Global Good Practices

Practice: **Create a website for testing standards compliance**

#TestingTool

Proper use of the latest versions of Internet standards is a crucial element for a robust Internet infrastructure. There is generally no lack of standards, but it is important to stimulate, encourage and ensure stronger implementation. Is your Internet connection, website or e-mail up to date with the use of recognised security standards? Let us test it through a simple tool.

Related thematic areas:

Culture and skills

Standards

Of particular interest to:

CIVIL SOCIETY

PRIVATE SECTOR

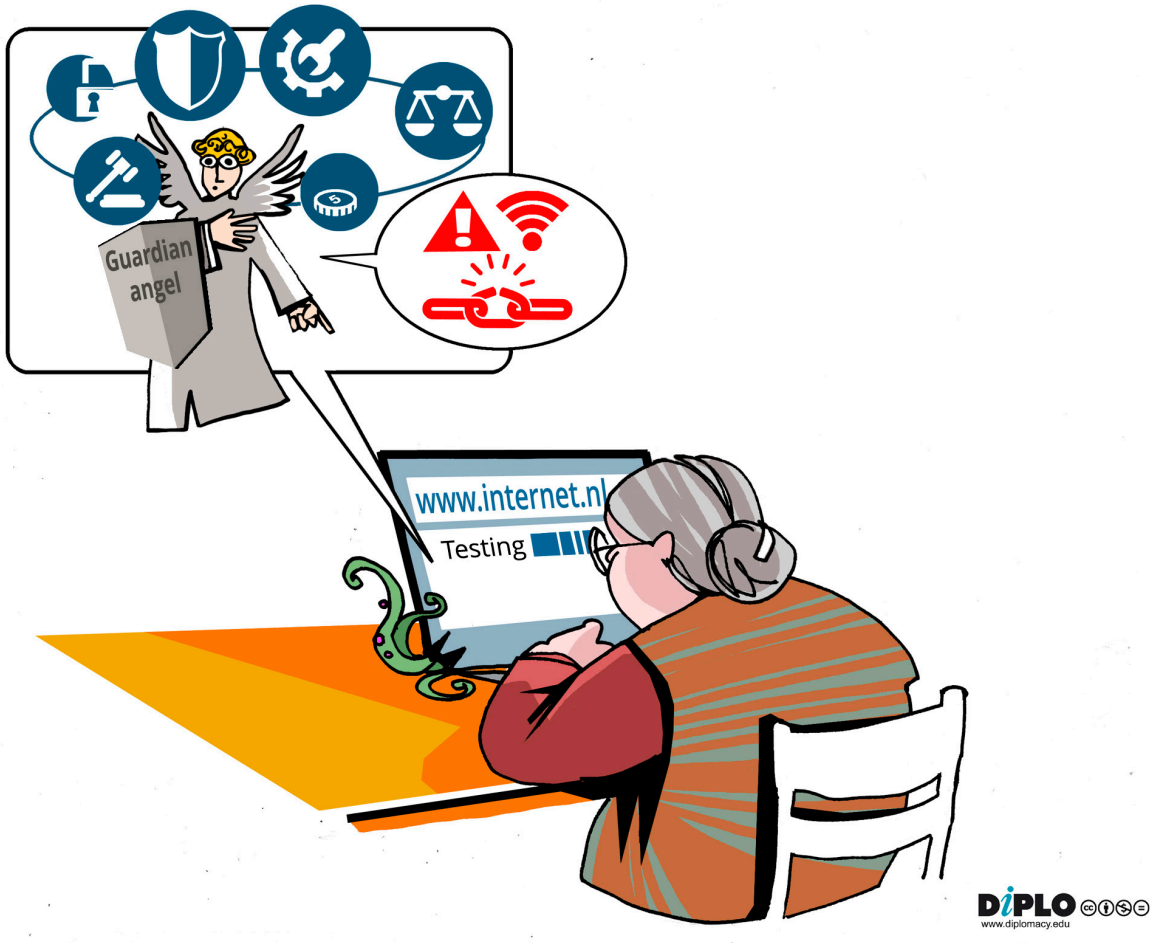
GOVERNMENT

Description

Fully implementing open standards for network services and functions can prevent abuse in various forms (e.g. phishing and botnet infection). Complete and correct standards compliance can diminish the impact of cybercrime and cyber-attacks and lead to more confidence and trust in the Internet, a prerequisite for innovation and fostering an online economy.

To enable and encourage individuals and organisations to use and comply with important standards, free public services for testing compliance with selected standards can be used. An online tool can be set up for the visitor who can – in real time – check any given domain name for security, whether used as a website or within an e-mail address. Users can also test the security of the Internet connection they are currently using when visiting the site. The online tool should provide documentation on the standards supported, as well as a communication channel and point of contact for any national initiative related to the implementation of standards.

While the tool is itself sufficient for technical communities able to identify gaps in standards implementations, the wider community – such as the corporate sector, organisations, and institutions – might need support along with the testing tool. Therefore, a more comprehensive approach involves a platform of organisations that provide support and discuss the implementation of standards (***#MSPlatform***).



Actors (or who this is for)

Targeted stakeholders who implement standards are in general all organisations that rely heavily on the Internet to communicate with users. Typically, these stakeholders are ISPs (access and e-mail), government authorities (e-governance), and the business sector (e-commerce). Yet anyone, including individuals, can use the test tool to check the level of implemented security standards in their own system.
Crucial stakeholders include technical organisations helping with expertise and knowledge, and civil society and governments promoting secure Internet use.

The big picture

The testing tool allows institutions to become more sensitive to respecting existing Internet standards, and thereby increases the overall health of the network.

On a broader scale, it also contributes to partnership building for providing support and coordinating efforts in implementing standards, by creating mechanisms and frameworks for cooperation and collaborative learning. In addition, it contributes at the organisational level by establishing more efficient processes and procedures for improving cybersecurity, especially integration into workflows.

The tool impacts capacity building in several ways:

- Encouraging mechanisms for cooperation on awareness-raising.
- Facilitating expert support and advice.
- Providing input for possible guidelines and good practices.
- Promoting technical standards and encouraging deployment.

Clear analysis of the test results includes easy suggestions for next steps, such as advice to contact your Internet provider to enable IPv6, etc. Complicated technical features are presented in an accessible format. As a result, a simple and intuitive online tool enables a wider circle of users to act independently, which is an important capacity.

Instructions

- Register a simple domain that people can remember.
- Prepare instructions in simple, non-technical language.
- Create a communication platform to promote your tool (***#MSPlatform***).
- Create a support team that will answer users' questions.
- Tailor the components of the web to your national context.

Adaptation to national/regional needs can be arranged based on the existing tool. Different implementations can be envisaged, from simply adding a different language version, to designing a new variant under a different domain, depending on arrangements for the use of source code.

Some possible challenges in replication of this practice include:

- Lack of awareness, which could be mitigated through awareness-raising campaigns (using simple terminology, potentially showcasing metrics).
- Language barriers, which may be addressed through the translation of materials and developing local content.

Timing

Development of a website and a testing tool can run in parallel with setting up a platform (***#MSPlatform***), provided there is a small group of initiators/first movers willing to invest in or put effort to it. The advantage is that the platform, once established, can be operational immediately.

Building a website or tool will take at least a few months (in the case of a straightforward duplicated/translated version of existing practices); while it could take from six to twelve months (if specific needs and adaptations are required).

The lifetime/goals of the platform determine how, and how long, the tools are used. Regardless of how the tools are developed, there will be a continuous need for improvement and further development during their lifetime. New versions should be anticipated as a consequence of testing improvement, new functions, user feedback, bugs, etc.

Example

The GFCE Internet Infrastructure Initiative promotes an up-to-date, open, secure, and future-proof Internet by helping stakeholders to implement open standards for secure e-mail and websurfing, and expanding the Internet address space.

The testing tool made available for the GFCE Internet Infrastructure Initiative, available at www.internet.nl, contributes to the implementation of standards through a variety of uses and mechanisms, for example stick, carrot, exposure, transparency, peer pressure:

- For technicians to improve their employer's ICT.
- For government to generate metrics on the development of security in their agencies and act on it.
- For the press to expose vulnerabilities, sometimes with political impact (the Dutch Minister of the Interior promised to fix the poor security of municipal e-mail across the country).
- For umbrella organisations to test their members.
- For best performing users to be named (hall of fame with 100% score).

The website/test tool www.internet.nl is available in English, Dutch, and Polish and can be used in any country, for any domain, and any Internet connection. Its universality makes it instantly suitable for any national/regional use.

Statistics on the use of the testing tool indicate an increasing trend, while all requests for support, expressed via e-mail to the Dutch community behind this testing tool, were successfully resolved with the parties likely implementing necessary security standards. The tool revealed a lack of security standards in some municipalities, and in response the Minister in charge promised to increase the adoption of standards. Other institutions and communities, such as APNIC, are moving towards implementing the testing tool and web platform.

Source, support, and mentoring

Internet Infrastructure Initiative at the GFCE website: https://www.thegfce.com/initiatives/i/internet-infrastructure-initiative

Internet testing tool: https://www.internet.nl

Contact point:
Thomas de Haan (T.S.M.dehaan@minez.nl)