

Beginner's Guide to DNS Security

DNS Security from the perspective of the vast majority¹

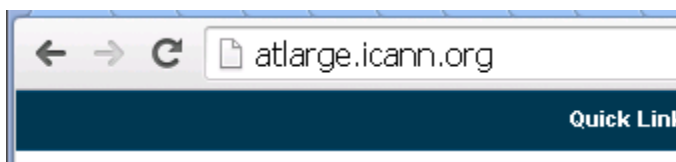
Being at the “end of the Internet pipe” us end users see it all experiencing the net sum of any inadequacies due to DNS security. But in some ways we have the greatest power to improve it – choice.

Background

For the vast majority of users a discussion regarding DNS security might begin with “what is DNS?” There have been volumes written on this topic including our own “Beginners Guide to Domain Names”².

A reasonable starting definition is that the Domain Name System (DNS) is like telephone directory assistance for the Internet. It's the way your device (phone, laptop, etc.) asks questions like “what is the address for www.google.com?”. It converts the names we use to reference web sites, email, and other services into numbers (called IP addresses, which is discussed next). Many experts find this analogy too simplistic for what might be considered a bit more general database, but we will fill in necessary details as we describe DNS security.

The numbers are Internet Protocol (IP) addresses and, like the telephone system, identify entry and exit points for the Internet and are used to route the actual data. The DNS lets us use names instead of numbers to simplify using the Internet. Typical IP addresses might look like 192.0.32.60 for IP version 4 (IPv4) or 2620:0:2d0:200::60 for the newer IP version 6 (IPv6) address. A simple example is that you type in a web site name like atlarge.icann.org into your browser, your computer asks the DNS for its IP address and gets 192.0.32.60, your computer uses that address to open a connection to the atlarge.icann.org webserver direct its query and your computer starts exchanging data with that IP address. The result of this is that you see the web page.



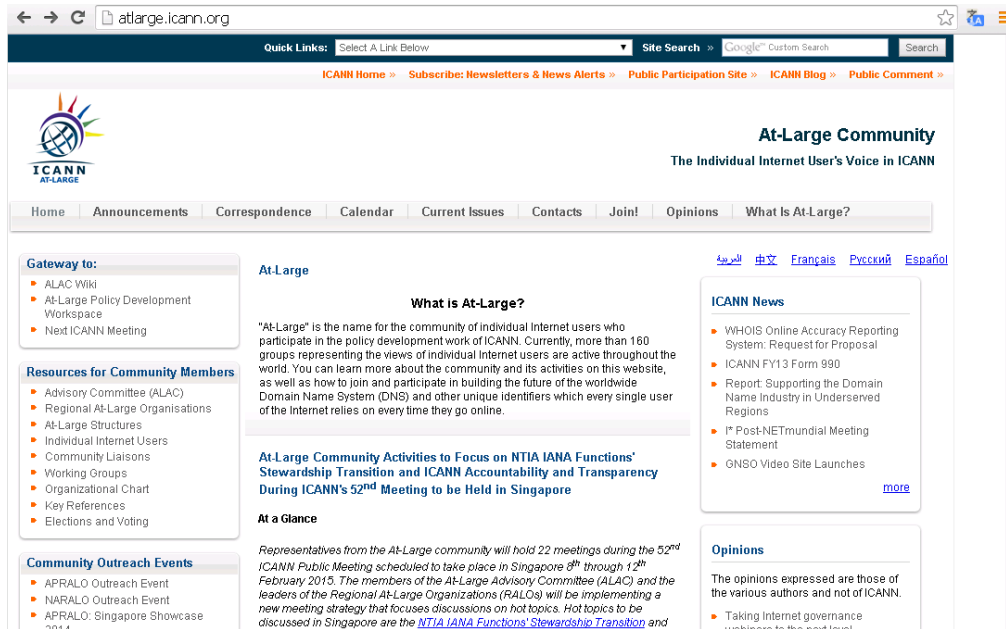
¹ Surf the web and have email and other accounts on the Internet

² Beginners Guide to Domain Names <https://www.icann.org/en/system/files/files/domain-names-beginners-guide-06dec10-en.pdf>

```
Command Prompt
c:\>nslookup atlarge.icann.org
Server: Unknown
Address: 10.101.186.13

Non-authoritative answer:
Name: atlarge.icann.org
Addresses: 2620:0:2d0:200::60
          192.0.32.60
```

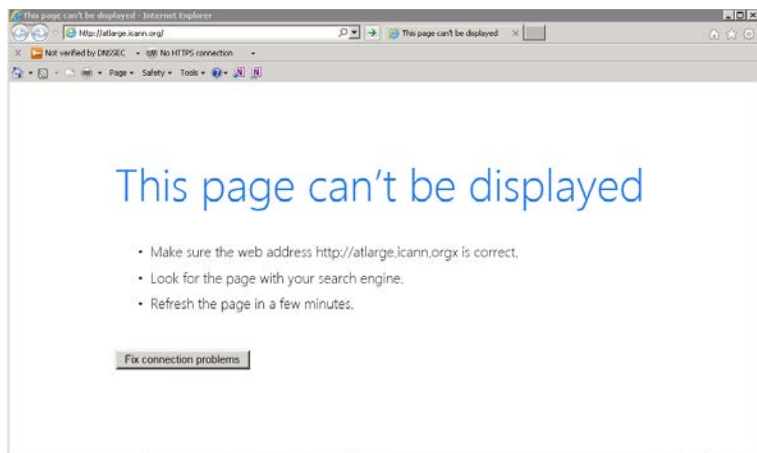
Example of a manual DNS lookup



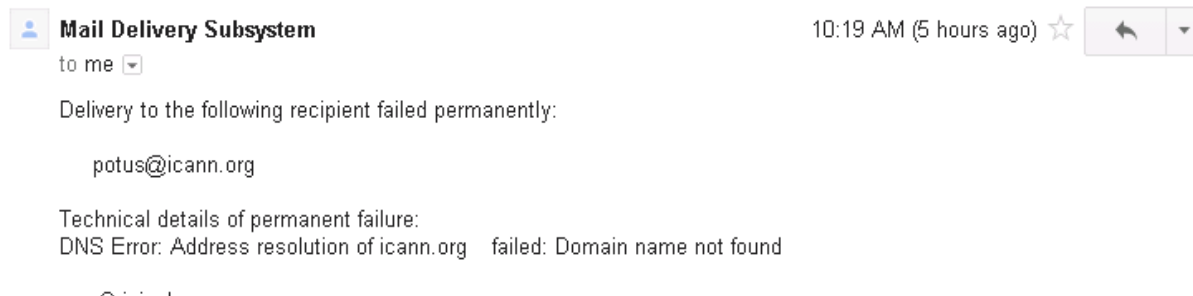
What do I need to look out for?

So what could go wrong? What if ICANN forgot to pay whoever they bought icann.org from (a Registrar like Godaddy)? Renewal fees are usually not large, but they are paid infrequently so unless they are being monitored for expiration, they are easy to forget. (Yes, ICANN could have a name expire, it does not get special treatment.)

The entry inside the DNS for icann.org would be dropped. This would mean your web browser would have no way of finding the IP address for ICANN's web server (e.g., 192.0.32.60) so all you would see is an error page or some search helper "service".



You might think this is not so bad, since someone would eventually send an email to ICANN to let them know something was wrong. But that would not work because email would be out of commission too since email also uses DNS to find icann.org's email server IP address (senders look at what is right of the "@" sign, e.g. icann.org from techsupport@icann.org).



Of course there is the telephone, but without being able to access the web page, it would theoretically require the use of an actual phonebook or telephone directory assistance to locate.

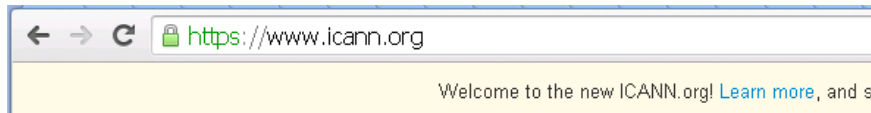
Back to our example, what if someone else registered icann.org after ICANN let it expire? Control of the DNS entries for icann.org would be handed over to the new Registrant³. Although ICANN would likely eventually regain control of the domain name, using various mechanisms such as Universal Dispute Resolution (UDRP)⁴ available to most, in the interim the new Registrant would be able to put up whatever web page they would like. In other words, instead of dropping DNS requests for atlarge.icann.org, the new Registrant could return 6.6.6.6 instead of 192.0.32.60 for the IP address which leads to a page made to look like the original ICANN web site. It could be also altered to ask for login information to various services and collect login and password credentials.

³ For ICANN accredited Registrars the name would be held for a renewal period by the Registrar and during this period only the original holder could register it. After that period, anyone could register it.

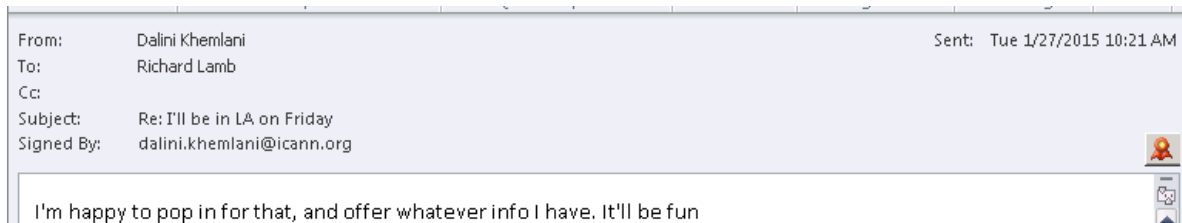
⁴ UDRP - <http://icannwiki.com/UDRP> URS - <http://icannwiki.com/URS>

Similarly, the new Registrant could set up an email server to receive all email for icann.org. Email frequently contains confidential or sensitive information.

Protocol security mechanisms such as SSL/HTTPS (frequently notated by a lock in the browser bar) whereby you would visit <https://www.icann.org> instead of <http://www.icann.org> do not protect you from a legitimate registration of icann.org by someone other than ICANN. Such mechanisms only rely on domain name registration information⁵.



As stated above, email from and to icann.org would be impacted. There would be no way other than looking at the style of the messages received to determine whether they came from ICANN the company or from the new registrant of icann.org. Similarly, there is no way to ensure email sent to icann.org reaches ICANN the company instead of the new registrant of icann.org. Secure email protocols⁶ like SSL for web sites could be deployed but, once again, the protocol security mechanisms rely only on domain registration information.

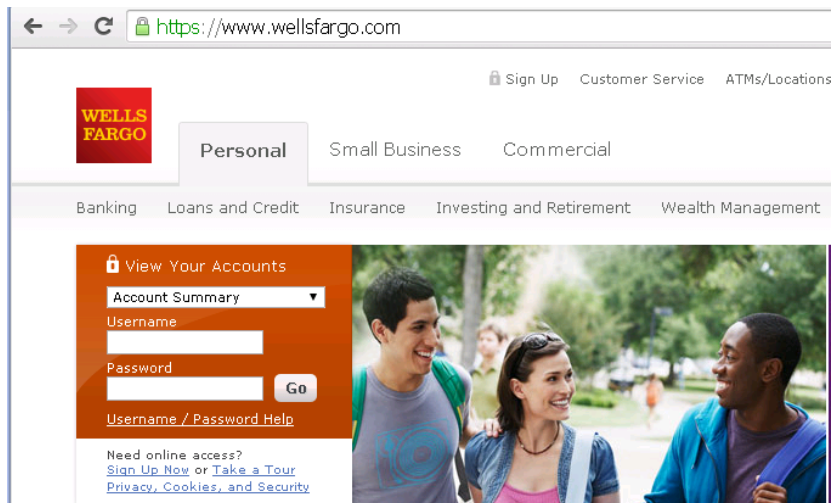


Replace ICANN with your bank or other financial institution in the examples above and you can see how registering and redirecting a dropped domain name could be profitable for some⁷.

⁵ Visitors to the web site could write down the details associated with a particular web site SSL certificate (found by clicking on the lock) and look for changes but this is cumbersome and unrealistic for most.

⁶ Through the same third party Certificate Authorities (CA) that provide SSL Web security.

⁷ Although not for fraudulent purposes, "drop-catching" - registering valuable domains immediately after they have expired - is an industry. http://en.wikipedia.org/wiki/Domain_drop_catching



Replace ICANN with the company you use for your email. What if you stopped receiving email? What if your incoming email went elsewhere or was made public?

Here is another example. Suppose ICANN was diligent about paying its bills from the Registrar⁸ to renew ICANN.org, but the person inside of ICANN responsible for updating icann.org information picked a simple password to log into the Registrar – or – the Registrar had poorly trained support staff? It then becomes a relatively simple matter for someone to hijack control of the domain name by either guessing ICANN's login credentials or using social engineering or phishing to get the Registrar to provide access to the account. With this control the hijackers can effect changes to the DNS to direct all web, email, and other traffic to their own servers for credential collection and other purposes. This DNS security issue has been experienced by a number of high profile corporations⁹.

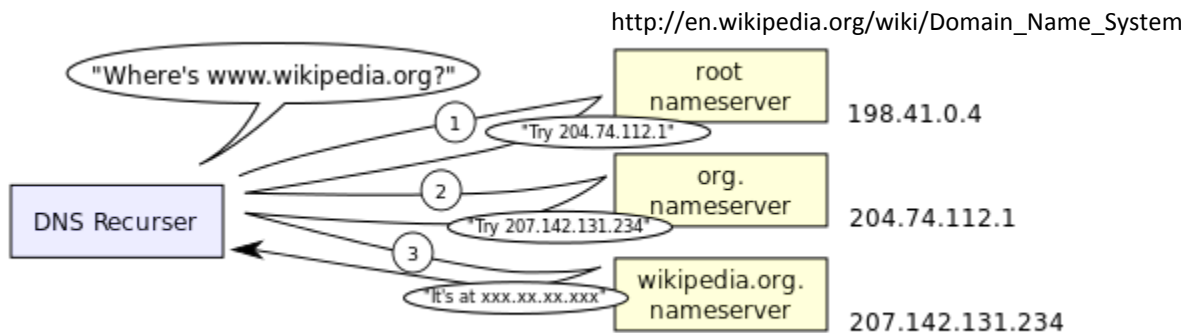
When we first described DNS, we told you that your computer asks the DNS for an address. When your computer asks the DNS for data it actually does so through an intermediary server operated by your ISP or enterprise called a name resolver or DNS recursor. This server then asks various other DNS servers on the Internet until it gets an answer¹⁰ and remembers (caches) it. By caching the answer, the next time someone asks for www.icann.org, the response can be returned immediately. This methodology saves a lot of time and bandwidth so it is a basic feature of the DNS. However, if the ISP's DNS recursor is not properly secured or configured incorrectly, it could be made to return the wrong IP address and send you to a rogue web

⁸ This is public information for all domain names and can be found using WHOIS protocol and tools.

⁹ See <http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf> for some examples shared by Google.

¹⁰ The DNS is hierarchical, e.g., to find the IP address corresponding to www.icann.org the caching server (referred to as a caching resolver or DNS recursor) asks the "root" servers and learns where the "org" servers are, then ask the "org" servers to find out where the "icann.org" servers are, and finally asks the "icann.org" servers which return the IP address for www.icann.org. Different groups/organizations manage each one of these sets of servers. Root server operators for the "root", PIR for "org", ICANN for "icann.org". See http://en.wikipedia.org/wiki/Domain_Name_System

site¹¹. Similarly, an industrious individual could intercept data on the wire/cable between you and your ISP and return anything they want. One solution might be for you to run your own DNS recursor¹² but not only would this add complexity to your setup, but there would be no benefit from the cached lookups from others. In addition the caching that occurs in a DNS recursor has its own set of threats that must be mitigated as we will see below.



Ok, you trust your ISP to secure their operations and the wire/cable between you and them – something you might justify¹³ as a purely contractual matter. Since the Internet was developed in an era where trust between the relatively small handful of players was assumed, legacy DNS has little in the way of built in security – you ask a question, you get an answer – with only a few checks that a response corresponds to a particular question.

Not surprisingly, people have found ways to lie to the ISP's caching recursor¹⁴ to effect a redirection of web, email, etc., traffic. Since the caching server remembers the lie, it also passes this lie to all of the ISP's other customers. This is referred to as cache poisoning and was a call to action for the Internet community to "fix" the DNS¹⁵. The result was DNS Security Extensions (DNSSEC)¹⁶. DNSSEC adds cryptographic records alongside existing DNS records that (DNSSEC enabled) DNS recursors can use to verify that records have not been modified. This can guarantee that what a domain name holder puts into the DNS (e.g., an IP address) comes out unchanged. Deployment of DNSSEC has been brisk, but since the DNS has not changed for over 20 years, it may be many years before we see the full benefits of DNSSEC. It is

¹¹ Brazil ISP case <http://securelist.com/blog/incidents/31628/massive-dns-poisoning-attacks-in-brazil-31/>

¹² A sample HowTo - <https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-caching-or-forwarding-dns-server-on-ubuntu-14-04>

¹³ Note however that most ISP agreements limit liability to the cost of the service.

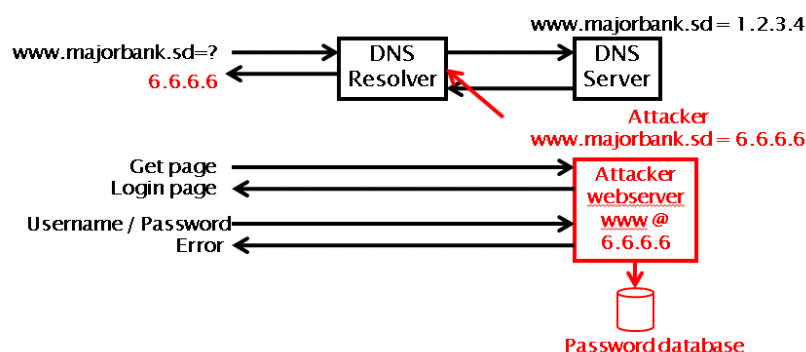
¹⁴ Cache poisoning details by Dam Kaminsky - <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>

¹⁵ Protocols were developed using the same technical, bottom-up approach that created the Internet itself with the Internet community (e.g., IETF, RIRs, ICANN, and others).

¹⁶ DNSSEC overview - <https://www.co.tt/files/amm-dnssec-business-case.pdf> and <http://www.internetsociety.org/deploy360/dnssec/>

important to note that DNSSEC does not fix all the problems with DNS security, but it is a step and one that has potential to secure much more than only DNS¹⁷.

DNS Cache Poisoning Attack



What do I do about it?

From the end user's perspective, poorly implemented DNS security, at best, means inaccessible web sites, bounced email and, at worst, means compromised credentials and email leading to financial loss, damaged reputation, and lost privacy.

So what should you do?

Exercise choice regarding services you use on the Internet as well as your ISP.

- Focus on their reputation, technical awareness and capabilities as criteria, e.g., do they have guidance for safety on-line?
- Is their web site secured with SSL?
- Do they use DNSSEC to protect their DNS or have plans to do so?
- If your ISP choices are limited, make requests that they incorporate available security options.
- Become that squeaky wheel and participate in consumer protection efforts¹⁸.
- Do not send confidential or sensitive information in email unencrypted.
- Be vigilant to sudden changes or any anomalies when visiting a web site.
- If something looks odd, has misspellings or other errors, research it further.
- Tools such as WHOIS¹⁹ to find out who a domain name is currently registered to can be helpful in determining actual ownership of a web site.


¹⁷ One application of DNSSEC – DANE - <http://www.internetsociety.org/deploy360/resources/dane/>

¹⁸ At ICANN and elsewhere. Governments also often have programs dedicated to safety on-line such as <https://www.stopthinkconnect.org/>. A well worded letter to the right officials can also do wonders.

¹⁹ The WHOIS protocol was developed along with the DNS and can be used to check the ownership records for almost every domain name out there. There are also many web sites that make using WHOIS easy, e.g., <http://whois.icann.org>. Some Registrars offer privacy options that do not publish the owner's identity even though recorded in internal records. This is certainly legitimate but makes independent verification difficult. In the end it is a matter of trust between you and your Registrar.

← → ↻ whois.icann.org/en/lookup?name=icann.org

简体中文 English Français Русский Español العربية

 **ICANN WHOIS BETA** ABOUT WHOIS POLICIES GET INVOLVED WI COM

icann.org **Lookup**

Showing results for: ICANN.ORG
Original Query: icann.org

Contact Information

<p>Registrant Contact Name: Domain Administrator Organization: ICANN Mailing Address: 12025 Waterfront Drive, Los Angeles California 90094-2536 US Phone: +1.4242171313 Ext: Fax: +1.4242171313 Fax Ext: Email: domain-admin@icann.org</p>	<p>Admin Contact Name: Domain Administrator Organization: ICANN Mailing Address: 12025 Waterfront Drive, Los Angeles California 90094-2536 US Phone: +1.4242171313 Ext: Fax: +1.4242171313 Fax Ext: Email: domain-admin@icann.org</p>	<p>Tech Contact Name: Domain Administrator Organization: ICANN Mailing Address: 12025 Waterfront Drive, Los Angeles California 90094-2536 US Phone: +1.4242171313 Ext: Fax: +1.4242171313 Fax Ext: Email: domain-admin@icann.org</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[SIDEBAR]

Phishing and DNS Security

Improving DNS Security ensures what you ask for from the DNS is what you get. It does not protect against the unscrupulous characters on the Internet - though it does make it more difficult for them to hide. Identifying them is still up to you.

Phishing²⁰ “is one such “impersonation attack”, and one of several ways attackers attempt to acquire sensitive information such as usernames, passwords, or credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication”.

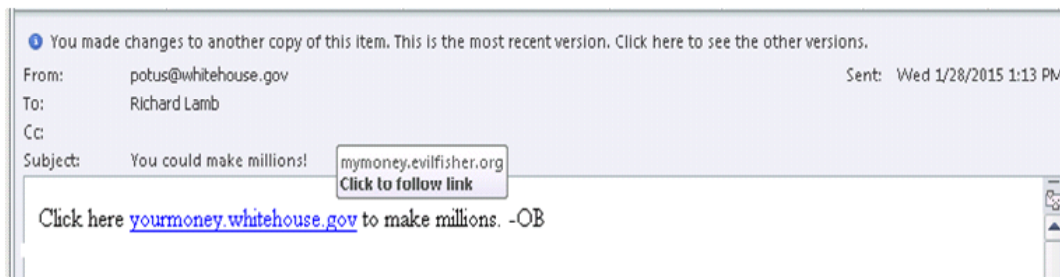
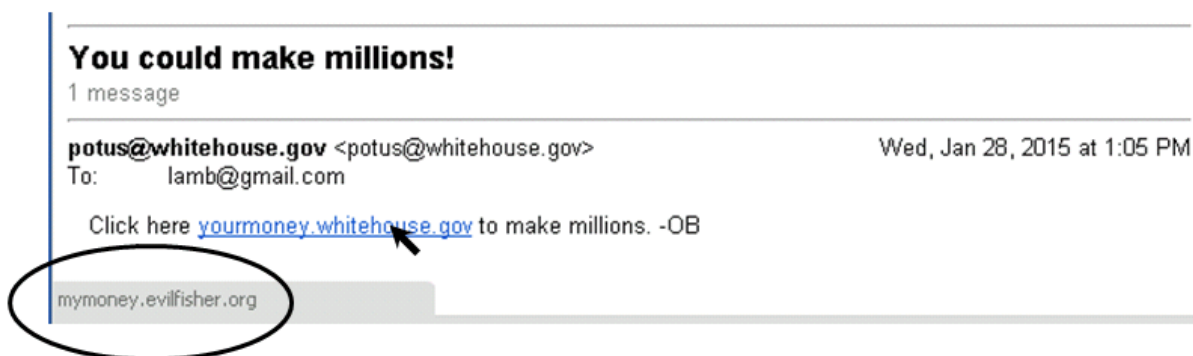
What do I need to look out for?

Phishing is mostly a social engineering attack where a message is presented in email or web site that looks like a legitimate one from, say, your bank with highlighted clickable

²⁰ <http://en.wikipedia.org/wiki/Phishing>

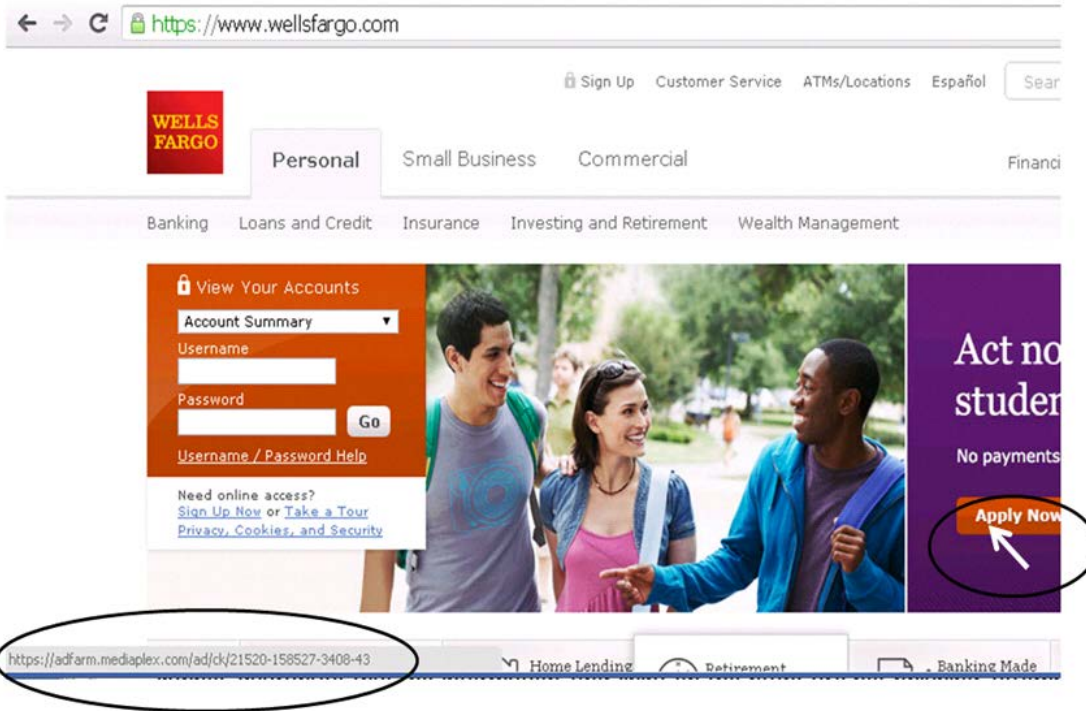
words or items in it. Attackers try to trick you into clicking on one of those links which will either install malware or take you to a login page that looks like your bank's to collect account and login information. For many email and web applications, hovering the mouse pointer over a link in the email exposes the true domain name where a click will take you. This should match your bank's domain name or a known source. However, today companies make use of a multitude of outsourced services so a legitimate link may not always be that obvious. Still, being cognizant of the real domain name in a link or for a web site goes a long way to not becoming a victim of a phishing attempt.

Unfortunately, currently, for email almost anyone can generate messages that appear to come from any email address. There are many measures being developed²¹ to make spoofing of email more difficult but they have yet to become universally deployed.



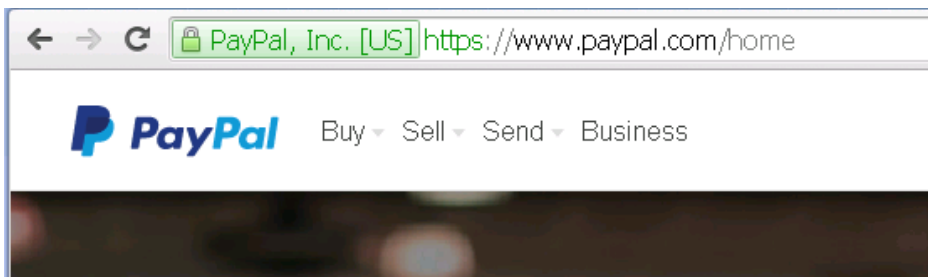
Clear Phishing Attempts

²¹ See - https://www.maawg.org/sites/maawg/files/news/MAAWG_Senders_Reputation_Concepts.pdf , SPF - http://en.wikipedia.org/wiki/Sender_Policy_Framework , DKIM - http://en.wikipedia.org/wiki/DomainKeys_Identified_Mail



**A link not matching the domain name but probably ok.
Other links on page match.**

Note that even an SSL authenticated web site (one with the lock icon in the browser) cannot guarantee that the information and links on the page are not phishing attempts. The “lock” only indicates that the web site was created by the holder of the domain name you see in the browser bar. This attestation is made by one of over 1500 third party certificate authorities (CA). A green lock area²² in the browser bar does indicate that the entity holding the domain name has been subjected to additional verification, so they might be easier to track down in case of difficulty. However, it is still not a check on the integrity of the entity and any one of 100 or more CAs can issue such certificates. Though less common, similar features are offered for secure email systems²³.



²² Extended Validation Certificate http://en.wikipedia.org/wiki/Extended_Validation_Certificate . Clicking on the lock typically displays more detailed information.

²³ S/MIME - <http://en.wikipedia.org/wiki/S/MIME>

What do I do about it?

In the end it is still up to you to decide what looks like phishing and what does not. Be suspicious of unsolicited messages²⁴. Verify any unsolicited requests by contacting your institution via previously verified means. Email readers and web browsers are improving and have learned to catch many phishing attempts and industry groups²⁵ continue working to solve the problem, but it is a cat and mouse game. Inspect the real domain name by hovering the mouse over any links. SSL web sites, particularly those with extended validation indicated by the green lock icon, do provide some level of security. But it is still important to inspect domain names in the browser bar and elsewhere to see if they make sense. For a deeper dive use tools like WHOIS described previously to see who owns the domain. And of course, if your browser emits a warning when visiting an SSL site, don't go on. If in doubt, don't click. But if you must visit the link, type it in yourself.

[/SIDEBAR]

DNS Security from the perspective of the domain name holder (Registrant)

Background

DNS Security from the perspective of the domain name holder (Registrant) has slightly different implications. For the Registrant a domain name is not only a mechanism to communicate with customers but it also represents an asset and brand and should be treated as such.

Control of this asset is critical. Beyond avoiding unintended expiration it is important to ensure you have clear title and full control of the domain name. With so many ways to obtain a presence on the Internet, it is not always clear who owns the domain name or who can change its associated information.

A lack of clarity here may cause difficulty later in resolving disputes, responding to accusations surrounding phishing or spam, changes to your DNS or web hosting infrastructure, or corporate ownership.

What do I need to look out for?

Let's say you use one of the many readily available web hosting companies to create a web page and handle email, you choose a "one-click" package. You might be able to set something up in an afternoon. As your business grows and your Internet visibility increases you a) outgrow your current hosting company and either need to choose another or bring web server and email operations in-house to improve service, security,

²⁴ <http://www.securityskeptic.com/anti-phishing-and-fraud-resources.html>

²⁵ <http://www.antiphishing.org/> and <http://en.wikipedia.org/wiki/MAAWG>

and data analysis; or b) get a lucrative offer to buy out your operation. At this point, you discover that the domain name you selected is tied to the “one-click” package you started with and is only leased from the hosting company. You have built a brand on this domain name but cannot move or sell it.



For the Registrant it is critical in today’s outsourced, cloud hosted world to find out who you are acquiring the domain name from, i.e., who is acting as the Registrar²⁶ and to make sure that Registrar records you as the domain name holder. You want to have clear title to that domain name²⁷, and full control over the parameters associated with the domain name such as the name servers²⁸ (IP addresses) and who is listed as administrative and technical contacts for the domain name.

You got a great hosting package deal that costs no more than a cup of coffee a month, including the domain name with you clearly listed as its holder. You know this because you used a look-up protocol called WHOIS²⁹ to independently check the published records for your domain name. Your web site and email are up and running and your business is processing orders. But you are a startup and have many more fires and emails to attend to than the \$5.95 warning messages coming from some organization you vaguely remember from a year ago. So your web site goes off-line (yes this happens often) and, even worse, someone else registers your domain name. Your customers are confused, orders stop coming in, and the new owner of the domain name is at best uncooperative or at worst, doing something that harms your reputation³⁰.

²⁶ Hosting companies are not always Registrars and Registrars do not always run their own hosting services.

²⁷ Policies vary depending on what top level domain (TLD) the name is under. TLDs such as .de, .ru, .tk, are country code TLDs (ccTLD) with policies ultimately dependent on their countries (Germany, Russia, and Tokelau in this case). TLDs such as .com .ibm or .كڤش are global TLDs (gTLD) and though having varying polices must adhere to a baseline set of policies set forth by ICANN. The takeaway here is to familiarize yourself with any special TLD policies.

²⁸ Being able to readily control what name servers will be queried by those seeking to visit your web site or send email is important to quickly mitigate attacks.

²⁹ See earlier section. The WHOIS protocol was developed along with the DNS and can be used to check the ownership records for almost every domain name out there (approx. 250million at time of writing).

There are also many web site that make using WHOIS easy, e.g., <http://whois.domaintools.com/google.com> for google.com. Some Registrars offer privacy options that do not publish the owner’s identity even though recorded in internal records. This is certainly legitimate but makes independent verification difficult. In the end it is a matter of trust between you and your Registrar.

³⁰ See ICANN SSAC 10 and 11. <https://www.icann.org/en/groups/ssac/renewal-advisory-29jun06-en.pdf>
<https://www.icann.org/en/groups/ssac/renewal-nameserver-07jul06-en.pdf>

Luckily you and the new Registrant used ICANN accredited Registrars³¹ that are required to have policies such as the Uniform Domain Name Dispute Resolution Policy³² (UDRP) in place to resolve such disputes. But the process takes time and leaves your current and potential customers looking elsewhere for product.

Alright, you pay your bills on time, even the small ones but you are not so good at keeping track of long passwords. So you use a simple password or are frequently calling up the Registrar and asking for a password reset. You go to the office one day and you notice very few email messages and no orders. So you try to go to your administrative web page to find out what is going on only to find that your web site appears to have been defaced. What has actually happened is that someone called your Registrar pretending to be you and said they forgot their password. Despite their best efforts, social engineering can be very effective and, this being a regular occurrence from you, Registrar personnel succumbed to the attack. The attacker has now logged in and changed the name server entries for your domain name to point to his name servers. His name servers now respond to lookups for your web site and email redirecting requests and emails to his web and email servers. You contact your Registrar to fix this but have a difficult time convincing them you are who you say you are.

What can I do about it?

Your initial questions for a Registrar or hosting provider also acting as a Registrar should be: do they have well defined processes for transferring domain names (and web content) away from (to) their infrastructure³³? How do they notify you of updates, expiration, and other status changes to your service (email, text, phone)? Do **YOU** have staff whose responsibilities include handling these notifications and monitoring the condition of the web site³⁴ and WHOIS record? Does the Registrar have published procedures for dispute resolution³⁵? How do they identify you (password, pin, favorite dog, government id)? Do they use two-factor authentication methods³⁶ (electronic token, text, one time passwords, etc) that might improve security while reducing the need for burdensome password policies?

³¹ <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

³² <http://apps.americanbar.org/dch/thedl.cfm?filename=PT021000/newsletterpubs/URS-UDRPComparisonChart.pdf>

³³ Many Registrars have options to “lock” your domain to prohibit transfer to another Registrar without you first turning the lock off from a management page as well as notifications and a grace period before a transfer is complete. Though not a guarantee, this adds another layer of protection.

³⁴ Various third party services exist to simplify this like “visual ping” and “pingdom”.

³⁵ Most often the solution is to simply contact the Registrar to find out what remedies exist before going to UDRP.

³⁶ http://en.wikipedia.org/wiki/Two_factor_authentication

2-factor authentication



A text message with your code has been sent to Mobile phone

Verification code

Verify



Enter Security Code

Secure Log In

Press the button on your security key and enter the 6-digit code that appears.

Serial number: 12345678901234567890

6-digit code:

Submit



There are well over 1000 ICANN accredited Registrars³⁷. Make an informed choice. In an effort to assist in this, ICANN's Security Stability Advisory Committee (SSAC) developed a list of questions to ask prospective Registrars. This can be found at "A Registrant's Guide to Protecting Domain Name Registration Accounts"³⁸. These include:

- What approach does the Registrar use to prove the Registrant's identity to thwart impersonation, social engineering hijack attempts, lost password recovery, transfer scams? Legal documents, government issued identification, etc?
- What sort of management interface is used to ensure only users the Registrant authorizes can access account and WHOIS information, name server, DNSSEC keys, and other technical parameters? Username and password (complexity and update requirements), two-factor authentication, one-time-passwords, digital certificates, SMS, telephone callback...? Is the Registrar's web site protected with HTTPS/SSL using a valid certificate? Is there per-domain or overall account access? How is account data secured against breach?
- How does the Registrar notify the Registrant of changes to their account or technical information? Email, call... Is there access to logs for account activity / updates / reporting / auditing?

³⁷ <http://www.internic.net/regist.html>

³⁸ ICANN SAC044 - <https://www.icann.org/en/system/files/files/sac-044-en.pdf>

- Does the Registrar support options to block unauthorized transfer of a Registrant's domain name or modification? Can this be performed at the Registry level (e.g., Domain Lock)? Does the Registrar provide any options to avoid unintended expiry of a domain name?
- How is communication with Registrant secured? Secure email (S/MIME, PGP), postal mail, telephone, SMS?
- Does the Registrar offer services to monitor failure/change/WHOIS/impersonation/hijack attacks on the Registrant's domain name?
- Does the Registrar support DNSSEC, i.e., can they accept and register DNSSEC key material?
- If desired, will the Registrar handle DNS and DNSSEC services for the Registrant? If so, is there a brief description of how and by whom this DNS hosting service is provided? How is it secured and how will it scale in the face of natural traffic growth and attacks?
- Does the Registrar have a streamlined process for transferring domain names to and from the Registrar should the Registrant elect to do so?
- Does the Registrar offer privacy protection services?
- Does the Registrar have published documentation on incident and abuse response practices including what assistance if any may be provided to the Registrant in registration disputes.
- Does the Registrar pass and maintain any third party audited certifications such as PCI, ISO 27000, SysTrust³⁹?

Although it is unlikely that Registrars can respond to all these questions with the highest assurances, they are a good starting point to assess whether the Registrar has made DNS security part of their overall business and therefore provide the Registrant with the domain name protection and peace of mind to focus on other aspects of their business. Some Registrars publish FAQs or other documents enumerating their services to make this process easier.

DNS Security from the perspective of Law Enforcement

Background

DNS Security from the perspective of law enforcement (LE) takes on a different meaning. Like the rest of society, criminals have embraced the Internet and are increasing relying on it to support their operations and using it as a vehicle for criminal activities. Identifying the source of such activities becomes a first step for LE and one in which the unique identifiers of the Internet, the DNS and IP addresses in particular, is key.

³⁹ ISO: http://en.wikipedia.org/wiki/ISO/IEC_27000-series SysTrust: <http://www.webtrust.org/> PCI: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

What do I need to look out for?

You are notified of an offending web site, say, one selling harmful pharmaceuticals and want to get it off the web⁴⁰. Tools like WHOIS⁴¹ applied to the domain name portion of the web page address are the first step to identifying the source. You can typically even get the phone number, email, and postal address of the domain name holder. However, WHOIS data is not sufficient or always accurate or available. Billing information which may be more accurate would fall under these privacy restrictions and therefore not visible via WHOIS.

Lets say the WHOIS information is accurate and we contact the Registrant and ask them to shut down their web site. If cooperative, we are done. Otherwise we might be looking at legal proceedings which could be particularly cumbersome across jurisdictions. An alternative is to work with the Registrar listed in the WHOIS to see if the Registrant is violating the Registrar's published Terms of Use (TOS)⁴² or Acceptable Use Policy (AUP). If the Registrant is violating these, it allows the Registrar to modify the name server records for the domain name effectively shutting down public access to the site even though they cannot shut down the site itself. To shut down the site investigators can contact the hosting provider operating the site⁴³ and ask them to shut it down based on their TOS or AUP.

Should these efforts prove fruitless an investigator could work with the top level domain (.com, .se, .link, etc...) operator to remove name server records (like with the Registrar) based on their TOS⁴⁴ or AUP.

⁴⁰ Detailed guidance is available here: <https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf>

⁴¹ See previous references

⁴² Example: <https://domains.google.com/tos>

⁴³ As we will see, WHOIS can be used to determine the organizations behind IP addresses as well as domain names. This would help in determining the hosting provider for a web site.

⁴⁴ Example <http://www.donuts.co/policies/acceptable-use/> for TLDS <http://www.donuts.co/tlds/>



com

Lookup

Showing results for: com

Original Query: com

Contact Information

Registrant Contact

Name: VeriSign Global Registry Services
Organization: VeriSign Global Registry Services
Mailing Address: 12061 Bluemont Way | Reston Virginia 20190, United States
Phone:
Ext:
Fax:
Fax Ext:
Email:

Admin Contact

Name: Registry Customer Service
Organization: VeriSign Global Registry Services
Mailing Address: 12061 Bluemont Way | Reston Virginia 20190, United States
Phone: +1 703 925-6999
Ext:
Fax: +1 703 948 3978
Fax Ext:
Email: info@verisign-grs.com

Tech Contact

Name: Registry Customer Service
Organization: VeriSign Global Registry Services
Mailing Address: 12061 Bluemont Way | Reston Virginia 20190, United States
Phone: +1 703 925-6999
Ext:
Fax: +1 703 948 3978
Fax Ext:
Email: info@verisign-grs.com

The final option may be a court order, but jurisdictional differences and bureaucracy often make this ineffective. By the time any formal international proceedings were brought to bear, the culprit would have moved Registrar/Registry/hosting operations on to other jurisdictions. The need for effective, common, cross-jurisdictional regulations in the borderless world of the Internet is well known and is the focus of many efforts⁴⁵.

Assuming you have gained the cooperation of the authorities in the Registrant's jurisdiction. However, what if the offending web site is just one of many sharing the same domain name, e.g., www.example.com/badwebsite/ and www.example.com/goodwebsite/ ? In this case the offending party may not be the Registrant of the domain name, although they may be complicit, but a customer of his or the company hosting the web sites. To limit collateral damage, any such efforts would therefore need to be coordinated with the hosting company and Registrant.

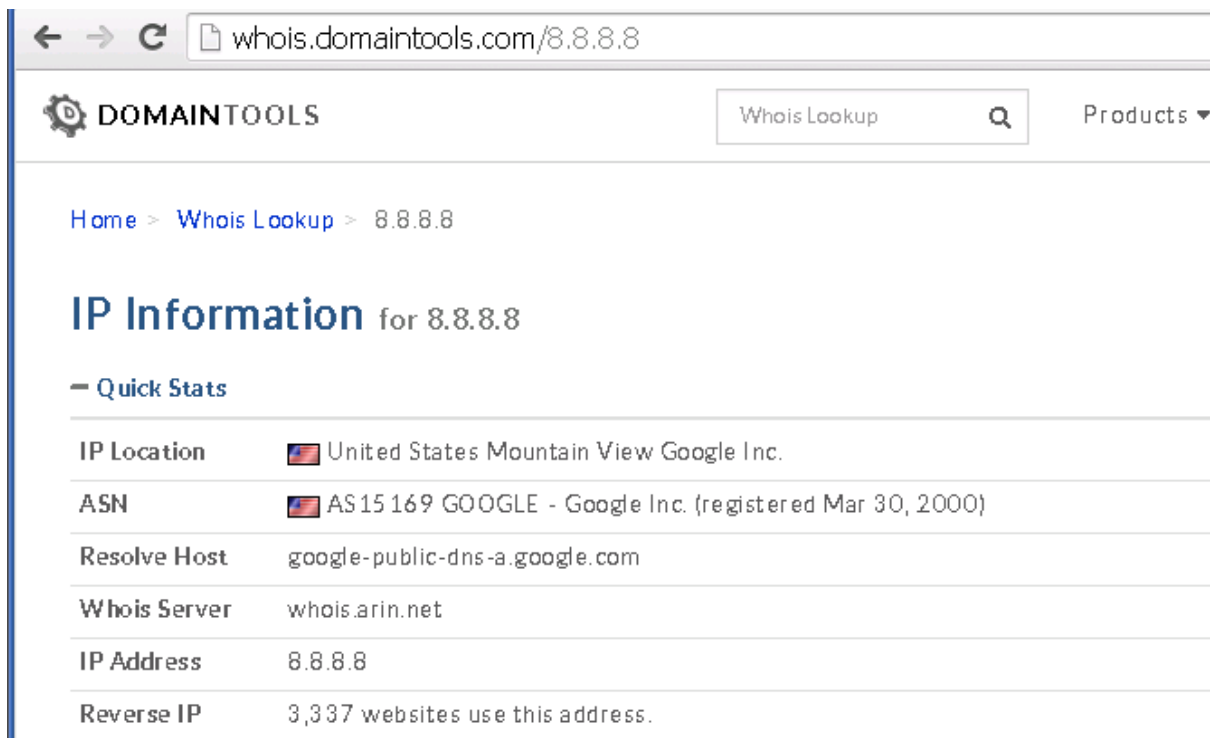
A similar interest may be in identifying the true source of an email by examining the domain name portion of the "from" address. This would follow the same approach as above eventually requiring the cooperation of the company hosting the email server for the Registrant to identify a particular account holder.

⁴⁵ <http://www.internetjurisdiction.net/progress-report-2013-14/>


However, since anyone can generate an email appearing to be from someone else⁴⁶ finding the true source of an email is a bit more difficult. Though not always made visible in email readers, an email message has a header section with To, From, Subject, Date and other information. In particular as an e-mail travels from the sending machine through various intermediate servers a “Received” line with IP and domain name information for each server is added.

Careful investigation of these headers can at least help track down the location of the machine originating the email. With only IP addresses this can be done using the DNS in reverse, i.e., looking up a domain name from an IP address (8.8.8.8 in example below) as well as querying WHOIS services for IP addresses. Although not as comprehensive as the forward DNS, it does provide clues as to the true identity of a bogus sender.

```
lamb@vms:~$ dig +short -x 8.8.8.8
google-public-dns-a.google.com.
```





← → ↻

 DOMAINTOOLS Products ▾

[Home](#) > [Whois Lookup](#) > 8.8.8.8

IP Information for 8.8.8.8

— Quick Stats

IP Location	 United States Mountain View Google Inc.
ASN	 AS15 169 GOOGLE - Google Inc. (registered Mar 30, 2000)
Resolve Host	google-public-dns-a.google.com
Whois Server	whois.arin.net
IP Address	8.8.8.8
Reverse IP	3,337 websites use this address.

⁴⁶ See previous references. Though usually done with a script, demonstration web sites exist. <https://ultimate-anonymity.com/web-based-remailer.htm> is just one of many examples.

What can I do about it?

Learn more about how the DNS works and what tools and resources are already available⁴⁷. The key here is having accurate Registrar and host provider records and clear take down policies. Work with the Registrar and other communities to encourage maintenance of accurate WHOIS information with proper privacy controls⁴⁸. Ensuring the security and accuracy of the registration information behind domain names not only helps LE quickly identify culprits but also makes sure the wrong person is not targeted. Building relationships with these communities and fellow LE personnel across national borders is the other key to achieving the desired outcomes⁴⁹. Share experiences with the technical community to help improve e-mail standards and security⁵⁰.

Summary

From the web and email, to brand identity, to authentication for secure communications, to the inter communications between systems and devices, and the Internet of Things, the DNS is intertwined with all aspects of the Internet. The security of the DNS affects us all. Therefore, in an attempt to raise awareness regarding DNS security this guide has presented an overview of the different issues members of the Internet ecosystem would experience related to the DNS. We have by no means covered all cases. Instead we have focused on the most prevalent issues for each community. However, common to the cases is a need to better formalize DNS operations – for the domain name holder/Registrant as well as the Registrar – and for end users to have a better understanding and be cognizant of what lies behind a domain name. Formalized processes and practices also clarifies ownership and helps resolve related disputes as well as helping law enforcement perform their duties with minimal impact on operations. The overarching requirement in all these efforts is cooperation. The basis for the Internet's existence is cooperation (at technical, business, and government levels). It is the same cooperation that is needed to keep it safe.

For Further Information

Here are some useful links to information on specific topics related to DNS security.

⁴⁷ ICANN regularly hosts LE workshops and provides free training to LE where there is sufficient interest. We also publish thought pieces such as: <https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf>

⁴⁸ WHOIS work inside ICANN - <http://whois.icann.org/en/policies>

⁴⁹ “DNS Changer” was an excellent example of what can be accomplished through building international relationships between investigators, private and civil sectors. <http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/>

⁵⁰ DNSSEC and its application to web site (SSL, DANE) and e-mail (S/MIME) security is one such outcome.

DNS videos:

<https://www.youtube.com/watch?v=72snZctFFtA>

<https://www.youtube.com/watch?v=2ZUxoi7YNgs>

<https://www.youtube.com/watch?v=6uEwzkfViSM> – DNS Resource Records

<https://www.youtube.com/watch?v=833Qnc-7-ug> – DNS Zone Files

Other IT free training videos:

https://www.youtube.com/channel/UCmJcrJ_30p6s_OTbyTFfbqQ

DNSSEC:

<http://www.infoworld.com/article/2608759/security/security-why-you-need-to-deploy-dnssec-now.html> Why you need to deploy DNSSec now

https://www.youtube.com/results?search_query=DNSSEC

DNS attack videos:

<https://www.youtube.com/watch?v=lb2vdxEB-C8> - cache poisoning

<https://www.youtube.com/watch?v=qftKfFVHVuY> - Kaminsky exploit

<https://www.youtube.com/watch?v=t6oYatt8x0E> - DNS changer

<https://www.youtube.com/watch?v=Gz2kmmsMpMI> - cryptolocker

<https://www.youtube.com/watch?v=qBXrncdEifo> - Steve Gibson

Distributed Denial of Service:

https://www.youtube.com/results?search_query=DNS+ddos+attacks