



<DNS Abuse>

An Individual User Education
Campaign

Matthias M. Hudobnik



<DNS Abuse>

An Individual User Education Campaign



<DNS Abuse>

An Individual User Education Campaign



Cybersecurity in Healthcare

- 1. Awareness**
Share information with healthcare staff. Brief them on the ongoing situation and ask them to disconnect in the case of infection. Raise awareness of the increase in cyber scams and the importance of cybersecurity for every individual.
- 2. Disconnect**
Freeze all activity if your system has been compromised. Disconnect the infected machines from others and from any external drive or medical device. Go offline from the network and immediately contact the national CSIRT.
- 3. Data backup and restore**
Effective backup and restore procedures ensure business continuity. Have a plan in place to deal with a system failure that may disrupt core services.
- 4. Medical Devices**
If medical devices have been impacted, coordinate incident response with the manufacturer and collaborate with vendors.
- 5. Network Segmentation**
Consider network segmentation to improve your organisation's cybersecurity. Segmentation can control the flow of traffic and limit how far an attack can spread.

Cyber secure ecommerce

- 1. Secure your website for customers**
You must have the right security to protect your business and your customers. Use https connections, enable two-factor authentication where possible and test the security of your website.
- 2. Protect your assets**
Like any other business asset, information needs to be managed and protected. Information security is the protection of information within a business, including the storage, processing and transmission of information.
- 3. Store passwords securely**
If customers need to create accounts to buy from your website, make sure all passwords are stored securely – according to the rules of the industry.
- 4. Comply with data protection requirements**
When processing customers' personal data, ensure you comply with the legal framework on data protection.
- 5. Monitor and prevent incidents**
Have a security incident response policy in place. Take measures to prevent, monitor and respond to security incidents, including personal data.



<DNS Abuse>

An Individual User Education Campaign



SIM SWAPPING – A MOBILE PHONE SCAM

SIM swapping occurs when a fraudster, using social engineering techniques, takes control over your mobile phone SIM card using your stolen personal data.



HOW DOES IT WORK?

A fraudster obtains the victim's personal data through e.g. data breaches, phishing, social media searches, malicious apps, online shopping, malware, etc.

With this information, the fraudster dupes the mobile phone operator into porting the victim's mobile number to a SIM in his possession



The fraudster can now receive incoming calls and text messages, including access to the victim's online banking



The victim will notice the mobile phone lost service, and eventually will discover they cannot log in to their bank account



WHAT CAN YOU DO?

- > Keep your software updated, including your browser, antivirus and operating system.
- > Buy from trusted sources. Check the ratings of individual sellers.
- > Restrict information and show caution with regard to social media.
- > Download apps only from official providers and always read the apps permissions.
- > Never open suspicious links or attachments received by email or text message.
- > When possible, do not associate your phone number with sensitive online accounts.
- > Do not reply to suspicious emails or engage over the phone with callers that request your personal information.
- > Set up your own PIN to restrict access to the SIM card. Do not share this PIN with anyone.
- > Frequently check your financial statements.



<DNS Abuse>

An Individual User Education Campaign



DNS OPERATORS' DECISION-MAKING GUIDE TO ADDRESS TECHNICAL ABUSE



REF: 20-108 | June 29, 2020

Acting at the DNS level can be justified to remediate technical/infrastructure abuse in order to protect the stability and security of the global infrastructure of the internet. DNS operators rely on a variety of internal and external resources to identify, evaluate and take action to remediate technical abuse¹. While establishing whether a domain is being used to perpetrate technical abuse tends to produce binary results (i.e. the domain is or is not engaged in technical abuse), care should nonetheless be taken to ensure that action at the DNS level to remediate said abuse is appropriate and proportionate.

A general approach to addressing technical abuse may be based upon the following steps:

- Identification or notification of the alleged technical abuse associated with the domain(s)
- Evaluation of scope of abuse
- Determination of the choice of appropriate and proportionate action
- Technical actions to ensure recourse and remediation

The table below lists a set of structuring questions that DNS Operators can use at each step to determine a course of action to address technical abuse on a voluntary basis.

| | Structuring Questions |
|---------------------------------|---|
| IDENTIFICATION AND NOTIFICATION | <ul style="list-style-type: none">• Is the domain within the DNS Operator's zone?• Does the notice allege technical abuse?• Does the notice contain all the necessary components² for identifying abuse and taking action, as appropriate?• Does the notice come from a court of applicable jurisdiction?• Does the notice come from a trusted, repeating or ad-hoc source?• Is there an agreement between the DNS Operator and this specific notifier? |
| EVALUATION OF ABUSE | <p>According to the type of technical abuse, what should DNS Operators take into consideration when evaluating alleged abuse, to ensure that the action taken is appropriate and proportionate?</p> <ul style="list-style-type: none">• Conduct own investigation (with help of 3rd parties if required) to |



<DNS Abuse>

An Individual User Education Campaign

