Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

2017

National study

French cyber security

Protecting
digital identity
by email

Ensuring
confidential
browsing

By Yuksel Aydin
Economic and Finance Ministries

Foreword

By Yann Bonnet
French Digital Council

5th EUROPEAN CYBER SECURITY MONTH
Anniversary

Foreword

Digital technology is an integral part of citizens' daily lives, our business activities and government operations. With the scaling up of the Internet of things, the development of algorithms, big data and new business models, with the dawning of a "world of calculations" – to borrow a phrase coined by Dominique Cardon – and with our messages, emails and traces going beyond national borders, the security and protection of data and exchanges is becoming a crucial issue.

A key point is that having everybody connected implies that everybody is also responsible for security in the digital environment. This extends to citizens, non-profit organisations, businesses and government departments. As a result, the digital literacy of citizens and civil servants is a contingent prerequisite for this security. The government will have to conduct a wide-reaching awareness-raising campaign for the target audiences.

As regards the challenges raised, the French Internet is still somewhat lagging behind. For instance, the stakeholders do not yet make adequate use of data encryption, particularly HTTPS. For citizens, this is a key factor for building confidence in the rollout of digital technology, as it allows for secure communications and mitigates the risk of the theft of personal or bank data. Every day, encryption protects billions of people against a countless number of threats. For businesses, it is the best way to parry industrial espionage – it is vital for protecting intangible assets from outside interference. For the government, it is one of the preconditions for its sovereignty.

This study couldn't come at a better time!

Yann Bonnet

Secretary General of the French Digital Council

National study on French cyber security

PROTECTING DIGITAL IDENTITY BY EMAIL

ENSURING CONFIDENTIAL BROWSING

2017

By Yuksel Aydin

Ministerial Deputy Head of Information Systems Security

Economic and Finance Ministries

Digital exchanges are made secure using a number of practices and technologies including HTTPS and email authentication.

HTTPS provides a secure communication protocol for website browsing. It ensures the confidentiality and integrity of information exchanged between the Internet user and the website. As a result, the content of exchanges cannot be either intercepted or modified "onthe-fly" by third parties listening in on the networks.

By using the HTTPS protocol, businesses assure customers that the information exchanged remains confidential (passwords, pages consulted, bank data, etc.)

Email authentication relies on the SPF, DKIM and DMARC technical protocols. As some of the information provided by these standards is in the public domain, they:

- provide assurance that an email allegedly originating from a sender was actually sent by that sender
- block emails from senders that do not have the pre-declared signature

Email authentication protects businesses' digital identity and provides their customers with heightened protection against the risks of identity theft such as phishing[1]

Some of the websites operating on the French Internet comply with these protocols but the overall picture is far from clear. First and foremost, an assessment needed to be carried out to analyse the current situation and to make a positive contribution to the development of the digital environment.

This study provides an overview of the French Internet in 2017 in respect of HTTPS and email authentication.

I Context

1.1 Scope

The assessment was carried out between 1 July and 31 August 2017 using two lists:

- The 500 websites most-visited by French Internet users[2]
- All .fr domain names (slightly over three million)[3]

These lists provided the basis for this study but the results for all the .fr domain names are only fully relevant if they are put in perspective with those of the web giants.

As a result, irrespective of where the servers are located, the French digital environment means the digital area actually used by the French population via the top 500 websites, on one hand, and the digital area comprised of .fr domain names, on the other.

1.2 Technical conditions

1.2.1 Domain name servers

Domain name resolution[4] and querying SPF, DKIM and DMARC records were carried out using servers with the IP address 8.8.8.8.[5]

[1] For information on phishing:

- Directorate General for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF): https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishinghameconnage-ou-filoutage
- Ministry of the Interior: https://www.police-nationale.interieur.gouv.fr/Actualites/L-actu-police/Faceau-phishing-soyez-vigilants
- French Data Protection Authority (CNIL): https://www.cnil.fr/fr/cnil-direct/question/375

[2] Alexa list (an amazon.com company): https://www.alexa.com/topsites/countries/FR (not limited to .fr websites)

[3] AFNIC, the .fr domain registry, provides free access to the list of registered domain names: https://opendata.afnic.fr/fr/produits-et-services/le-fr/opendata-fr.html

[4] How DNS works: https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml.

1.2.2 Calculation method

The calculation method differed according to the type of analysis:

- **SPF, DMARC**

DKIM was excluded from the scope of this study as the information provided by this record is a combination of the DNS record and the signature contained in an email. Automated verification is technically impossible unless one actually has an email in one's possession.

The presence of SPF and DMARC markers was checked using all the domain names. Searches for websites associated with the domain name were not carried out beforehand as certain domain names are only used to send emails.

- **HTTP/S**

The analysis was conducted on four versions of websites in two different categories:

- http:// and http://www. versions
- https:// and https://www. versions

A category was allocated a result when the latter was positive for a version with or without "www.".

The results used were those that returned an HTTP 200 status[6] and those located on the same queried domain name (without external forwarding).

The examination of HTTP/S headers was carried out on all domain names associated with a website except those configured with a response header to prevent robot indexing.[7]

HTTP/S pages were consulted for all domain names associated with a website except those whose HTTPS header of the robots.txt[8] file blocked search indexing, or when such exclusion was contained in the page itself.[9]

Lastly, and specifically for HTTPS, the validity of the certificate was checked. When there was an HTTPS version of a website, it was only included if it was valid.

[5] Google Public DNS : https://developers.google.com/speed/public-dns/

[6] For information on http statuses: https://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

[7] Noindex in the HTTP header: "X-Robots-Tag: noindex". For further information: https://developers.google.com/search/reference/robots_meta_tag#using-the-x-robots-tag-http-header

[8] Robots.txt is a file at the root of websites.

- Here are two examples: https://www.economie.gouv.fr/robots.txt or https://www.google.com/robots.txt

- For the purposes of this study, we followed the robots.txt directives in respect of the Wget utility, even though this command program was not used.

[9] Noindex contained in a web page: https://support.google.com/webmasters/answer/93710?hl=fr

The result of factoring in these various criteria caused the studied volume to differ according to the examination carried out. This means that the volume is specified for each test.

II Fighting email identity theft: SPF and DMARC

2.1 Overview of SPF, DKIM and DMARC

Ill-intentioned persons use email as a means of stealing a third party's identity to make a current or potential customer share confidential information (password, bank details, etc.), pay an amount or install malware on the Internet user's computer.

Such actions, which are quite easy to implement, directly compromise the digital and/or financial interests of both businesses and consumers.

Three techniques, that represent a form of email signature, can be used to verify the sender's actual identity:

- Sender Policy Framework[1] (SPF) links the email sending address and the domain name of the SMTP envelope
- DomainKeys Identified Mail[2] (DKIM) validates the message's integrity and that of its sender's domain on the message itself
- Domain-based Message Authentication, Reporting and Conformance[3] (DMARC) informs third parties of the action to be taken when an email sent in their name is subject to a DMARC record but is not authenticated against SPF and DKIM or when the envelope address and that of the message do not match

2.2 SPF and DMARC rollout

Out of the 500 most-popular websites with French users, three-quarters have introduced the SPF protocol and one-third the DMARC protocol.

An analysis of all the .fr domain names flags up a fairly high level for SPF (1/3) but virtually no use of DMARC (<1%).

[1] https://tools.ietf.org/html/rfc7208

[2] https://tools.ietf.org/html/rfc6376

[3] https://tools.ietf.org/html/rfc7489

Table 1 – Assessment of SPF and DMARC in the French digital environment

	MOST-POPULAR – FRANCE	.FR
SPF	74%	34.45%
DMARC	29.6%	0.89%
Studied volume	500 domain names	3,141,369 domain names

In respect of DMARC, the holder may ask the third party checking this signature to carry out an action:[4]

- None: no filter is applied, data report request only
- Quarantine: quarantining, data report request
- Reject: the suspicious email is blocked, data report request

Table 2 – Assessment of DMARC actions

DMARC	MOST-POPULAR – FRANCE	.FR
None	47.30%	76.65%
Quarantine	12.84%	6.01%
Reject	39.19%	12.77%
Studied volume	148	27,962

An examination of DMARC record actions shows that, almost 50% of the time, the protocol is only used for reporting.

2.3 Protocol comparison using the domain name's creation date

We look at whether SPF and DMARC protocols had been implemented based on the year that a domain name had been created.

Table 3 – Existence of SPF and DMARC protocols based on the year of domain name creation

.FR (year of creation)	2000	2005	2010	2015

[4] For information on DMARC actions: https://dmarc.org/overview/

SPF	30.64%	30.23%	30.24%	30.34%
DMARC	1.17%	1.07%	0.73%	0.80%
Volume studied	20,682	53,281	194,431	341,680

These results reveal no positive or negative change based on the year of domain name creation.

Email messaging service providers and domain name providers could stimulate deployment of SPF and DMARC protocols

2.4 Comparison between France and the US

Data from France should be compared with that from a similar digital area, such as the US. Regarding this, the Federal Trade Commission has issued a white paper on the implementation of the SPF and DMARC protocols.[14]

Table 3 – Use of SPF and DMARC in France and the United States

	MOST POPULAR – FRANCE August 2017	MOST POPULAR –USA July 2016
SPF	74%	85.94%
DMARC	29.6%	29.52%
Volume studied	500	569

France and the US show similar levels of use of DMARC.

Use of SPF is high in both zones, with the TOP USA sites the higher of the two.

An assessment of DMARC's actions, however, shows that there is a higher spam rejection rate in the French digital area.

Table 4 – DMARC actions in France and the United States

DMARC	MOST POPULAR – FRANCE August 2017	MOST POPULAR – USA July 2016
None	47.30%	68.45%[15]
Quarantine	12.84%	5.95%
Reject	39.19%	25.60%

Volume studied	148	168

[14] Paper issued in March 2017:

- https://www.ftc.gov/system/files/documents/reports/businesses-can-help-stop-phishing-protect-theirbrands-using-email-authentication-ftc-staff/email_authentication_staff_perspective.pdf

[15] The percentages given in the FTC paper have been recalculated to arrive at comparisons, all other things being equal.

Conclusion:

- **The SPF protocol is very widely used for major websites. Its rollout rate for the entire .fr domain is at a respectable level.**

- **The DMARC protocol is deployed on one-third of major websites, but its use is negligible on smaller sites.**

Dedicated public/private efforts are needed to ensure large-scale rollout of these protocols.

III HTTPS: Making it safer to surf the web

3.1 Introduction to HTTPS

When Internet users search the web, they use networks over which they have no control. Information sent over these networks may be intercepted or modified “on-the-fly”.

To ensure that exchanges are kept confidential, a standard, known as HTTPS, was developed based on encryption of the communication between the browser and the server.

Websites that offer this level of security have URLs that begin with https://.[5]

This prefix allows a user to connect to an account without worrying that a third party will be able to intercept his or her login details. Users should not create an account or connect to an account on a site whose URL begins with http://, but rather should only do so when it begins with https://.

[5] In 2016, the use of HTTPS was made mandatory for economic and financial ministry websites (e.g. https://www.economie.gouv.fr, https://www.entreprises.gouv.fr, https://www.impots.gouv.fr, https://pro.douane.gouv.fr/, etc.).

The Firefox[6] and Chrome[7] browsers currently warn users about the dangers of online forms on non-secure websites (http://), and soon the same browsers will indicate non-HTTPS sites. As a result, to prevent being sidelined in a very competitive digital arena, Internet sites should only be available in https://.

Global awareness of the need for confidentiality in exchanges began in 2012, driven by major Internet stakeholders,[19] who published announcements like the following:

- EFF: https://www.eff.org/encrypt-the-web
- Twitter: https://blog.twitter.com/official/en_us/a/2012/securing-your-twitterexperience-with-https.html
- Facebook: https://www.facebook.com/notes/facebook-engineering/securebrowsing-by-default/10151590414803920/
- Google: https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html
- Wikipedia: https://blog.wikimedia.org/2015/06/12/securing-wikimedia-sites-withhttps/
- Bing: https://blogs.bing.com/webmaster/2015/06/15/bing-moving-to-encryptsearch-traffic-by-default/

3.2 Implementing the HTTPS protocol in the French digital environment

The results show that protecting Internet connections is a key expectation of French Internet users:

➢ More than half of the major sites provide an HTTPS version

Table 5 – Assessment of HTTPS in the French digital area

	MOST POPULAR –FRANCE	.FR
HTTP	38.66%	76.87%
HTTPS	61.34%	23.13%
Volume studied	432 websites	1,932,160 websites

Although more than 50% of major French Internet sites are available in an HTTPS version, less than one-quarter of .fr domain sites offer a secure connection.

[6] https://blog.mozilla.org/security/2017/01/20/communicating-the-dangers-of-non-secure-http/

[7] https://blog.chromium.org/2017/04/next-steps-toward-more-connection.html

There are three salient points to be made about these results:

- Some websites are available in both HTTP and HTTPS, but the HTTPS configuration is incomplete[8] (invalid certificate, redirection to the HTTP version, etc.)
- Some HTTP sites contain an authentication page that generates an exchange of private and unprotected data
- Some HTTPS sites contain an incorrectly configured authentication form (POST in HTTP), thus invalidating the security measures taken

3.3 Assessment of supplementary security data

When an Internet user connects to a website, background exchanges of data take place between the browser and the server. Some of this data is used to make the connection more secure.

The supplementary security data is invisible to the user. The protocols used for the purpose of this study (solely with respect to HTTPS sites) include:

- HSTS,[9] which allows a web server to instruct a web browser to use a secure connection
- HttpOnly,[10] which puts cookies out of reach of scripting languages
- SecureFlag,[11] which helps keep cookies confidential
- XSS-protection,[12] which activates the filters built into certain browsers
- Same Origin Policy,[13] which prevents third-party sites from displaying a website

The results of the study reveal a piecemeal implementation of these various protocols.

Table 6 – Supplementary security data for HTTPS websites

HTTPS	Most popular – France	.FR
HSTS	28.70%	8.02%
HttpOnly and secure cookies	9.81%	3.87%
XSS	22.64%	2.64%
Same origin	34.34%	3.72%
Volume studied	265	446,870

[8] The sites were not included in the results.
[9] https://fr.wikipedia.org/wiki/HTTP_Strict_Transport_Security
[10] https://www.owasp.org/index.php/HttpOnly
[11] https://www.owasp.org/index.php/SecureFlag
[12] https://developer.mozilla.org/fr/docs/Web/HTTP/Headers/X-XSS-Protection
[13] https://www.w3.org/Security/wiki/Same_Origin_Policy

It should be pointed out that, out of the most popular HTTPS French sites, only six domain names incorporated all of the supplementary security data, and only 799 for the entire .fr domain (HTTPS).

3.4 HTTPS implementation based on year of creation

HTTPS implementation is likely to vary based on the year that a domain name was created, as training for developers has changed over time.

Table 7 – HTTPS implementation based on year of creation

.FR (year of creation)	2000	2005	2010	2015
HTTPS	20.16%	18.67%	24.78%	24.88%
Volume studied	12,146	29,486	109,521	218,418

This shows that domain names created in the early 2000s are less likely to have an HTTPS version than those created starting in 2010.

3.5 International implementation of HTTPS

Thanks to a 2017 study[26] of the top 1 million websites around the world, we can compare the results from the .fr domain with the global digital environment.

Table 8 – Comparison of HTTPS implementation in France and worldwide

	.FR	MOST POPULAR – WORLD[27]
HTTPS	23.13%	45.80%
Volume studied	1,932,160	1 million

The .fr domain lags behind in comparison with the top 1 million websites around the world.

On a positive note, the study of websites worldwide reveals a significant and speedy upswing in HTTPS implementation in a short period of time:

Table 9 – Global trend in HTTPS

	April 2016	October 2016	June 2017
HTTPS	29.64%	33.57%	45.80%

Volume studied	1 million	1 million	1 million

Implementation of HTTPS in the .fr domain is thus below the worldwide level observed 18 months ago. France must join this global trend by implementing the HTTPS protocol systematically on every new Internet site, and deploying it on legacy sites, in an order determined by a risk analysis.[28]

[26] Study carried out in 2016, and updated in 2017: https://blog.mozilla.org/security/2017/06/28/analysis-alexatop-1m-sites/

[27] List freely available on Alexa: https://s3.amazonaws.com/alexa-static/top-1m.csv.zip

[28]

About risk management:

- https://www.iso.org/fr/iso-31000-risk-management.html
- https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-desecurite/ (EBIOS method)

To conclude:

- **The results of the study reveal that protecting users' digital identities, combating spam and keeping exchanges confidential are a priority for the 500 most-popular websites with French users.**

- **Comparatively speaking, the French digital environment is robust, despite a noticeable lag in implementing HTTPS, due to a sustained global trend in which sites that provide a secure connection to customers are to be distinguished from those who do not bother with their customers' security needs.**

- **In the interests of both consumers and businesses, secure messaging and HTTPS protocols should be a tangible and measurable priority in 2008 for the French digital area. Public policy can provide impetus to coordinate the actions of digital economy stakeholders.**

To learn more

Combating email identity theft:

- FTC paper cited above: https://www.ftc.gov/system/files/documents/reports/businesses-can-help-stopphishing-protect-their-brands-using-email-authentication-ftcstaff/email_authentication_staff_perspective.pdf

- Volumetric study: https://dmarc.org/presentations/CMD-2016-Jones--for-publication-v3.pdf

- Implementation by the British government: https://gdstechnology.blog.gov.uk/2016/06/28/updating-our-securityguidelines-for-digital-services/

- ANSSI recommendations: https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

- German governmental recommendations (BSI): https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSICS_098.pdf?__blob=publicationFile

- Recommendations by US governmental agencies: https://www.justice.gov/criminal-ccips/file/872771/download

Strengthening secure web browsing:

- Study by the Mozilla (Security) Observatory cited above: https://pokeinthe.io/2017/06/13/state-of-security-alexa-top-one-million-201706/

- A study along the same lines using a methodology specific to its author: https://scotthelme.co.uk/alexa-top-1-million-analysis-aug-2017/ https://www.usenix.org/system/files/conference/usenixsecurity17/sec17felt.pdf http://paulsec.github.io/blog/2014/05/13/http-security-headers-on-top-10kalexa-websites/

- Site measuring HTTPS implementation on US government websites: https://pulse.cio.gov/https/domains/

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

5th
EUROPEAN
CYBER
SECURITY
MONTH
Anniversary