- Protecting and securing domain names (passwords, authentication, lock, how to detect Phishing).
- Good domain name security management, projects, and campaigns, HTTPS.
- Introduction to DNSSEC, what it protects against and how.
- DNSSEC implementation, NPOC promotion of DNSSEC implementation to NGOs

Brian Gutterman and David Huberman, **ICANN** Org

NPOC Webinar Series #5

31 March 2021

ICANN

ICANN Learn

- Free, online learning platform: https://learn.icann.org
- Set your dashboard to your preferred language.
- Registrant Basics: Essentials for Domain Name Holders.
- Cybersecurity Basics

NPOC Webinar Series – February-April 2021

Webinars 5, 6 and 7
31 March; 7 April, 14 April - 14:00 UTC

- Protecting and Securing Domain Names
- Good domain name security management, projects, and campaigns, HTTPS.
- Introduction to DNSSEC, what it protects against and how.
- DNSSEC implementation, NPOC promotion of DNSSEC implementation to NGOs.
- DoH (DNS-over-HTTPS) and DoT (DNS-over-TLS).
- Webinar series wrap-up; Q&A; next steps

Protecting and securing domain names (passwords, authentication, locks,).

Domain Names are valuable assets

For many registrants, domain names (and the services connected to them, like websites and emails) are essential to their professional and personal lives. Whether used for online commerce, or simply to communicate with family and friends, domain names are valuable assets and should be managed with care.

Protecting your domain name(s)

Best practices to help you prevent hijacking or unauthorized transfer of your domain name:

- **Register with an email address that is not connected to your domain name.** When you register your domain name, you will be asked to provide contact information, including your email address. This information goes into the WHOIS record for your domain name, which might be viewed publicly. It is best to use an email address that is not associated with the domain name you are registering. For instance, if your domain name is example.com, a best practice is to use an address in WHOIS that is not user@example.com.

- **Here's why.** if your domain name is hijacked by someone who has gained access to your account with the registrar, that person will likely alter the WHOIS information to remove you as the registered holder of the domain name. If you used an email address that is not associated with your domain name in WHOIS, you will be able to provide that email address as evidence to the registrar that you were the registered holder of the domain name before it was altered by unauthorized access to your account.

Protecting your domain name(s)

(Contd.) Best practices to help you prevent hijacking or unauthorized transfer of your domain name:

- **Create a strong, unique password.** Protect your domain name from cybercriminals by creating a unique, strong password. Online services are compromised frequently, making user names and passwords available to criminals who may attempt to hijack your domain name using the information you provide for other accounts. Avoid this by creating a strong password that you use exclusively for your domain name account.

- **Do not share your password.** You are responsible for the security of your domain name. You should never give anyone the login information to your online account. This includes web hosting providers or web designers as well as friends and colleagues. It is not recommended that you list website designers, hosting providers, or any other third parties as the registrant(s) of your domain name. If you choose to do so, seek legal advice as to contractual obligations that third parties should adhere to with regards to the administration of your domain.

Protecting your domain name(s)

(Contd.) Best practices to help you prevent hijacking or unauthorized transfer of your domain name:

- **Inquire about multistep authentication.** Some registrars offer registrants the ability to implement a multistep authentication when accessing your account. This provides added protection by requiring a unique security code, in addition to your username and password, to access your online accounts. Refer to the terms of your registration agreement to see if multistep authentication is available.

- **Check the email account(s) associated with your domain frequently.** Whatever email address or addresses you provide, you must be sure they are active accounts and that you check them regularly. You want to keep your contact information up to date to be sure you receive WHOIS Data Reminder Policy (WDRP) notifications, renewals, and other important notices from your registrar. This is particularly important for those who use a privacy or proxy service. If you use a privacy service, consider leaving your name as the registrant of record in the WHOIS. This can serve as another evidence to your registrar that you were the registered holder of the domain name.

Protecting your domain name(s)

(Contd.) Best practices to help you prevent hijacking or unauthorized transfer of your domain name:

- **Ask your registrar to put a *transfer lock* on your domain name.** You can request that your registrar put a *transfer lock* on your domain name. Putting this lock on your domain name is not a fail-safe way to guard against unauthorized transfer or hijacking of your domain name, but it could be another layer of security. Each registrar has a different way of implementing the transfer lock. Some require two-factor authentication to remove the lock; some simply require authorization from the registrant. Check with your registrar about their policies regarding transfer lock and decide whether it is a service that's right for you.

- **Be smart about your online behavior.** Be cautious with the links you click in emails, with the attachments you open, and with the websites you visit. These are means that criminals can use to steal your username and password.

Beware of phishing scams (and how to protect yourself)

Beware of Phishing Scams

- Phishing attacks are a type of fraud that cybercriminals utilize to lure others online, including registrants, into doing what the criminals want them to do. Phishing may result in others voluntarily giving away their username and password or clicking a link that will lead to their devices being infected with malware, which is software that, when installed, performs unwanted or malicious activity.

- If an attacker can gain access to a registrant's private domain name registration information and passwords, they can potentially redirect the domain to wherever they like. As such, it's immensely important that you take note of any suspicious or unsolicited emails.

Beware of Phishing Scams

- Phishing emails may claim that your domain name registration needs to be renewed and that you must pay some sort of fee to get it back. These malicious campaigns typically use deceptive techniques such as forging a trusted sender's address or domain or using a similar or lookalike domain. Phishing messages typically ask for the reader to reply, call a phone number, click a link, or open an attached file, which results in stealing personal information or gaining some other advantage over the victim.

- Sometimes phishing emails aimed at registrants may appear to come from ICANN (even using ICANN's branding and logo or sender email addresses containing the name "ICANN"). It is important to know that ICANN does not send emails directly to registrants about managing their domain names, and never requests payment of fees from registrants.

Protecting yourself from Phishing

- Carefully review every email you receive
- Phishing emails and websites often mirror familiar visuals and language, may include the logos and branding of the organization and appear that the organization is the sender
- Be suspicious of any email or webpage from ICANN that offers domain renewals or registration services.
- ICANN org does not process domain renewals or send WHOIS data privacy notices.

Protecting yourself from Phishing

- Email attachments may contain malware
- Hyperlinks may direct you to malicious websites or forms
- Never enter your password into a page you arrived at by following a link in an email
- Phishing emails often contain a false sense of urgency (such as legal scams, expiring domain renewals)

Measures for additional protection

- Be suspicious of any email that offers domain name management services from ICANN. ICANN does not offer domain name management services or process domain registrations and will never collect fees from registrants directly.

- ICANN will never send registrants a WHOIS Data Reminder Policy (WDRP) notice, registration data verification request, domain name expiration reminder, or domain name renewal request message. If you receive an email about your domain that purports to come from ICANN, contact your sponsoring registrar directly to enquire about the validity of that message.

- Contact your sponsoring registrar directly for any concerns about the status of your domain name.

Measures for additional protection

- Use ICANN-accredited registrars to register and manage your domain name(s) and always research the reputation and service record of registrars before selecting one. If you're not entirely comfortable with a registrar after you register a domain name with them, you can and should consider transferring your domain name to a registrar you trust.

- Use Transport Layer Security (TLS) HTTPS when you access your domain name registration account to prevent someone intercepting your communication with your registrar.

- **Always be proactive!** Domain name registrants are important players in combating DNS abuse. We encourage you to always be vigilant and proactive in securely and responsibly managing your domain name(s).

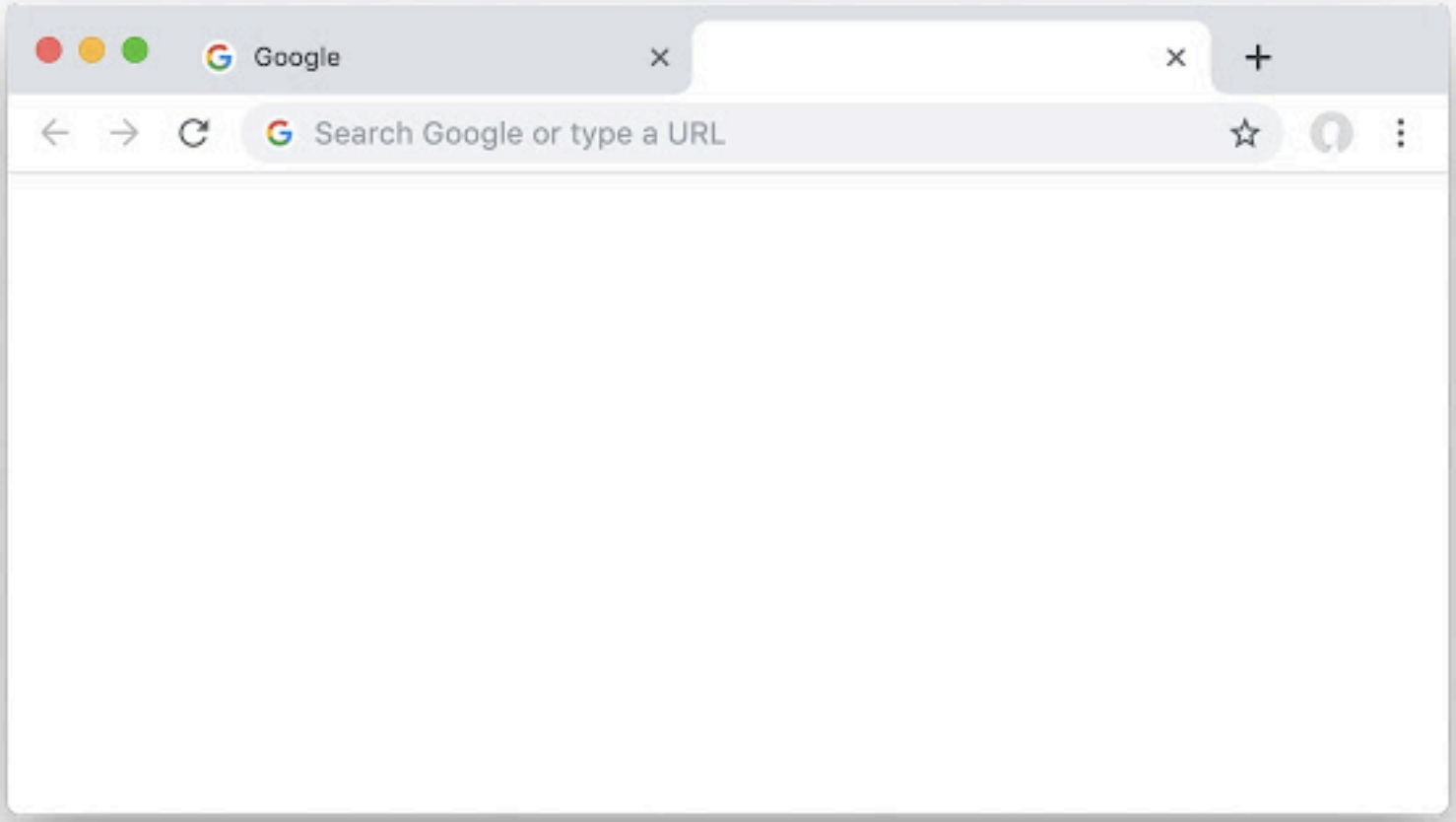
Sign Your DNS Zones With DNSSEC

- Another step you can take to protect your domain name and contribute to the overall security of the Domain Name System (DNS) is by DNSSEC-signing all the data associated with each of your domain names.

- DNSSEC (Domain Name System Security Extensions) reduces the chances an attacker will be able to substitute their answers in response to DNS queries. By creating digital signatures over your domain's zone data, clients looking up your domain names can verify the information they receive is what you had placed in the zone.

- Many DNS software packages and registration systems have tools that automate DNSSEC-signing. Check to ensure that DNSSEC-signing is enabled in your DNS software and at your registrar and that your registrar has the necessary information (your Delegation Signer record or your DNSKEY) to help establish trust in the information they just signed.

Introduction to DNSSEC


Google
Search Google or type a URL

What is DNSSEC

DNSSEC is shorthand for:

- Domain Name System Security Extensions

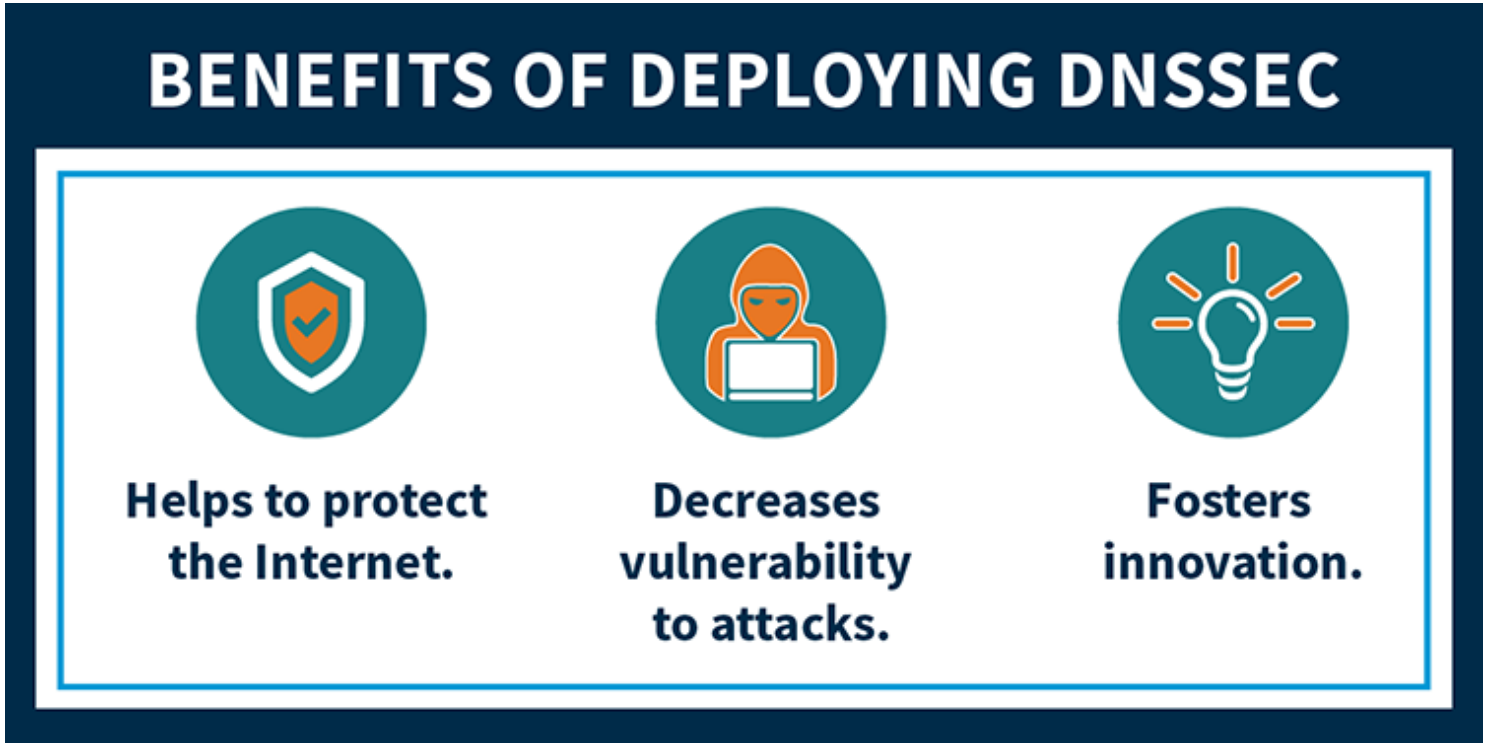
What DNSSEC Does

- DNSSEC uses public-key cryptography and digital signatures to provide:
  - Data origin authentication
    - "Did this response really come from the *example.com* zone?"
  - Data integrity
    - "Did an attacker (e.g., a man in the middle) modify the data in this response since the data was originally signed?"
- DNSSEC offers protection against spoofing of DNS data

What DNSSEC Doesn't Do

- DNSSEC does not:
  - Provide any confidentiality for DNS data
    - No encryption
    - The data in DNS is presumed public
  - Address attacks against DNS software
    - DDoS
    - "packets of death"
    - Etc.

DNSSEC is Good!



DNSSEC Implementation for NGOs

Some Important Lessons

- We have decades of experience with implementing DNSSEC on resolvers.
- Experience teaches us it's challenging.
  - Learning curve isn't steep
  - Maintaining a properly operating and validating resolver requires good (and written down) processes and procedures
  - To ensure continuity of operations over months and years, more than one staff member needs to understand basic DNSSEC skills
  - Key management needs to be properly thought out and documented

ICANN Offers Practical Learning Opportunities

- ICANN's Office of the CTO (OCTO) has developed courses to build skills with DNS and DNSSEC
- Hands-on DNSSEC workshops are available to be scheduled through your local GSE representative
- At ICANN meetings, we offer DNSSEC hands-on workshops, typically lasting a full day

Engage with ICANN

Thank You and Questions

For more information: icann.org/registrant

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann