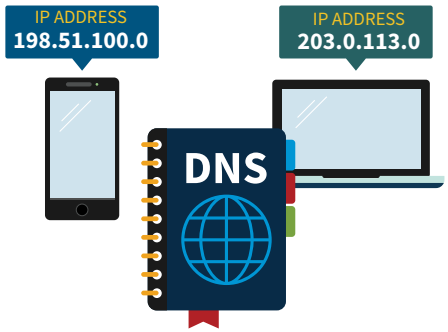
Internet Corporation for Assigned Names and Numbers

ICANN



What's in this Guide?

What is the Domain Name System?



The **Domain Name System (DNS)** helps users find their way around the Internet. Each device or website on the Internet has a unique address – like a telephone number. This address is a complicated series of numbers, or a series of numbers and letters called an **IP address.** IP stands for Internet Protocol.

IP addresses can be hard to remember. The DNS makes navigating the Internet easier.

IP addresses can be hard to remember. The DNS makes navigating the Internet easier by allowing users to type in familiar letters – the **domain name** – instead of the **IP address.** For example, you only need to type in **https://icann.org** to reach ICANN's website, instead of its **IP address – 192.0.43.7**

What are DNS Security Threats?

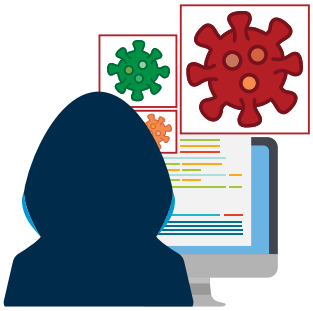
There are various forms of content-related **abuse** in the Internet space. Some of these abuses include websites that provide a platform for illegal activities like child exploitation and human trafficking. Others promote cyberbullying or are a digital haven for selling nonexistent or fake products.

However, ICANN's remit excludes regulation of Internet content.

The ICANN organization (org) focuses its efforts on specific **DNS Security Threats**, which have a narrower scope than content-related abuse. So, what are DNS Security Threats?

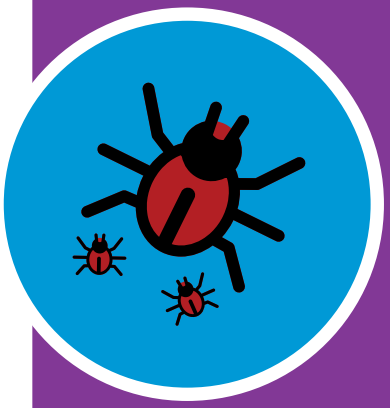
DNS Security Threats include any malicious activity aimed at disrupting the DNS infrastructure or causing the DNS to operate in an unintended manner.

Domain Name Security Threat Information Collection and Reporting (DNSTICR)



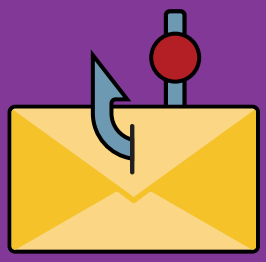
The **Domain Name Security Threat Information Collection and Reporting (DNSTICR)** project produces reports on recent domain registrations that ICANN org believes to be using the COVID-19 pandemic for phishing or malware campaigns.

These reports contain the evidence that leads ICANN org to believe the domains are being used maliciously. Along with other background information, the reports help the responsible registrars to determine the correct course of action.



The DNSTICR project is specifically designed to search for malware injection and phishing attempts.

Malware
Software installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.

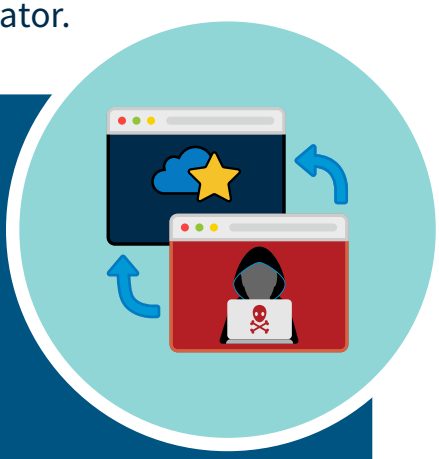


Phishing
Occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (account numbers, login IDs, passwords, etc.), by sending fraudulent or look-alike emails, or luring users to copycat websites.

The DNSTICR project is not intended to search for the following Internet-related malicious practices:

Botnets

Collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.



Pharming

The redirection of users to fraudulent sites or services, typically through DNS hijacking or poisoning.

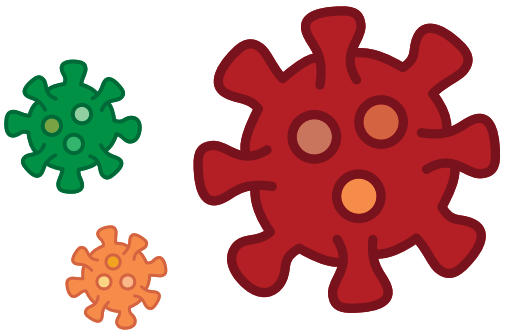
- DNS hijacking occurs when attackers use malware to redirect victims to the attacker's site instead of the one initially requested.
- DNS poisoning causes a DNS server or resolver to respond with a false IP address bearing malicious code. Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.

Spam (As it is used to propagate other DNS security threats)

Unsolicited bulk email, where the recipient has not granted permission for the message to be sent and where the message was sent as part of a larger collection of messages, all having substantively identical content. A generic unsolicited e-mail alone does not constitute a DNS security threat, but it would if that email is part of a phishing scheme.

Origins of the DNSTICR project.

During the **COVID-19 pandemic**, criminals phished the vulnerable, the inattentive, the elderly, children, and the less fortunate. These criminals target victims all over the world and in many languages, to steal money and personal information.



Criminals and scammers call, email, or text victims to trick them into revealing their personal information, or into buying fake vaccine IDs, bogus COVID-19 tests, or fake cures.

To combat COVID-19 Internet phishing and malware, ICANN org developed the **DNSTICR** project. It searches for and reports potentially malicious activities of domain names and their background information to registrars. It provides another layer of defense in ICANN org's fight to protect Internet users from DNS security threats.

As the pandemic continues, the terms and topics searched for through the DNSTICR project are updated. This update is a relatively simple technical process. For example, additional topics include **passport,** related to **immunity passports** used in some countries, and **ivermectin,** an anti-parasitic drug, which has become associated with the pandemic.

Other terms could include the titles of prominent government COVID-19-related sponsored programs intended to provide aid to people in need. More generic terms like respirators, N95 masks, and sanitizers are also incorporated.

However, ICANN org lacks the resources or mandate to verify whether all sites offering these supplies are legitimate.

Help us protect the Internet from COVID-19 malware and phishing attempts in your part of the world.

Are you a health care provider, financial manager, government regulator, policy maker, public safety official, or security professional?

We need you!

Here's how we can work together to protect Internet users from DNS security threats:

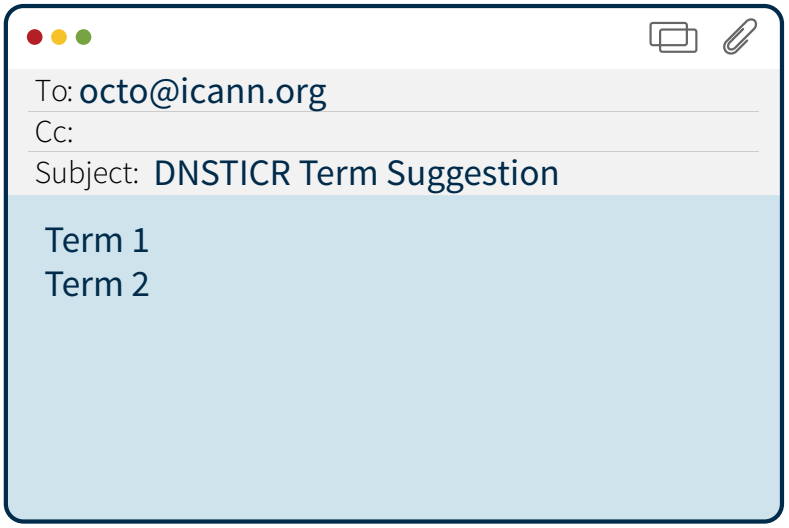
Step 1
Make a list of words in your native language and character sets related to the COVID-19 pandemic that are being used or could potentially be used in your region to target people or organizations.

Step 2
Email your list to **octo@icann.org** with the subject line: **DNSTICR Term Suggestion**

New suggestions should be submitted one per line in the body of the email.

For example:
Term 1
Term 2

If the terms require an explanation, add the explanation after your list of terms.



Learn about the Domain Name System Security Threat Information Collection and Reporting (DNSTICR) project and how you can contribute to making the Internet a safer place!

Learn More
Visit our dedicated DNSTICR webpage:
https://www.icann.org/dnsticr

Explore
Find out about ICANN org-wide efforts to mitigate DNS security threats:
https://www.icann.org/dnsabuse

Acronyms and Terms
Click on the links below to read more about the acronyms and terms used in this guide via ICANN's Acronyms and Terms feature: https://go.icann.org/acronyms

Domain Name
Domain Name Label
Domain Name System (DNS)
Internet Protocol (IP)
Internet Protocol Address
Internet Protocol version 4 (IPv4)
Internet Protocol version 6 (IPv6)

CONNECT WITH US

https://icann.org
flickr.com/icann
@icann
linkedin/company/icann
facebook.com/icannorg
soundcloud/icann
youtube.com/icannnews
instagram.com/icannorg

Or visit our dedicated social media page:
https://go.icann.org/socialmedia