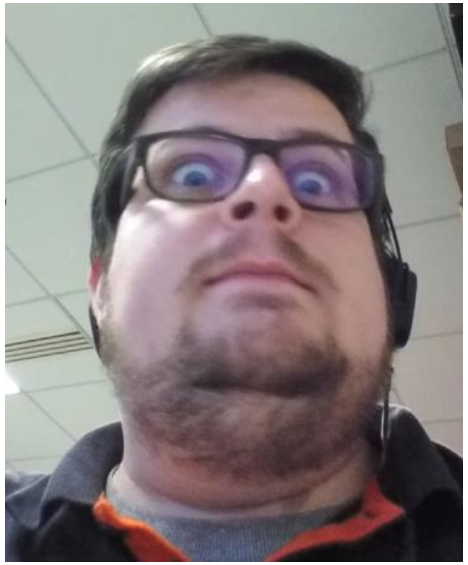
IDNs and its possible bad uses

fladnaG (Max) French independent Pentester/Trainer/Sysadmin BalCCon 2k22

@fladna9 on Twitter pro@fladnag.net

Disclaimer

- Don’t have the dumbs like me.
- What will be presented here may be considered illegal in many countries, and may send you to jail.
- This is not a point-and-shame presentation.
  - This technique is not prevalent yet, but seen more and more each year.
  - The goal here is to demonstrate it can happen to anybody.



Plan

- Quick introduction to Domain Names
- What are IDNs?
  - Punycode?
- Let’s play a game >:)
- Attacks in the wild
  - Some historical examples
  - My IDNs homograph attacks
- How to protect ourselves?

Quick introduction to Domain Names

Once upon a time…

RFC 608 – Jan 1974
HOST NAMES ON-LINE

`<basic-part>.<attribute-item><eol>`

- **`<basic-part>`** is up to 48 chars, **`/^[A-Z][A-Z0-9\-]+[A-Z0-9]$/i`**
- `<attribute-item>`

SERVER, USER, TIP, UNKNOWN

- HOSTS.TXT file shared via FTP…

RFC 882 + 883 – Nov 1983
DOMAIN NAMES

- Concept and facilities
  Explaining the rationale behind DNS.
- Implementation and specifications.
  Technical specifications.

> *Name servers and resolvers must compare labels in a case-insensitive manner, i.e. A=a, and hence **all character strings must be ASCII** with zero parity*
> -- RFC 883

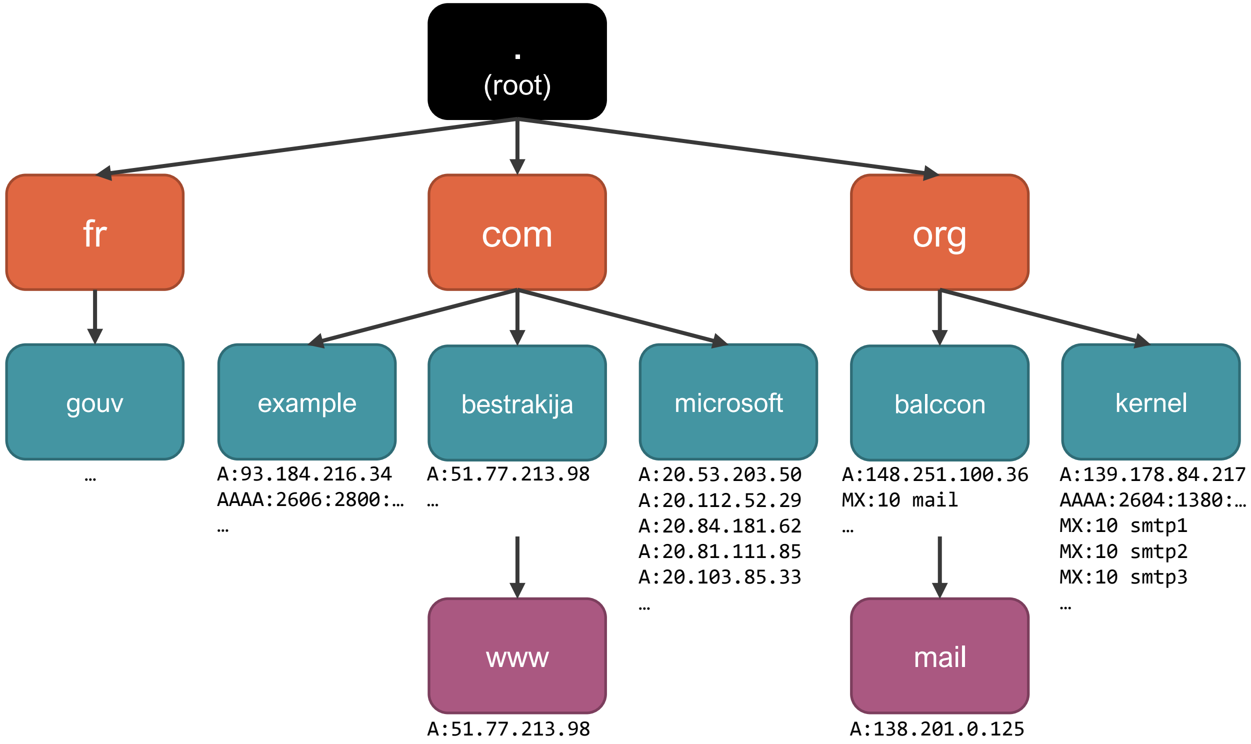
RFC 1034 + 1035 – Nov 1987
DOMAIN NAMES

- Update from RFC882 and RFC883.
- The basis of what we call DNS today.
- Many features where broght in since then… we'll see one or two.

DNS

Domain Names System

- Mainly translate domain names into IP addresses (A for IPv4, AAAA for IPv6), but also for mails (MX), configuration (DKIM, DMARC, SPF, SOA), text (TXT), etc. These are called records organized as a tree-based search and consultation.
- `www.bestrakija.com` (read from right to left) → Fully Qualified Domain Name (FQDN)
  - `COM` is a label, the TLD (Top Level Domain).
  - `BESTRAKIJA` is a label, is a domain.
  - `WWW` is a label, a sub domain.
- Labels are ASCII encoded chars as seen before.
- Distributed protocol via recursive servers UDP port 53.



DNS

Vocabulary

- Registry
  - Company/fundation/administration governing the TLD.
- Registrar
  - Company where end users can register domain names to the Registry as « first asked first served » policy. It’s like a Registry proxy, as many Registries don’t allow direct domain reservation.
- Registrant
  - Individual/company/fundation/administration registering a Domain Name through a Registrar to the Registry.

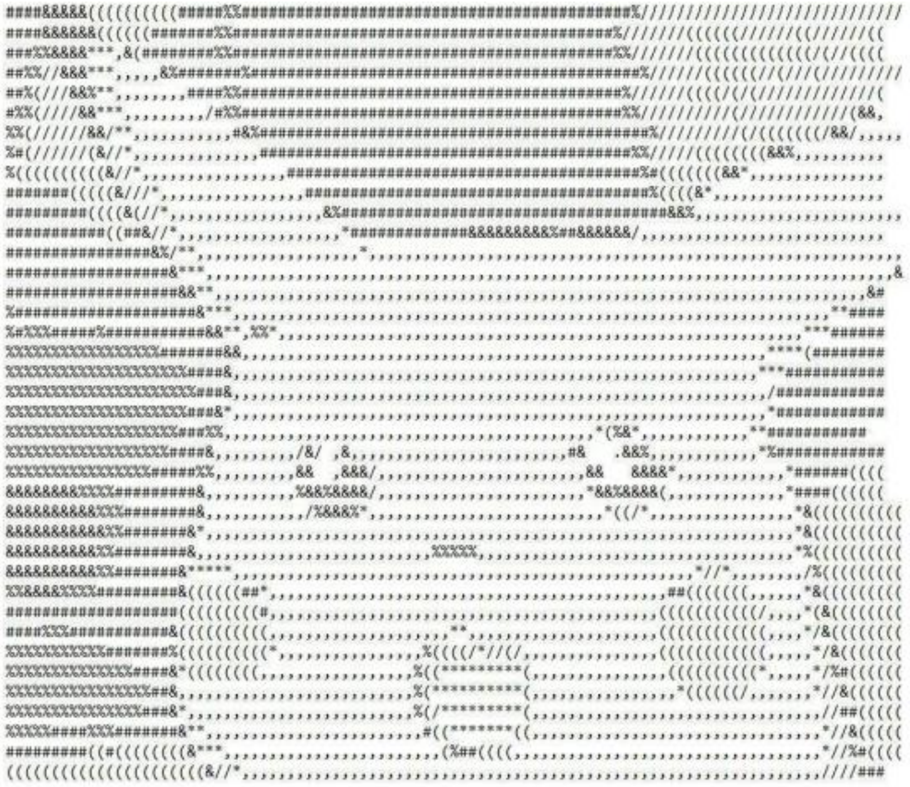
So what?

Domain Names are old but it works

- At least, it works well for ASCII-based languages…
- But the problem is: ARPANET became INTERNET, with many countries and languages.
  - Except for English-speaking countries, ASCII is no longer enough to support all the planet.

- So how to satisfy everybody and every language, allowing regional chars in domain names without breaking everything?

What are Internationalized Domain Names?



Once upon a time (again)…

« Houston, we have a problem »

- March 1998: Singapore University
  Aware of the all-ASCII problem, working on it.
- July 1998: APNIC creates a working group, called iDNS.
- 1999: tests done on `.cn` domains with Chinese traditional characters.
- 2000: IETF and ICANN get involved, IDN working group created.

RFC 3454, 3490, 3491, 3492 – in 2003
Internationalized Domain Names

- Encoding function and syntax.
  Called IDN2003
- June 2003: ICANN publishes its IDN guidelines for Registries.
- Updated in 2008.
  Called IDN2008

What are IDNs?

How to make it work?

- Without changing current Domain Names systems, requiring ASCII [A-Za-z0-9\-]…
- If only there was a **`UNI`**versal way to en**`CODE`** all characters from all characters from all languages in the world…

Punycode

What is punycode?

Standardized in RFC3492, Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Application (IDNA)

- Thanks to bootstring, an algorithm designed to encode Unicode characters in ASCII, we can name a domain with Unicode.
- Bootstrap is
  - Simple, efficient and quick,
  - Unique and Reversible,
    ```
    ASCII = P(UNICODE)
    UNICODE = P-1(ASCII)
    ```
  - Readable as ASCII and UNICODE (next slide).

Punyencoding with bootstrap simplified

xn--<ASCII .. -><punycode>

- IDN punycoded domains will start with xn--
- Then ASCII part
  - If there is one, ended with –
  - If not, no ending dash
- Then punycode
  - Encoding is rather easy, for each non-ASCII char,
    - i = position
    - n = UNICODE numeric – 127
    - ASCII encoded result = EnhancedBase36(i*n)
  - Decoding is a finite state machine
    - Not going to talk about it, no more math today

How it looks?

UNICODE	ASCII Punycoded
Aerodrom-Nikola-Tesla-Beograd	Aerodrom-Nikola-Tesla-Beograd
Аеродром-Никола-Тесла-Београд	xn------5cdbbbhsdiced2b6ardlvrbfj5acsu1a
Aéroport-Nikola-Tesla-Belgrade	xn--aroport-nikola-tesla-belgrade-buc
🏴‍☠️	xn--h4hx200o
日本語。ＪＰ	xn--wgv71a119e.jp

Top level domain IDN support

.com registry (Verisign, inc., commercial)

- Many Unicode sub-charsets allowed, but you have to choose an alphabet
  - Latin, Japanese, Vietnamese, Chinese, Cyrillic, etc.
  - For example, cannot combine ASCII with Cyrillic…
  - … but sometimes with exceptions, including strange chars.
- Many documents, hard to search and read through.

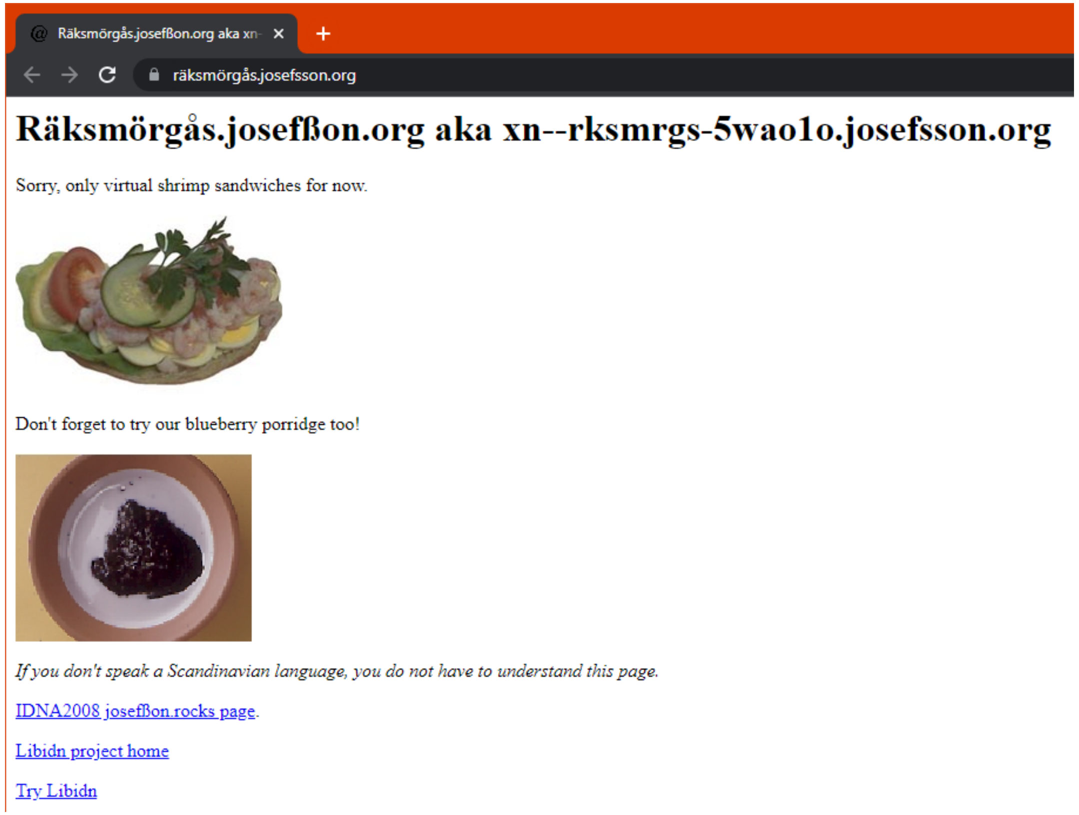
https://www.verisign.com/en_US/channel-resources/domain-registry-products/idn/idn-policy/registration-rules/index.xhtml

.fr registry (AFNIC, fundation)

- Charset defined clearly in Naming Rules document
  - `a, à, á, â, ã, ä, å, æ, b, c, ç, d, e, è, é, ê, ë, f, g, h, i, ì, í, î, ï, j, k, l, m, n, ñ, o, ò, ó, ô, õ, ö, œ, p, q, r, s, t, u, ù, ú, û, ü, v, w, x, y, ý, ÿ, z, ß, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, -`
  - Very restricted, to french chars + historical local languages (corse, breton, alsacien, lorrain, gascon, provençal…)

Web browser support

Google® Chrome® (💩)



Räksmörgås.josefßon.org aka xn--rksmrgs-5wao1o.josefsson.org

Sorry, only virtual shrimp sandwiches for now.

Don't forget to try our blueberry porridge too!

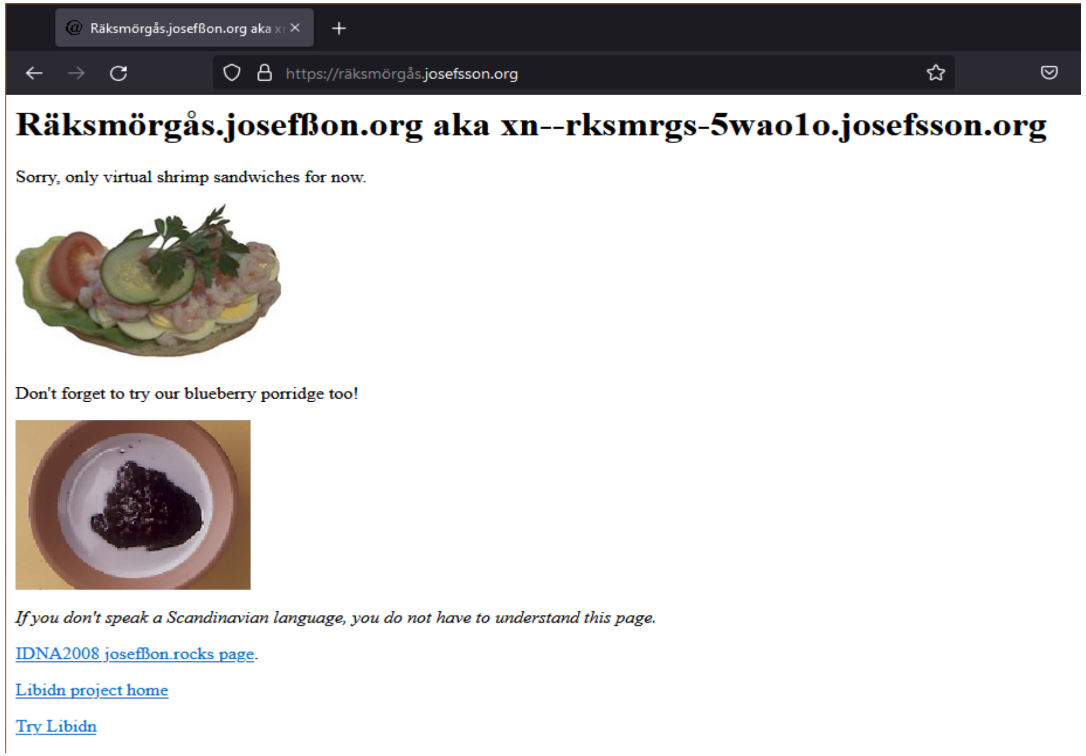
If you don't speak a Scandinavian language, you do not have to understand this page.

IDNA2008 josefßon.rocks page.

Libidn project home

Try Libidn

Mozilla Firefox (💖)


Räksmörgås.josefßon.org aka x
https://räksmörgås.josefsson.org

Räksmörgås.josefßon.org aka xn--rksmrgs-5wao1o.josefsson.org

Sorry, only virtual shrimp sandwiches for now.

Don't forget to try our blueberry porridge too!

If you don't speak a Scandinavian language, you do not have to understand this page.

IDNA2008 josefßon.rocks page.

Libidn project home

Try Libidn

Let’s play a game >:)

Rules

Guess game

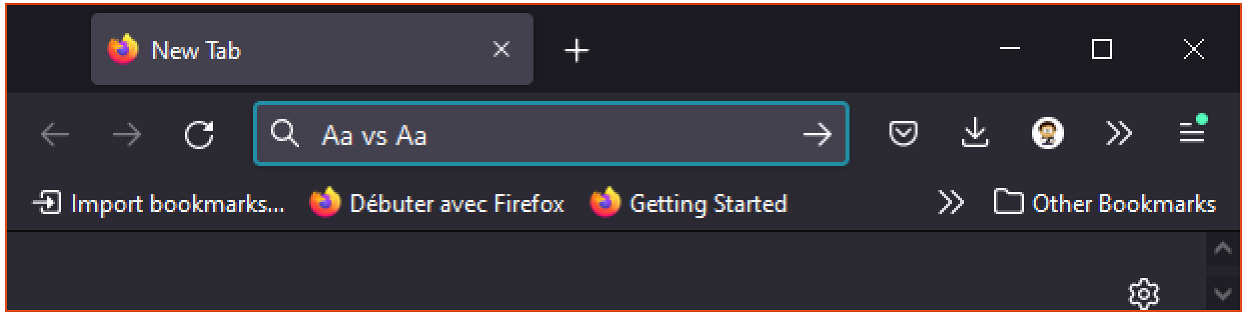
- 2 chars. 2 types.
- Guess which is which.
- Ready?

For your information, nothing to win, ok? Except maybe a beer.

Round 1/5

Cyrillic (UNICODE) versus Latin (ASCII)
Which is which?

Aa vs Aa

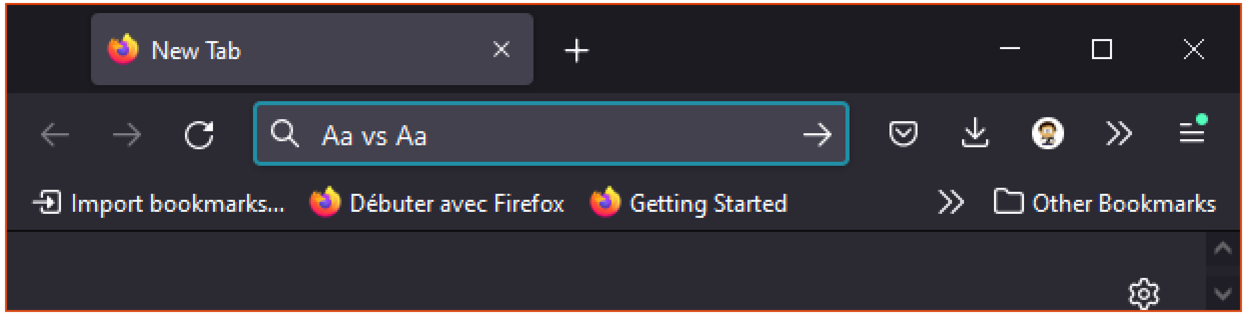


Aa vs Aa

Round 1/5 - Answer

Cyrillic (UNICODE) versus Latin (ASCII)

Aa$_{\text{scii}}$ vs Aa$_{\text{cyrillic}}$

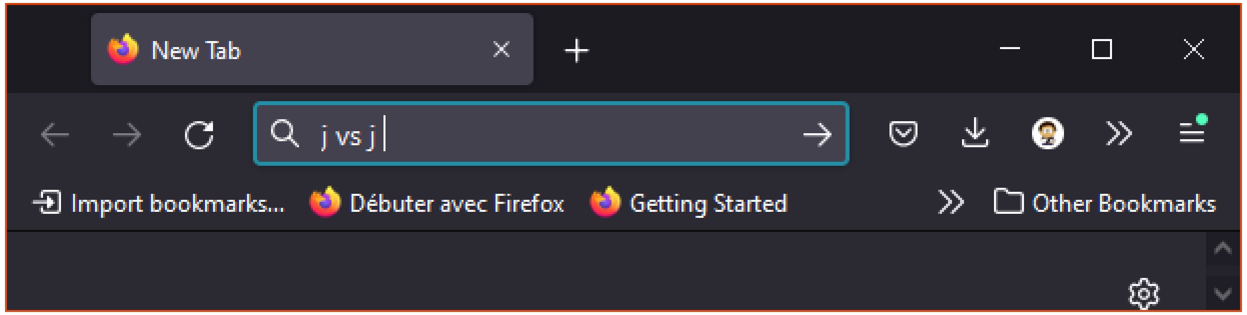


Aa vs Aa

Round 2/5

Greek (UNICODE) versus Latin (ASCII)
Which is which?

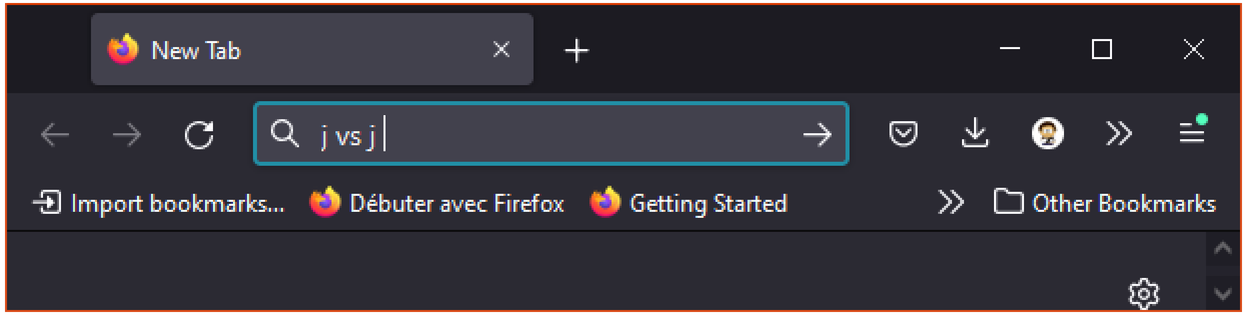
j vs j



Round 2/5 - Answer

Greek (UNICODE) versus Latin (ASCII)

j (ASCII) VS ϳ (greek)

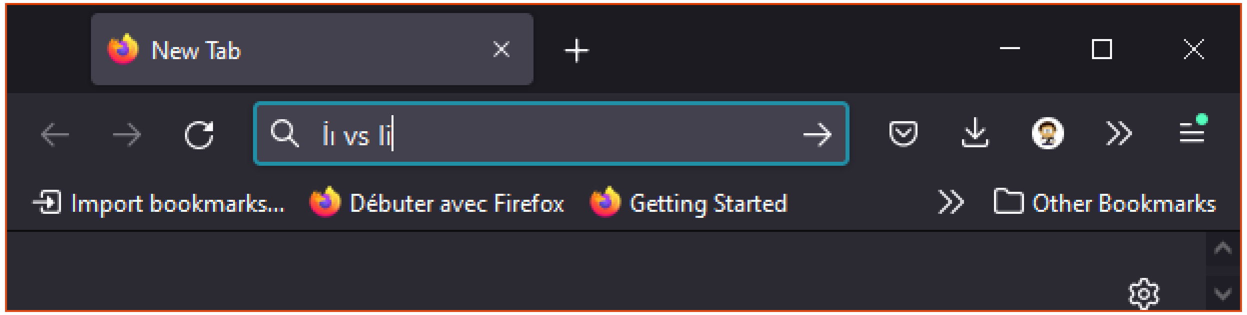


j vs ϳ

Round 3/5

Latin Extended (UNICODE) versus Latin (ASCII)
Which is which?

İı vs Ii

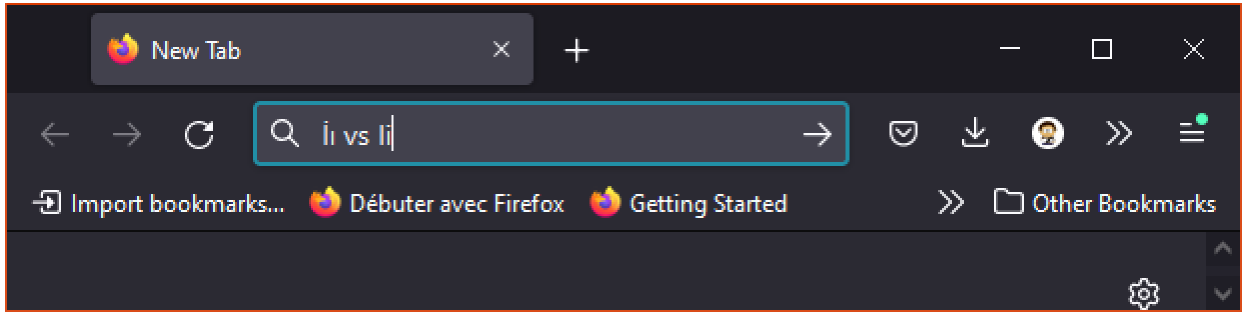


İı vs Ii

Round 3/5 - Answer

Latin Extended (UNICODE) versus Latin (ASCII)

İı (latin extended) vs li (ASCII)

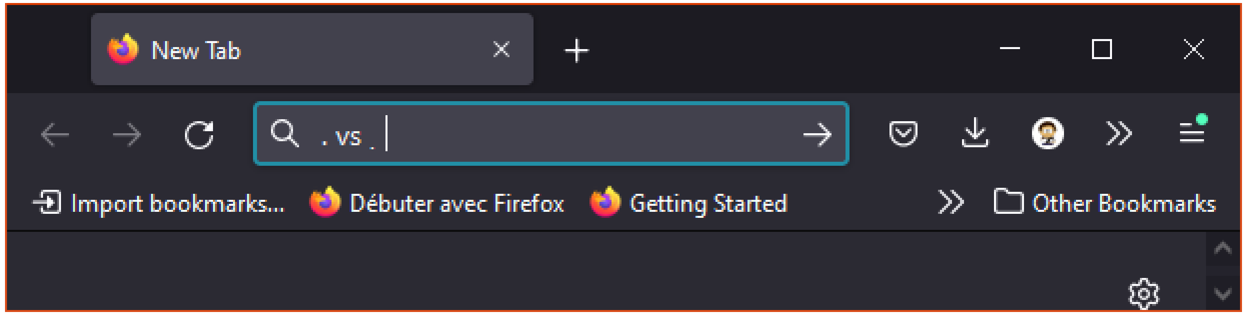


İı vs li

Round 4/5

Diacritic (UNICODE) versus Latin (ASCII)
Which is which?

. VS .

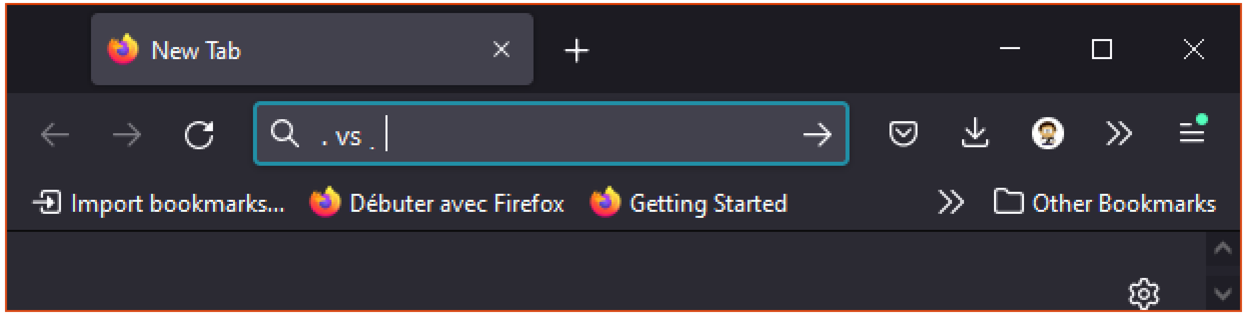


. vs .

Round 4/5 - Answer

Diacritic (UNICODE) versus Latin (ASCII)

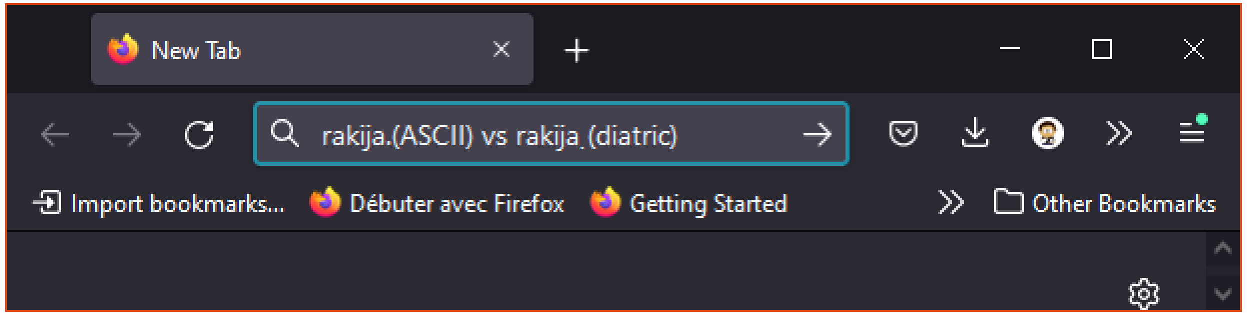
. (ASCII) VS ◌̣ (diacritic)



Round 4/5 - Answer

Diacritic (UNICODE) versus Latin (ASCII)
Diacritic is an accent, a combining character.

rakija.(ASCII) VS rakijạ (diacritic)

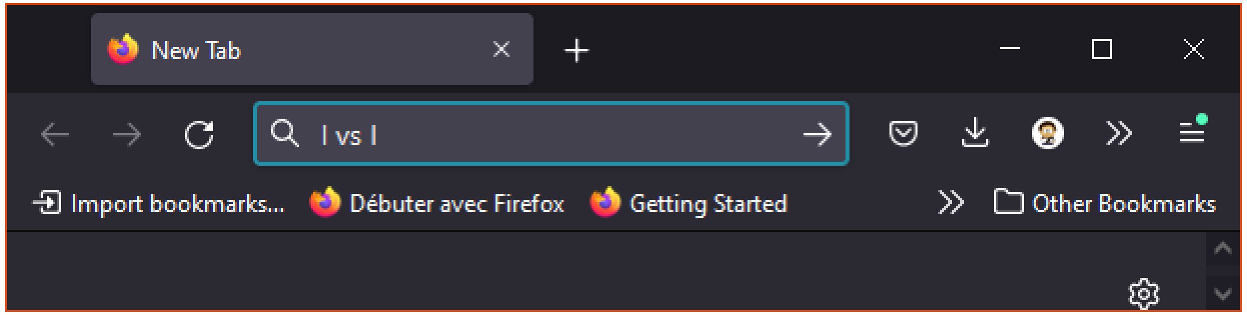


rakija.(ASCII) vs rakijạ(diatric)

Round 5/5

No help. It’s too easy.
Which is which?

l vs I

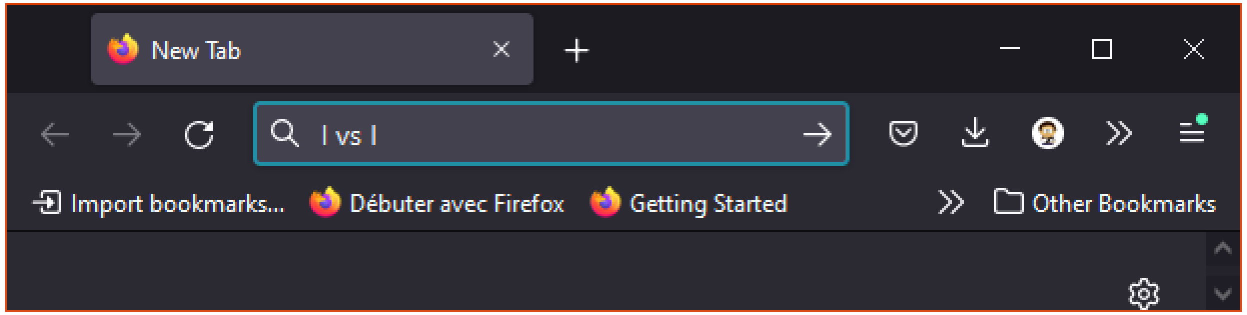


l vs I

Round 5/5 - Answer

No help. It’s too easy.

l (lowercase L) VS I (uppercase i)



Tor

Wake up, Neo…

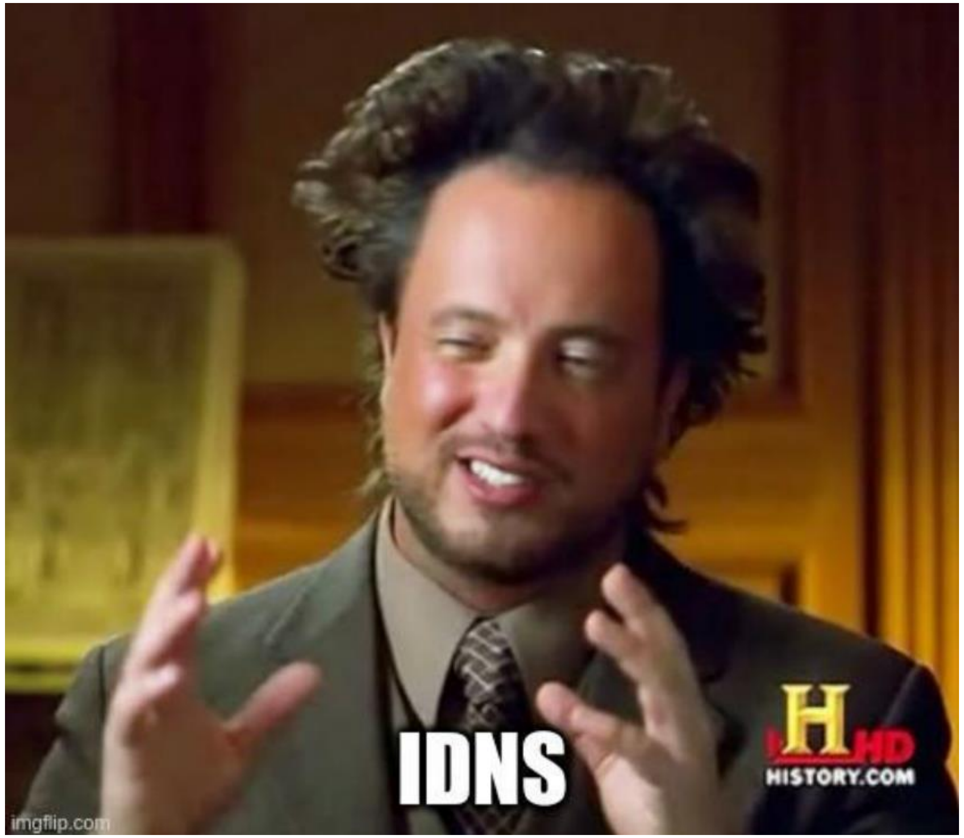
Game TL;DP (Too Long;Didn’t Play)

- Sometimes hard to recognize one charset to the other with naked eye.
- Also, people may not understand that u and ü are different domains, so possibly illegal sites.
- So, are attacks possible? We’ll see about that.

Typosquatting, homograph and similar attacks on domains typo

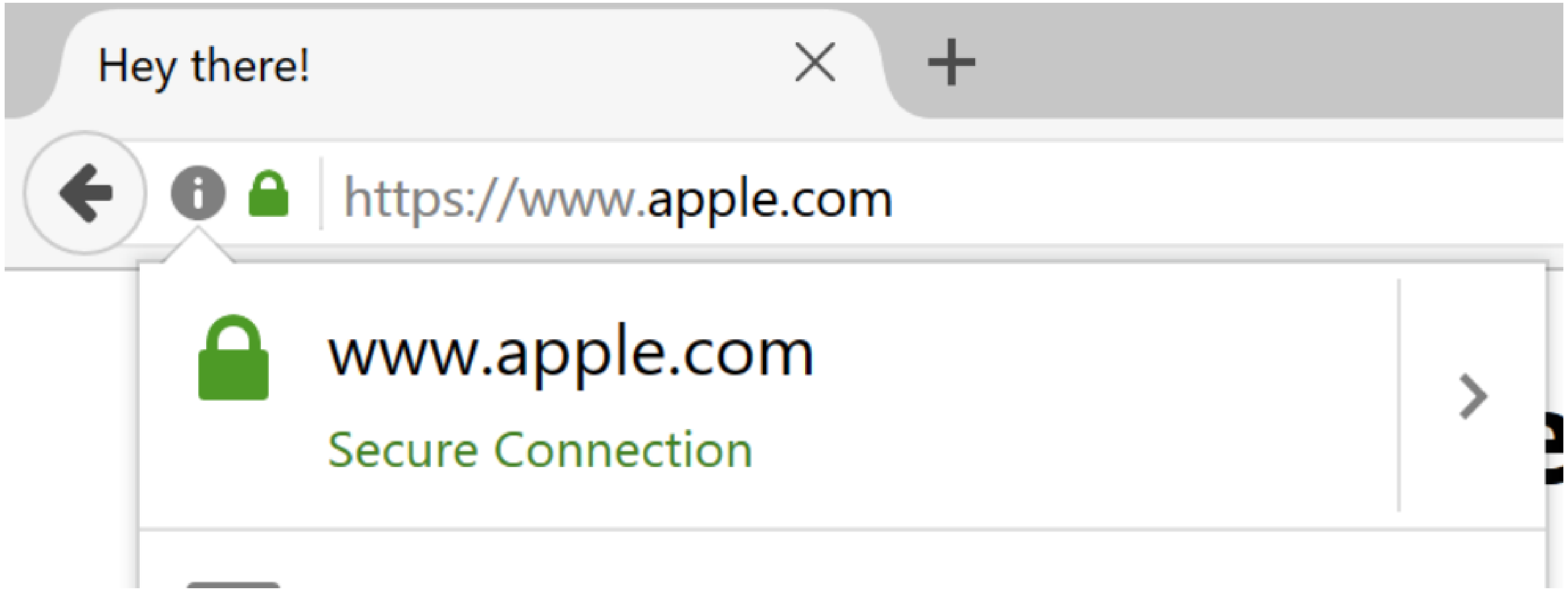
- Typosquatting is the generic term for cybersquatting and brandjacking with domain names. Techniques used:
  - Bad spelling,
  - Plural instead of singular,
  - A different TLD/ccTLD,
  - **Homographic attacks, using with different alphabets to have same or similar looking websites.**
- Combosqutting: appending an arbitrary word on a domain that may seem appropriate/logical.
- Doppelganger domain: fusionning two domain labels into one.

Some historical homograph attacks in the wild



apple.com – cyrillic a

Xudong Zeng, 14th of April 2017



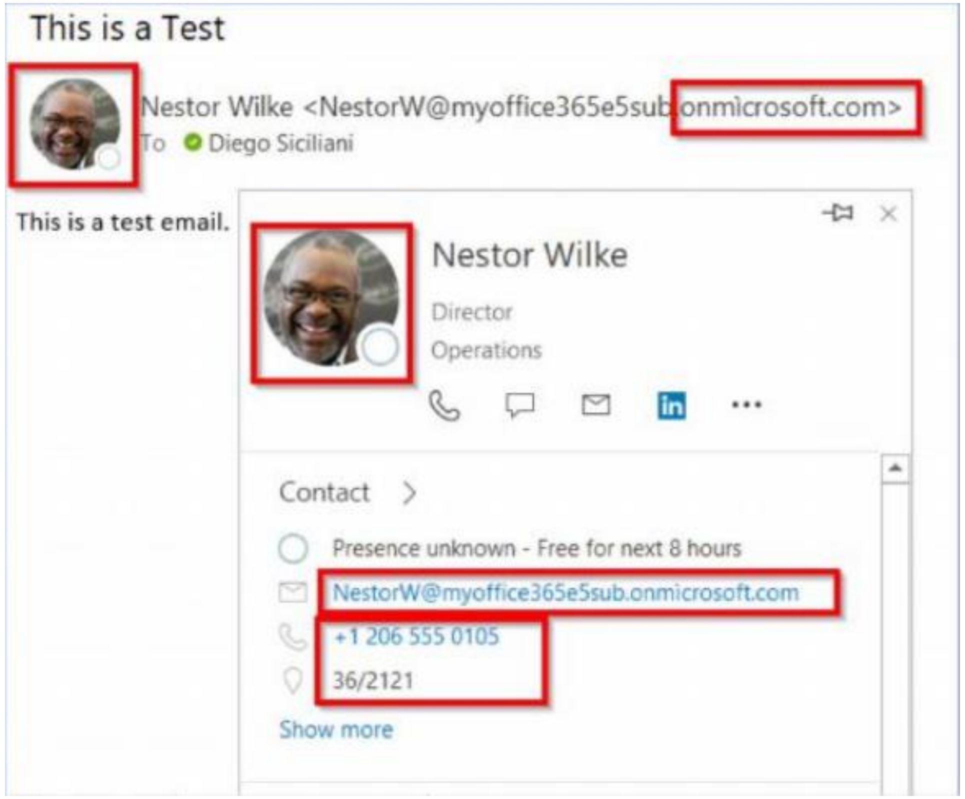
www.apple.com

Secure Connection

M1cr0$0ft Outlook vulnerability

DobbyWanKenobi, 2021

- Imagine you have your good friend, Jean Bon, email `jean.bon@mycompany.onmicrosoft.com` in your address book.
- The code thingy linking an address book's contact to a mail 'simplifies' some accentuated chars.
- Meaning that if you receive a phishing email from `jean.bon@mycompany.onmìcrosoft.com`, it will link it to your good friend in your address book, Jean Bon, which it is not.



This is a Test

Nestor Wilke <NestorW@myoffice365e5sub.onmìcrosoft.com>
To Diego Siciliani

This is a test email.

Nestor Wilke
Director
Operations

Contact >

Presence unknown - Free for next 8 hours
NestorW@myoffice365e5sub.onmicrosoft.com
+1 206 555 0105
36/2121
Show more

What about bad guys?

APWG – Anti phishing working group

Status – APWG report from 2016 (last one with an IDN section)

- Phishers don’t seem to be interested a lot in these, even though the occurrence of IDNs homograph seem to increase a bit.
  - Phishers are right: many people don’t check the FQDN of a phishing page, as long as email + landing page seems convincing.
- My guess: as more and more people will be cautious about domains, these attacks will be used a lot more.

Examples

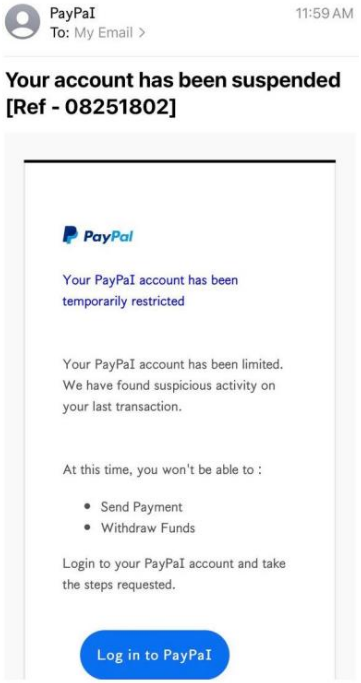
- From 2007 to 2014
  - Only 9 real homograph attacks.
- In 2015
  - `xn--paypl-680b.com` aka **paypḁl.com**
- In 2016
  - About 185 IDNs used for phishing.
  - 2 real homograph attacks:
    - `xn--fcbook-wta9d.com` aka **fâcêbook.com**
    - `xn--arbnb-b4a.com` aka **aįrbnb.com**

PayPal – since mid 2000s

Look again above, it is paypai (capital i)

- Created in mid-2000.
  - Reused in 2011, 2012, 2017, 2020
- Phishing to get credentials.
- Website registered by a company named Network Solutions, to a certain Birykov in Russia.

Screenshot credit to u/xellos30 on Reddit



PayPaI
To: My Email >
11:59 AM

Your account has been suspended [Ref - 08251802]

Your PayPaI account has been temporarily restricted

Your PayPaI account has been limited. We have found suspicious activity on your last transaction.

At this time, you won't be able to :

- Send Payment
- Withdraw Funds

Login to your PayPaI account and take the steps requested.

assurance-maladie.fr, 06/09/2022

Ll and li, again. Probably against French citizens.

Domain WHOIS

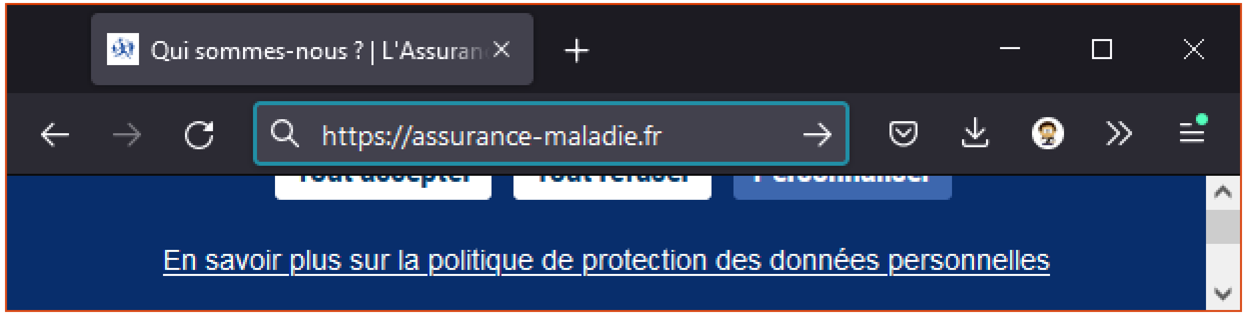
- Registrar : AMEN / Agence des Médias Numériques
  - Created Date: July 9, 2022 11:07:18 UTC.
  - Updated Date: Sept 7, 2022.
- Holder : Restricted access
  - Administrative contact : Restricted access (Thanks GDPR).
  - Technical contact : AMEN France.

IP Whois

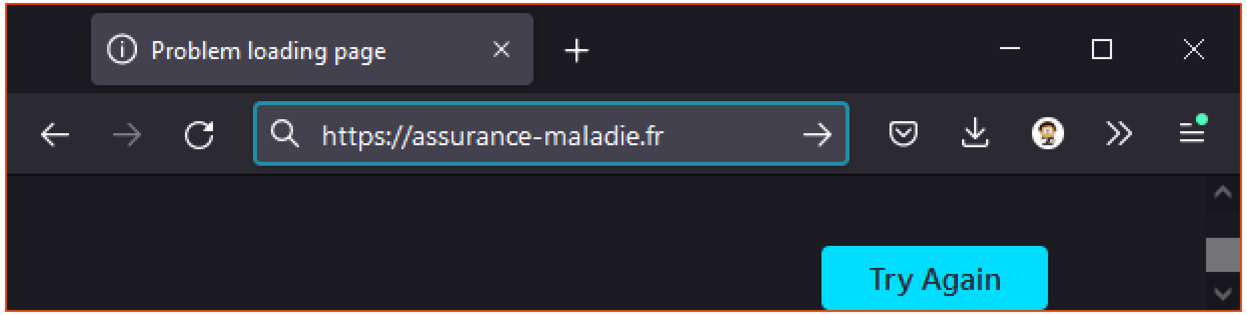
- Sept 6: Russian hosting provider solutions, so not an official website…
- Sept 7: Digital Ocean.

- Server no longer responding…
  - Was showing an auto-index with many PHP pages and frameworks.

Guessing domain is on hold/seized due to the alert



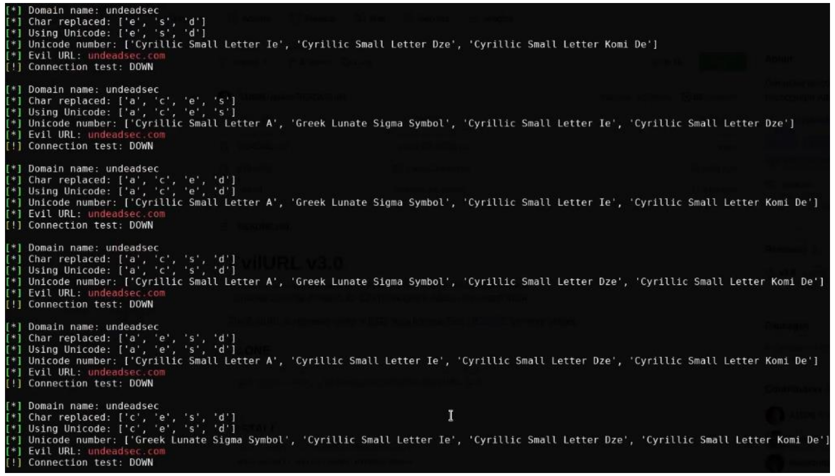
En savoir plus sur la politique de protection des données personnelles



Attacker/pentester toolboxes

IDN Homograph + Lazy? EvilURL!

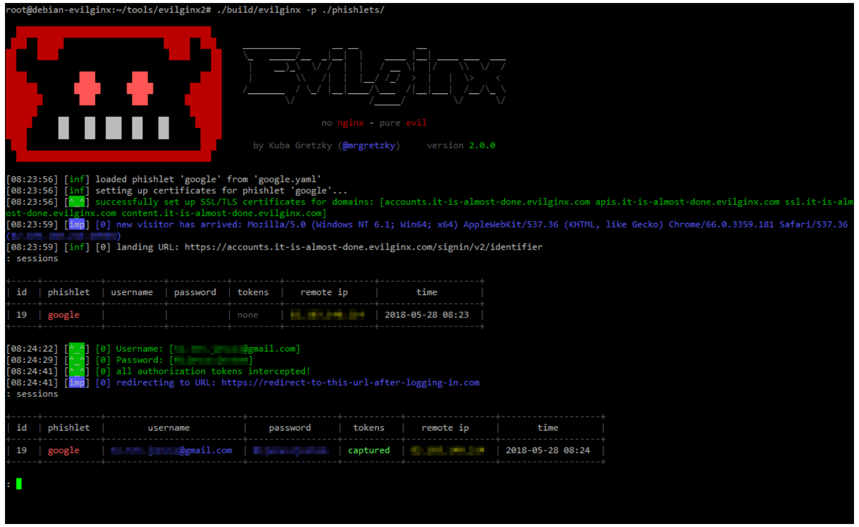
- IDN generator for a domain name of your choice, noice.
- Can also be used to detect homograph attacks on your domain.



```
[*] Domain name: undeadsec
[*] Char replaced: ['e', 's', 'd']
[*] Using Unicode: ['e', 's', 'd']
[*] Unicode number: ['Cyrillic Small Letter Ie', 'Cyrillic Small Letter Dze', 'Cyrillic Small Letter Komi De']
[*] Evil URL: undeadsec.com
[!] Connection test: DOWN

[*] Domain name: undeadsec
[*] Char replaced: ['a', 'c', 'e', 's']
[*] Using Unicode: ['a', 'c', 'e', 's']
[*] Unicode number: ['Cyrillic Small Letter A', 'Greek Lunate Sigma Symbol', 'Cyrillic Small Letter Ie', 'Cyrillic Small Letter Dze']
[*] Evil URL: undeadsec.com
[!] Connection test: DOWN

[*] Domain name: undeadsec
[*] Char replaced: ['a', 'c', 'e', 'd']
[*] Using Unicode: ['a', 'c', 'e', 'd']
[*] Unicode number: ['Cyrillic Small Letter A', 'Greek Lunate Sigma Symbol', 'Cyrillic Small Letter Ie', 'Cyrillic Small Letter Komi De']
[*] Evil URL: undeadsec.com
[!] Connection test: DOWN

[*] Domain name: undeadsec
[*] Char replaced: ['a', 'c', 's', 'd']
[*] Using Unicode: ['a', 'c', 's', 'd']
[*] Unicode number: ['Cyrillic Small Letter A', 'Greek Lunate Sigma Symbol', 'Cyrillic Small Letter Dze', 'Cyrillic Small Letter Komi De']
[*] Evil URL: undeadsec.com
[!] Connection test: DOWN

[*] Domain name: undeadsec
[*] Char replaced: ['a', 'e', 's', 'd']
[*] Using Unicode: ['a', 'e', 's', 'd']
[*] Unicode number: ['Cyrillic Small Letter A', 'Cyrillic Small Letter Ie', 'Cyrillic Small Letter Dze', 'Cyrillic Small Letter Komi De']
[*] Evil URL: undeadsec.com
[!] Connection test: DOWN

[*] Domain name: undeadsec
[*] Char replaced: ['c', 'e', 's', 'd']
[*] Using Unicode: ['c', 'e', 's', 'd']
[*] Unicode number: ['Greek Lunate Sigma Symbol', 'Cyrillic Small Letter Ie', 'Cyrillic Small Letter Dze', 'Cyrillic Small Letter Komi De']
[*] Evil URL: undeadsec.com
[!] Connection test: DOWN
```

Evil reverse proxy + Lazy? EVILGINX!

- Custom Nginx for MiTM, getting session cookies, bypass bad 2FA (SMS, mail, OTP)



```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                              no nginx - pure evil

                    by Kuba Gretzky (@mrgretzky)      version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-alm
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+----+----------+----------+----------+--------+-------------+------------------+
| id | phishlet | username | password | tokens |  remote ip  |       time       |
+----+----------+----------+----------+--------+-------------+------------------+
| 19 | google   |          |          | none   | [redacted]  | 2018-05-28 08:23 |
+----+----------+----------+----------+--------+-------------+------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+----+----------+----------------------+---------------+----------+-------------+------------------+
| id | phishlet |       username       |   password    |  tokens  |  remote ip  |       time       |
+----+----------+----------------------+---------------+----------+-------------+------------------+
| 19 | google   | [redacted]@gmail.com | [redacted]    | captured | [redacted]  | 2018-05-28 08:24 |
+----+----------+----------------------+---------------+----------+-------------+------------------+

: 
```

My experiences with IDNs homographs

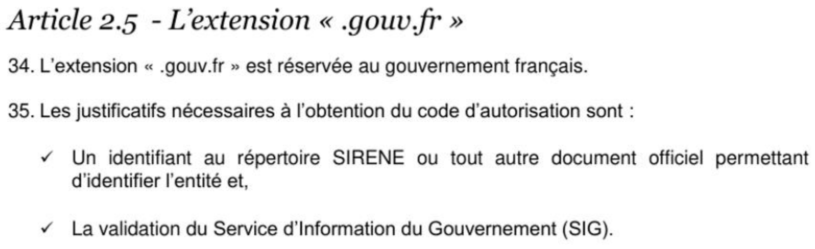
A bad idea later…

In a cold December night, in 2019…

- During a phone call with a friend, we wanted to use stoopid homograph attacks to make a demo website for our students/trainees to learn about this kind of attacks, as it may be powerful for spear-phishing attacks and is not well known/not a lot used for now.
- What could be a good and impacting demo for our French participants?
- Must be a domain name every French knows.

Looking at AFNIC's Naming Policy at the time (changed since then)

- Version 25th of May 2018



Article 2.5 - L'extension « .gouv.fr »

34. L'extension « .gouv.fr » est réservée au gouvernement français.

35. Les justificatifs nécessaires à l'obtention du code d'autorisation sont :

✓ Un identifiant au répertoire SIRENE ou tout autre document officiel permettant d'identifier l'entité et,

✓ La validation du Service d'Information du Gouvernement (SIG).

Nothing about IDNs, right?

göuv.fr aka `xn--guv-sna.fr` and göüv.fr aka `xn--gv-fkay.fr`

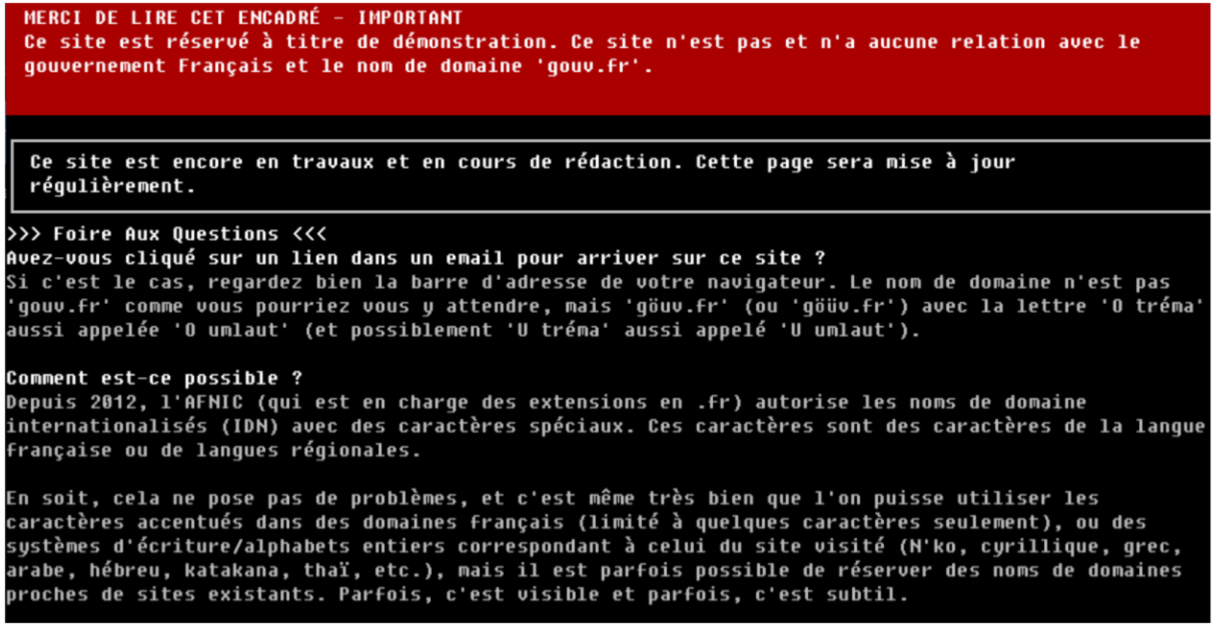
Additional information

- `Gouv` was not a « restricted » term.
  - A « restricted » terms (extremism, racism, administration etc.) must follow some rules and are subject to approval.
- Cannot have a name too close to administration, except if:
  - Good will: *white hat sec engineer*,
  - Legitimate interest: *trainings/demos in cybersecurity*.

What i’ve done…

… not to end up in jail.

- Static HTML page explaining the attack.
- HTTPs with Let’s Encrypt:
  - `impots.göuv.fr`
  - `defense.göuv.fr`
  - `interieur.göuv.fr`
  - …
- Way of contacting me on the page.

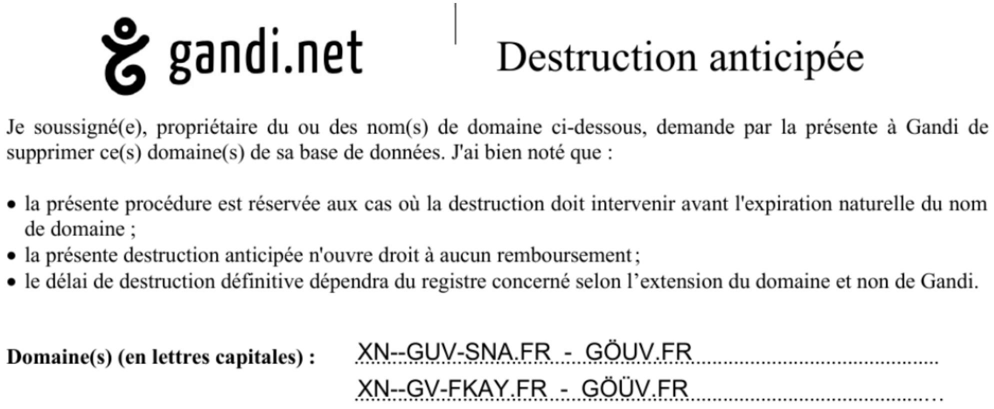


```
MERCI DE LIRE CET ENCADRÉ - IMPORTANT
Ce site est réservé à titre de démonstration. Ce site n'est pas et n'a aucune relation avec le
gouvernement Français et le nom de domaine 'gouv.fr'.

Ce site est encore en travaux et en cours de rédaction. Cette page sera mise à jour
régulièrement.

>>> Foire Aux Questions <<<
Avez-vous cliqué sur un lien dans un email pour arriver sur ce site ?
Si c'est le cas, regardez bien la barre d'adresse de votre navigateur. Le nom de domaine n'est pas
'gouv.fr' comme vous pourriez vous y attendre, mais 'göuv.fr' (ou 'göüv.fr') avec la lettre 'O tréma'
aussi appelée 'O umlaut' (et possiblement 'U tréma' aussi appelé 'U umlaut').

Comment est-ce possible ?
Depuis 2012, l'AFNIC (qui est en charge des extensions en .fr) autorise les noms de domaine
internationalisés (IDN) avec des caractères spéciaux. Ces caractères sont des caractères de la langue
française ou de langues régionales.

En soit, cela ne pose pas de problèmes, et c'est même très bien que l'on puisse utiliser les
caractères accentués dans des domaines français (limité à quelques caractères seulement), ou des
systèmes d'écriture/alphabets entiers correspondant à celui du site visité (N'ko, cyrillique, grec,
arabe, hébreu, katakana, thaï, etc.), mais il est parfois possible de réserver des noms de domaines
proches de sites existants. Parfois, c'est visible et parfois, c'est subtil.
```

…and what happened

31 of March 2021 (about a year and a half in)

- Contacted by ANSSI (French ITSec authority) via Twitter DMs, then exchanging by GPG emails.
- Asked me to destroy my two domains. Which i did, no jail is good.
- Changed the French law, no longer possible to do without risking jail time.
- Still on archive.org :)

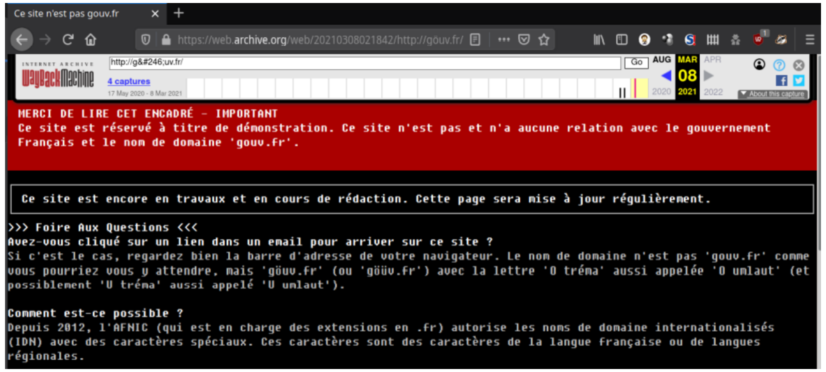


gandi.net | Destruction anticipée

Je soussigné(e), propriétaire du ou des nom(s) de domaine ci-dessous, demande par la présente à Gandi de supprimer ce(s) domaine(s) de sa base de données. J'ai bien noté que :

- la présente procédure est réservée aux cas où la destruction doit intervenir avant l'expiration naturelle du nom de domaine ;
- la présente destruction anticipée n'ouvre droit à aucun remboursement ;
- le délai de destruction définitive dépendra du registre concerné selon l'extension du domaine et non de Gandi.

Domaine(s) (en lettres capitales) : XN--GUV-SNA.FR - GÖUV.FR
XN--GV-FKAY.FR - GÖÜV.FR



```
MERCI DE LIRE CET ENCADRÉ - IMPORTANT
Ce site est réservé à titre de démonstration. Ce site n'est pas et n'a aucune relation avec le gouvernement
Français et le nom de domaine 'gouv.fr'.

 Ce site est encore en travaux et en cours de rédaction. Cette page sera mise à jour régulièrement.

>>> Foire Aux Questions <<<
Avez-vous cliqué sur un lien dans un email pour arriver sur ce site ?
Si c'est le cas, regardez bien la barre d'adresse de votre navigateur. Le nom de domaine n'est pas 'gouv.fr' comme
vous pourriez vous y attendre, mais 'göuv.fr' (ou 'göüv.fr') avec la lettre 'O tréma' aussi appelée 'O umlaut' (et
possiblement 'U tréma' aussi appelé 'U umlaut').

Comment est-ce possible ?
Depuis 2012, l'AFNIC (qui est en charge des extensions en .fr) autorise les noms de domaine internationalisés
(IDN) avec des caractères spéciaux. Ces caractères sont des caractères de la langue française ou de langues
régionales.
```

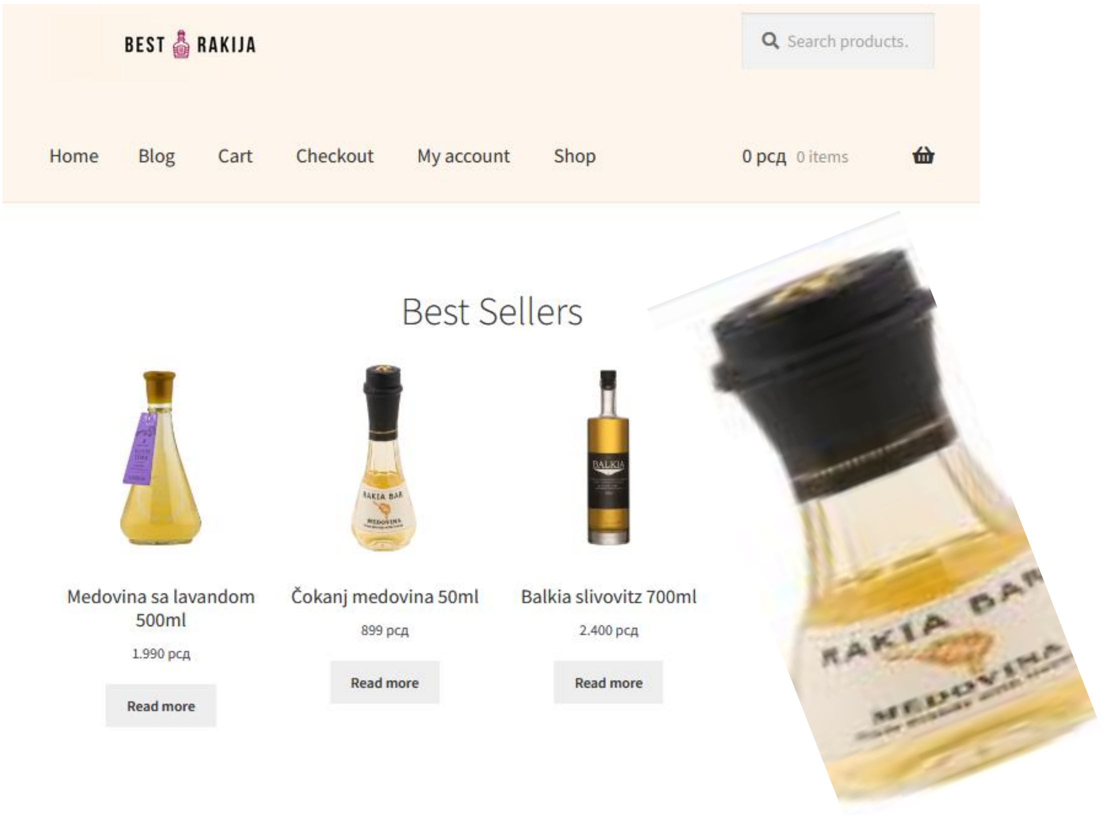
Demonstration

bestrakija.com

BEST RAKIJA

I love rakija.
not all rakija btw, but medovina and šljivovica 😵‍💫 🥰 🥴

- So I created the now world famous **`bestrakija.com`**, as a standard ASCII domain for the sake of the demonstration.
  - Buy your favorite rakija today…
    … except this is not a real eshop.
  - `Wordpress` + `Woocommerce` plugins on a dedicated VPS.
- **But also two homograph IDNs.**
  - And another 🏴‍☠️dedicated VPS.
- **Let go to the demo.**



BEST RAKIJA

Search products.

Best Sellers

Medovina sa lavandom 500ml
1.990 рсд
Read more

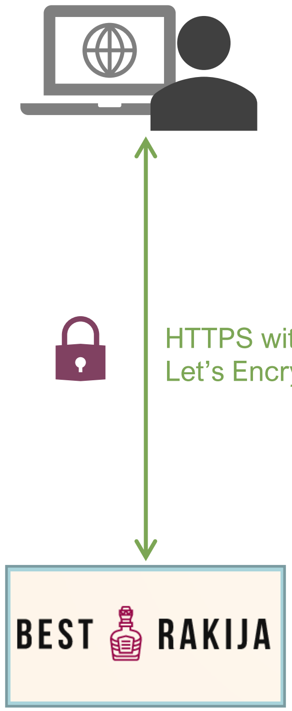
Čokanj medovina 50ml
899 рсд
Read more

Balkia slivovitz 700ml
2.400 рсд
Read more

https://menu.bestrakija.com/

bestrakija.com

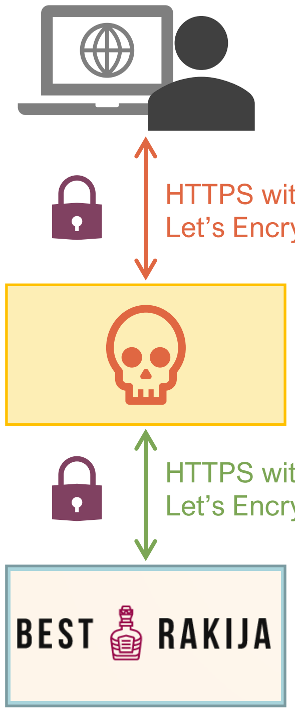
Legitimate connection



HTTPS with TLS1.2
Let’s Encrypt certificate for `bestrakija.com`

IP: 51.77.213.98
Apache + Wordpress + Woocommerce
Like a real ecommerce website ;)

🏴‍☠️ connection



User phished, clicked on a bad link, etc.

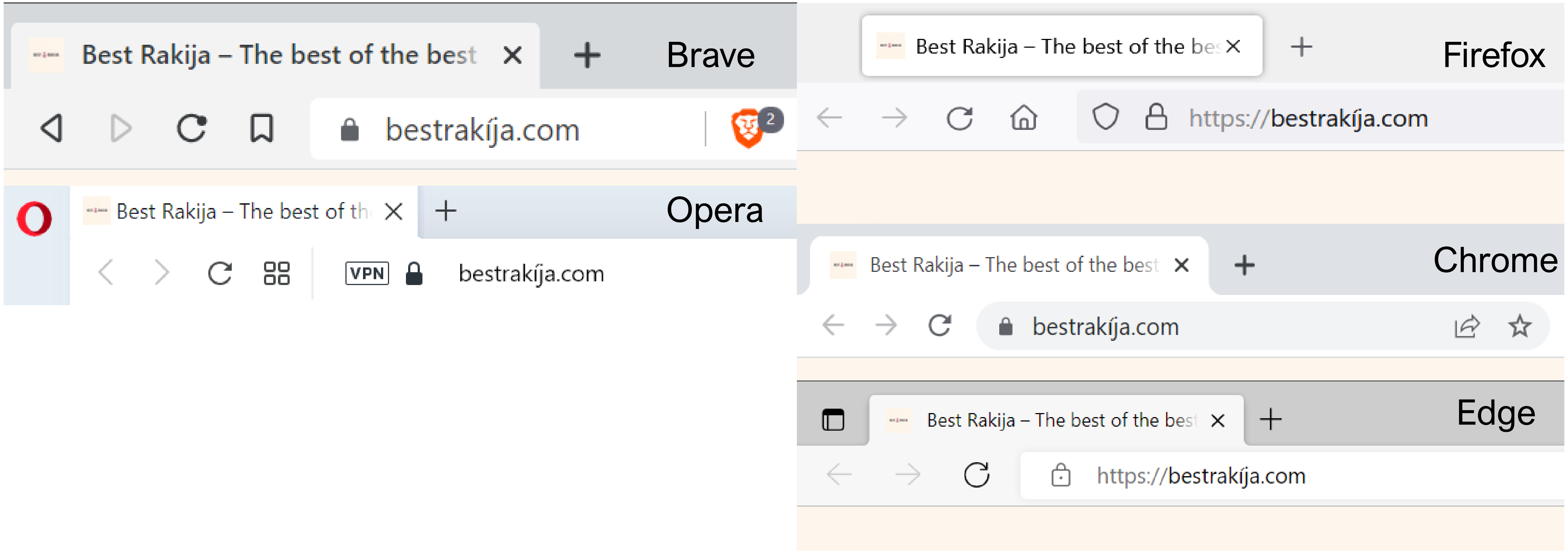
HTTPS with TLS1.2
Let’s Encrypt certificate for `xn--bestrakja-m5a.com`

IP: 51.77.213.99
Apache configured as Reverse proxy
Small 🏴‍☠️ PHP script parsing POST DATA coming through.

HTTPS with TLS1.2
Let’s Encrypt certificate for `bestrakija.com`

IP: 51.77.213.98
Apache + Wordpress + Woocommerce
Like a real ecommerce website ;)

bestrakíja.com in browsers



Brave

Best Rakija – The best of the best

bestrakíja.com

Opera

Best Rakija – The best of th

VPN

bestrakíja.com

Firefox

Best Rakija – The best of the bes

https://bestrakíja.com

Chrome

Best Rakija – The best of the best

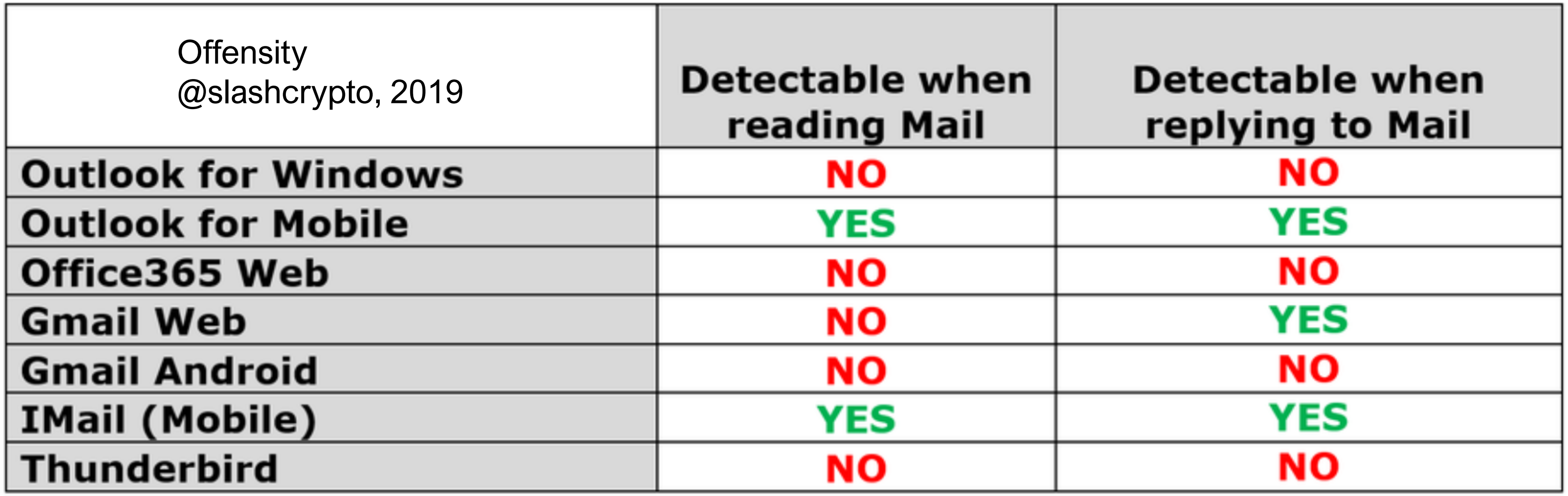
bestrakíja.com

Edge

Best Rakija – The best of the best

https://bestrakíja.com

bestrakíja.com in emails



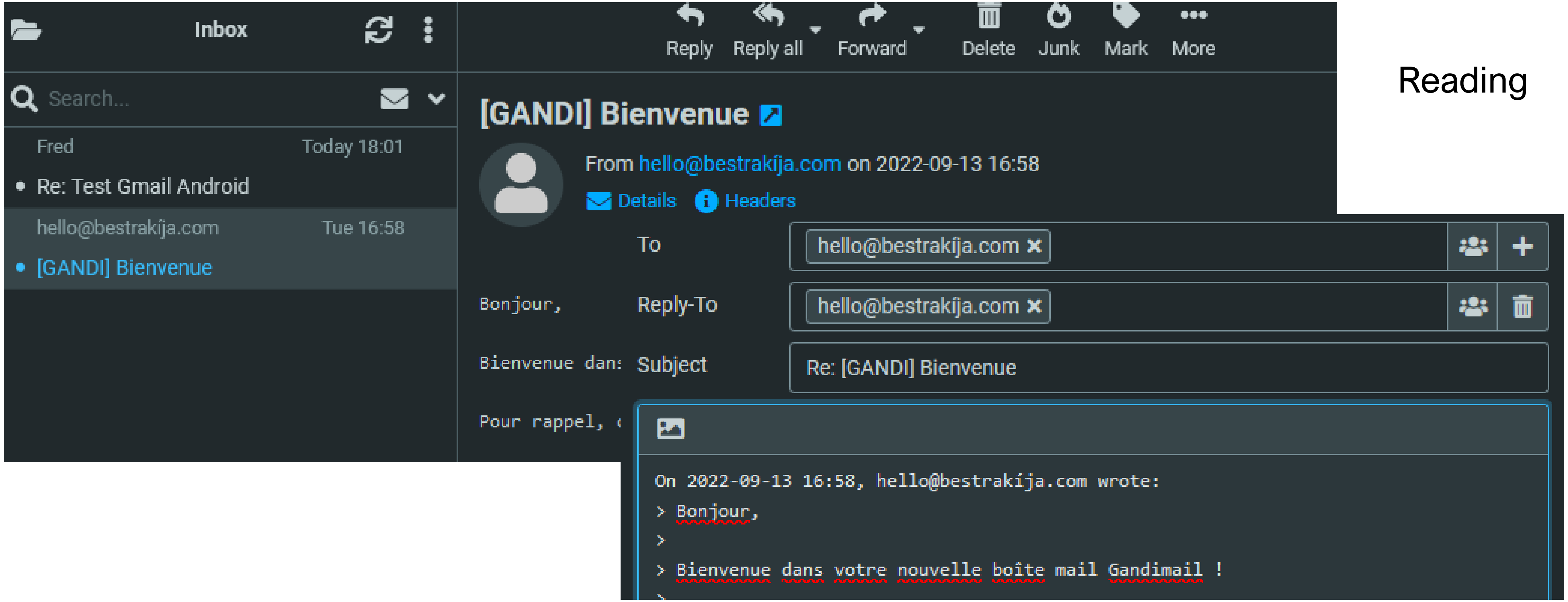
Offensity @slashcrypto, 2019	Detectable when reading Mail	Detectable when replying to Mail
Outlook for Windows	NO	NO
Outlook for Mobile	YES	YES
Office365 Web	NO	NO
Gmail Web	NO	YES
Gmail Android	NO	NO
IMail (Mobile)	YES	YES
Thunderbird	NO	NO

bestrakíja.com in Roundcube

Preview

Reading

Replying



Fred Today 18:01
Re: Test Gmail Android

hello@bestrakíja.com Tue 16:58
[GANDI] Bienvenue

[GANDI] Bienvenue

From hello@bestrakíja.com on 2022-09-13 16:58

Bonjour,

Bienvenue dan:

Pour rappel,

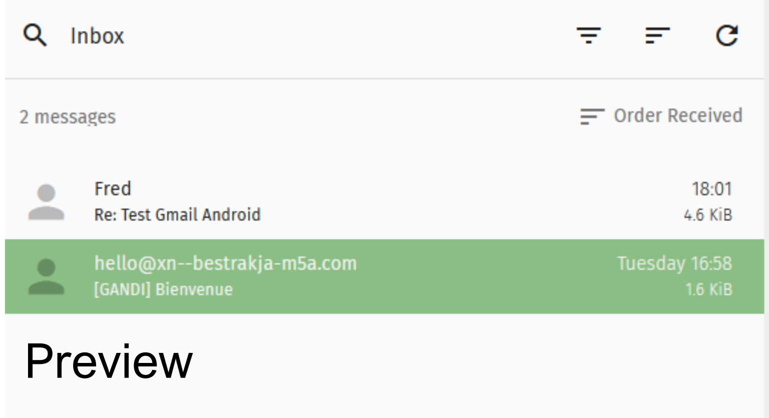
To: hello@bestrakíja.com

Reply-To: hello@bestrakíja.com

Subject: Re: [GANDI] Bienvenue

```
On 2022-09-13 16:58, hello@bestrakíja.com wrote:
> Bonjour,
>
> Bienvenue dans votre nouvelle boîte mail Gandimail !
```

bestrakíja.com in SOGo

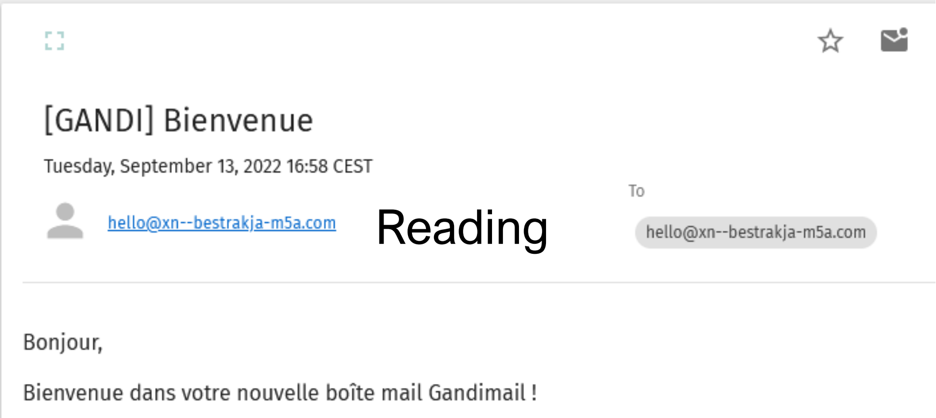


2 messages — Order Received

Fred — 18:01
Re: Test Gmail Android — 4.6 KiB

hello@xn--bestrakja-m5a.com — Tuesday 16:58
[GANDI] Bienvenue — 1.6 KiB

Preview



[GANDI] Bienvenue

Tuesday, September 13, 2022 16:58 CEST

hello@xn--bestrakja-m5a.com

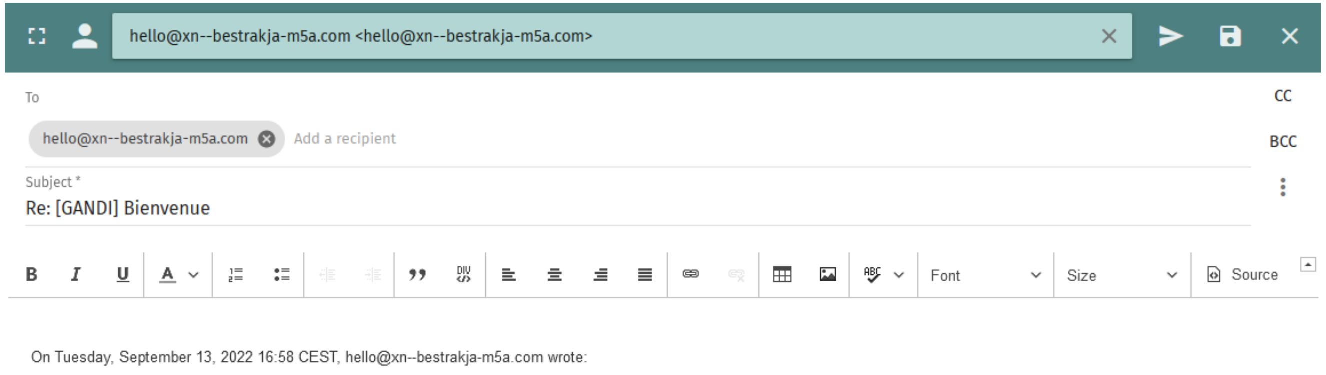
To
hello@xn--bestrakja-m5a.com

Reading

Bonjour,

Bienvenue dans votre nouvelle boîte mail Gandimail !

Replying



hello@xn--bestrakja-m5a.com <hello@xn--bestrakja-m5a.com>

To
hello@xn--bestrakja-m5a.com

Subject *
Re: [GANDI] Bienvenue

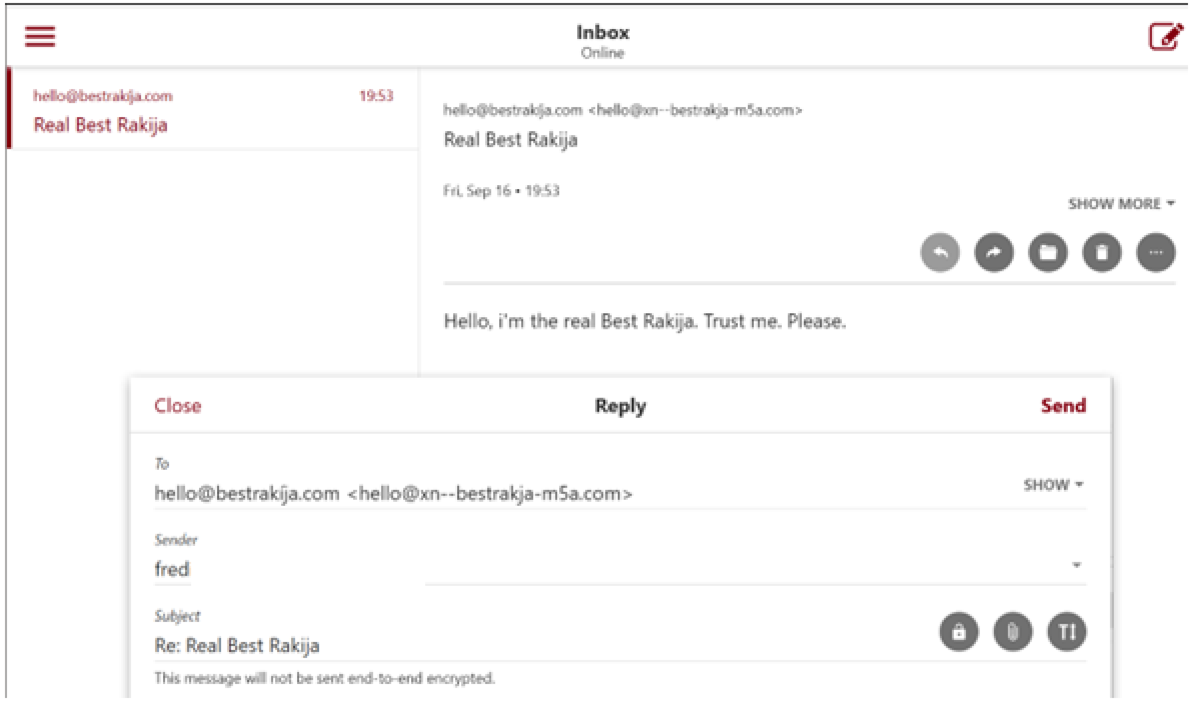
On Tuesday, September 13, 2022 16:58 CEST, hello@xn--bestrakja-m5a.com wrote:

bestrakíja.com in Tutanota

Preview

Reading

Replying



hello@bestrakíja.com 19:53
Real Best Rakija

hello@bestrakíja.com <hello@xn--bestrakja-m5a.com>
Real Best Rakija
Fri, Sep 16 • 19:53

Hello, i'm the real Best Rakija. Trust me. Please.

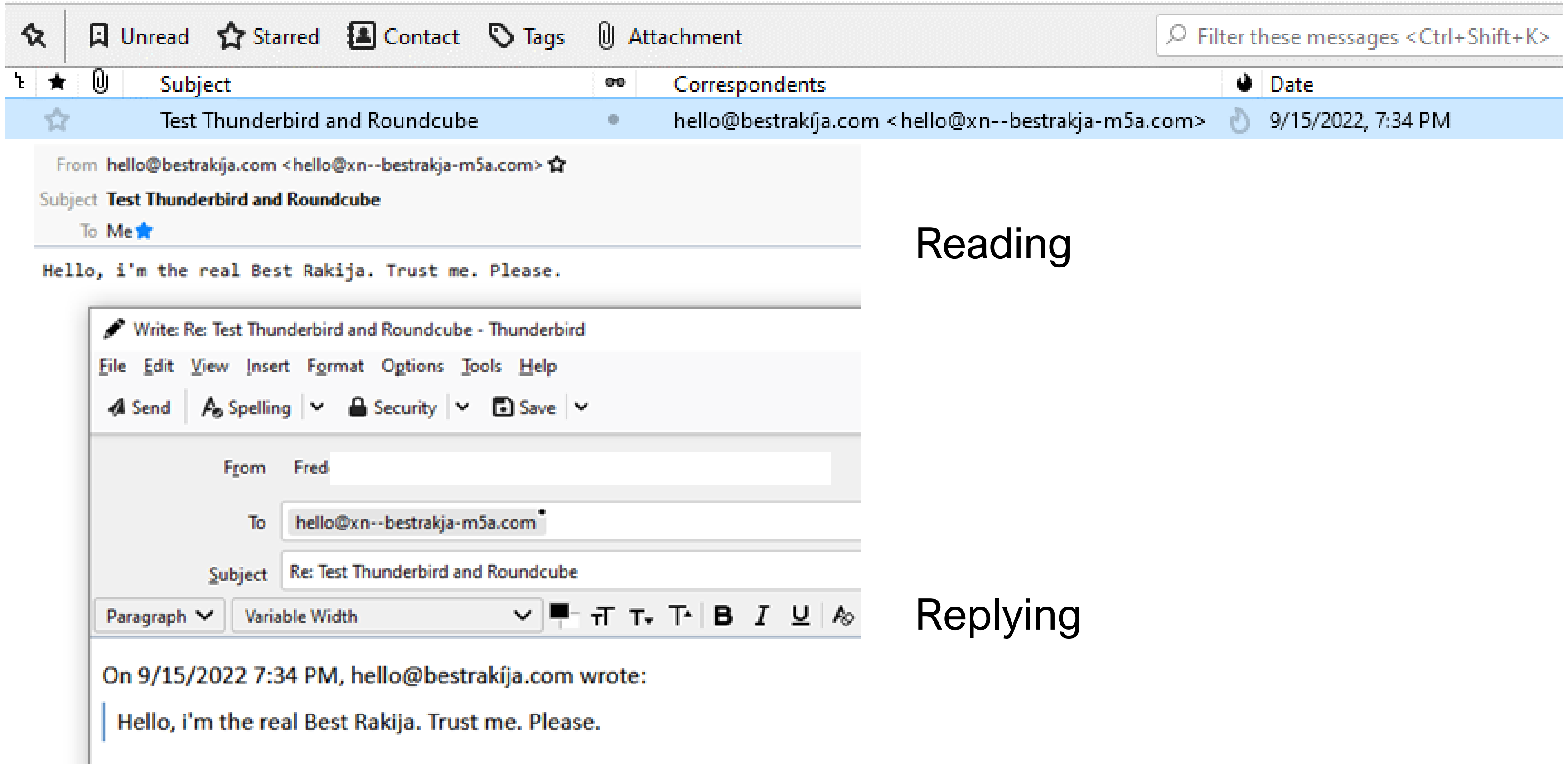
To
hello@bestrakíja.com <hello@xn--bestrakja-m5a.com>

Sender
fred

Subject
Re: Real Best Rakija

This message will not be sent end-to-end encrypted.

bestrakíja.com in Thunderbird



Subject	Correspondents	Date
Test Thunderbird and Roundcube	hello@bestrakíja.com <hello@xn--bestrakja-m5a.com>	9/15/2022, 7:34 PM

Preview

From hello@bestrakíja.com <hello@xn--bestrakja-m5a.com>
Subject **Test Thunderbird and Roundcube**
To Me

```
Hello, i'm the real Best Rakija. Trust me. Please.
```

Reading

Write: Re: Test Thunderbird and Roundcube - Thunderbird

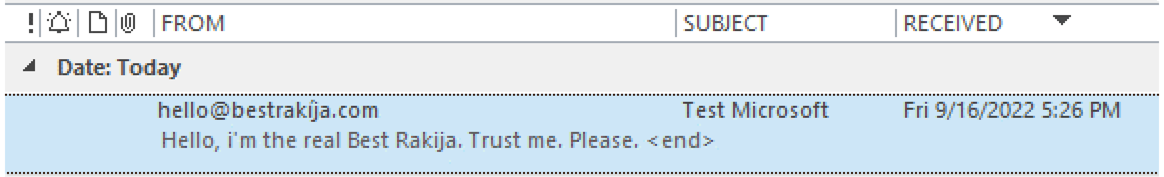
From Fred
To hello@xn--bestrakja-m5a.com
Subject Re: Test Thunderbird and Roundcube

On 9/15/2022 7:34 PM, hello@bestrakíja.com wrote:

> Hello, i'm the real Best Rakija. Trust me. Please.

Replying

bestrakíja.com in Outlook Desktop

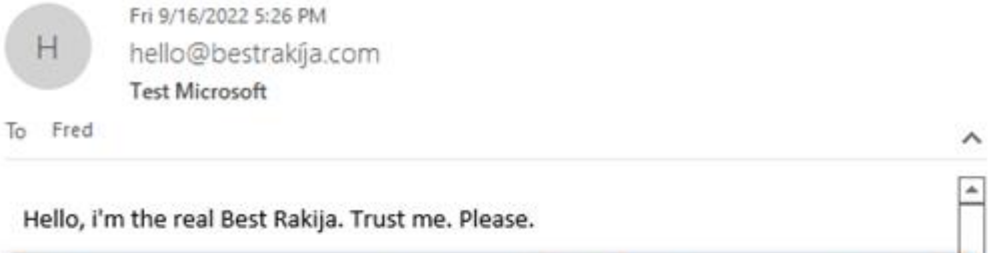


Date: Today

hello@bestrakíja.com Test Microsoft Fri 9/16/2022 5:26 PM

Hello, i'm the real Best Rakija. Trust me. Please. <end>

Preview



Fri 9/16/2022 5:26 PM

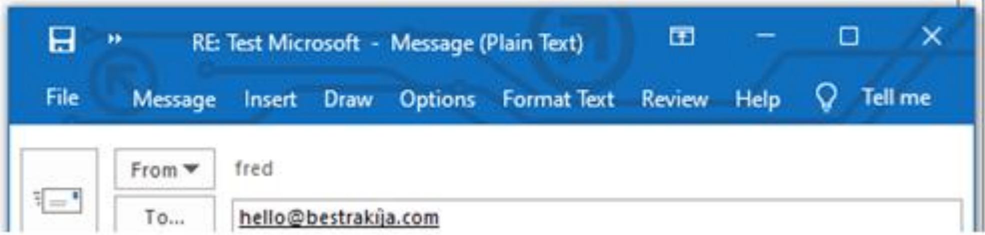
hello@bestrakíja.com

Test Microsoft

To Fred

Hello, i'm the real Best Rakija. Trust me. Please.

Reading



RE: Test Microsoft - Message (Plain Text)

From fred

To... hello@bestrakíja.com

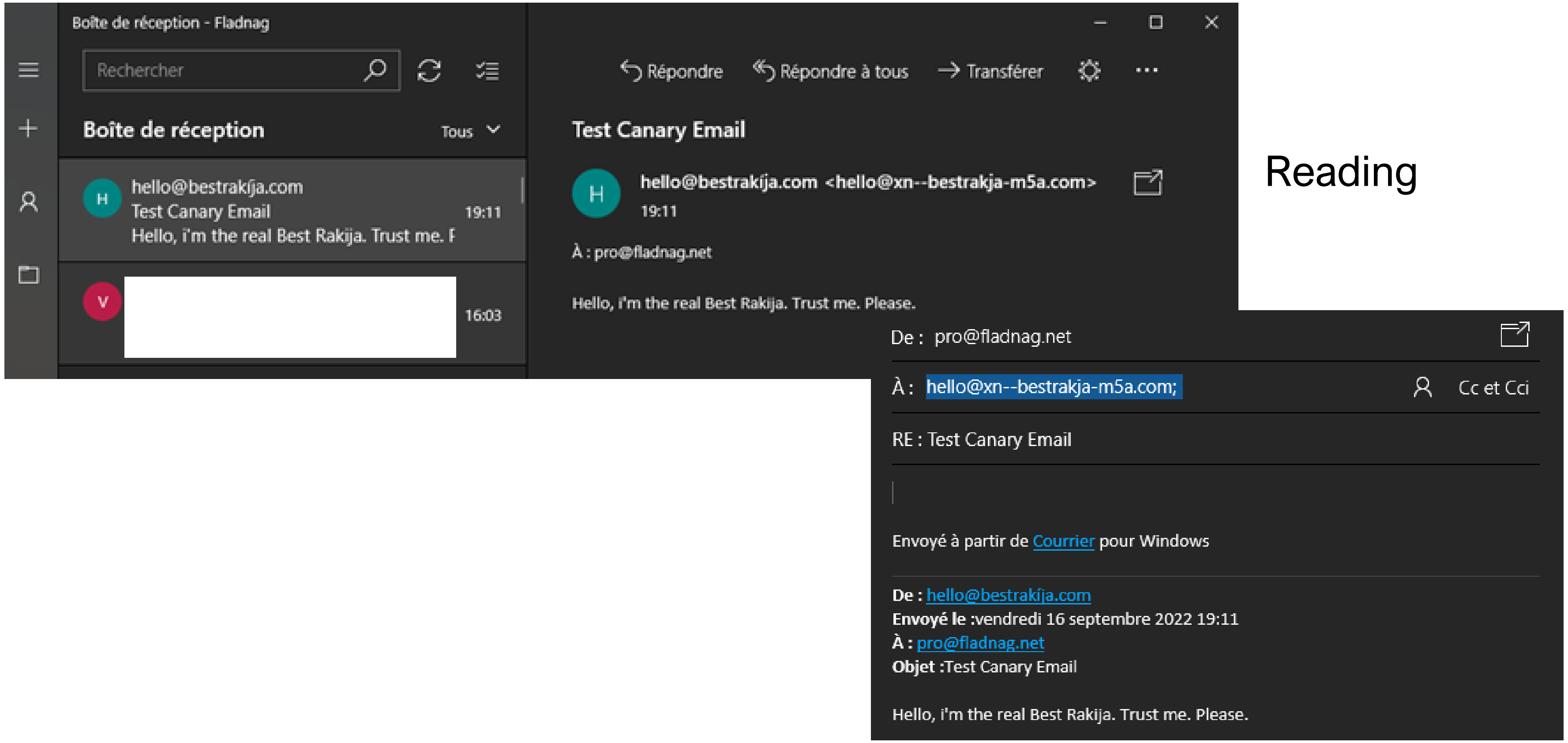
Replying

bestrakíja.com in Windows 10 Mail app

Preview

Reading

Replying



hello@bestrakíja.com
Test Canary Email 19:11
Hello, i'm the real Best Rakija. Trust me. P

V 16:03

Test Canary Email

hello@bestrakíja.com <hello@xn--bestrakja-m5a.com>
19:11

À : pro@fladnag.net

Hello, i'm the real Best Rakija. Trust me. Please.

De : pro@fladnag.net

À : hello@xn--bestrakja-m5a.com;

RE : Test Canary Email

Envoyé à partir de Courrier pour Windows

De : hello@bestrakíja.com
Envoyé le :vendredi 16 septembre 2022 19:11
À : pro@fladnag.net
Objet : Test Canary Email

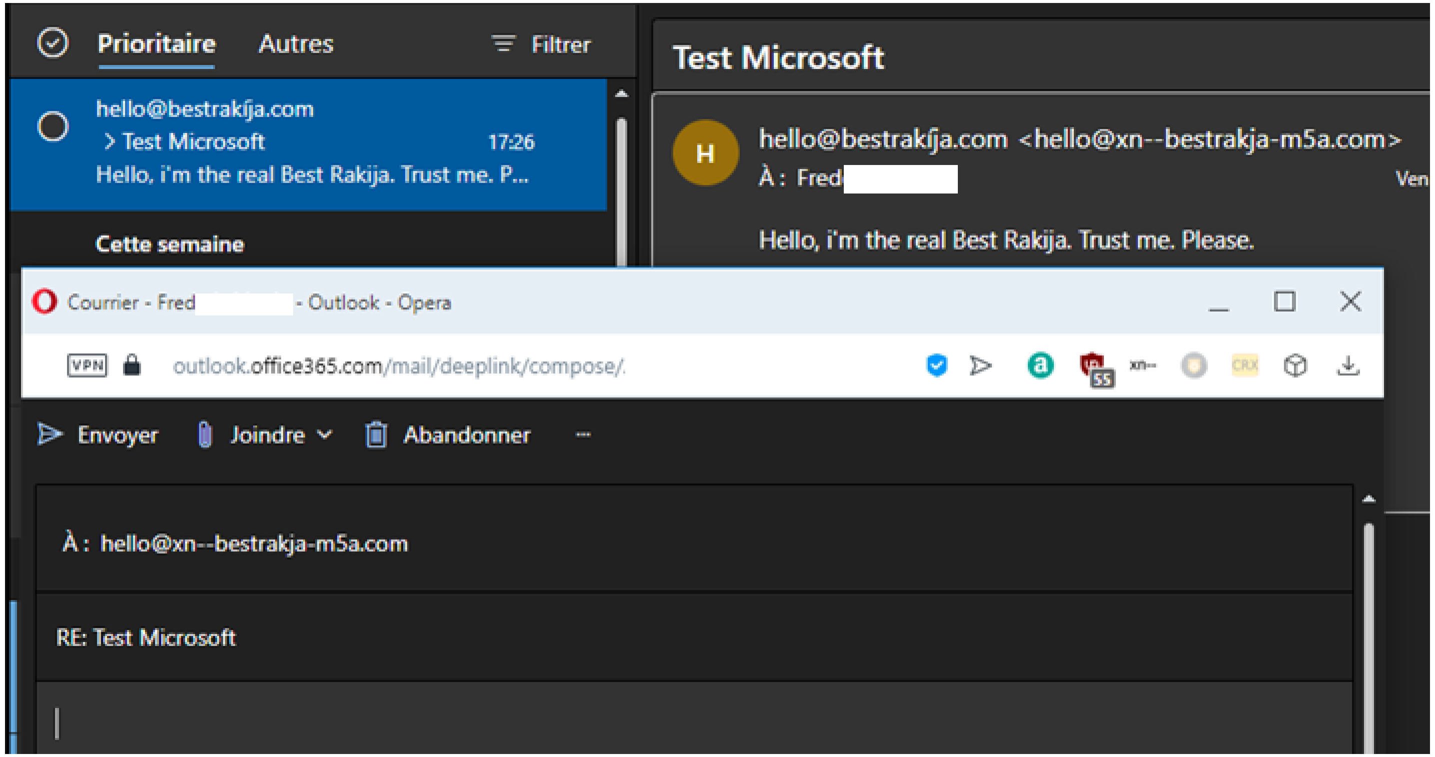
Hello, i'm the real Best Rakija. Trust me. Please.

bestrakíja.com in Office 365 webmail

Preview

Reading

Replying



hello@bestrakíja.com
> Test Microsoft 17:26
Hello, i'm the real Best Rakija. Trust me. P...

Test Microsoft

H hello@bestrakíja.com <hello@xn--bestrakja-m5a.com>
À : Fred [redacted]
Ven

Hello, i'm the real Best Rakija. Trust me. Please.

Courrier - Fred [redacted] - Outlook - Opera

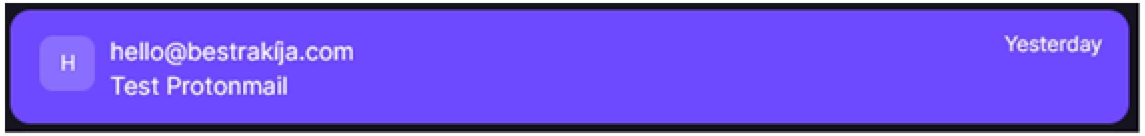
outlook.office365.com/mail/deeplink/compose/.

À : hello@xn--bestrakja-m5a.com

RE: Test Microsoft

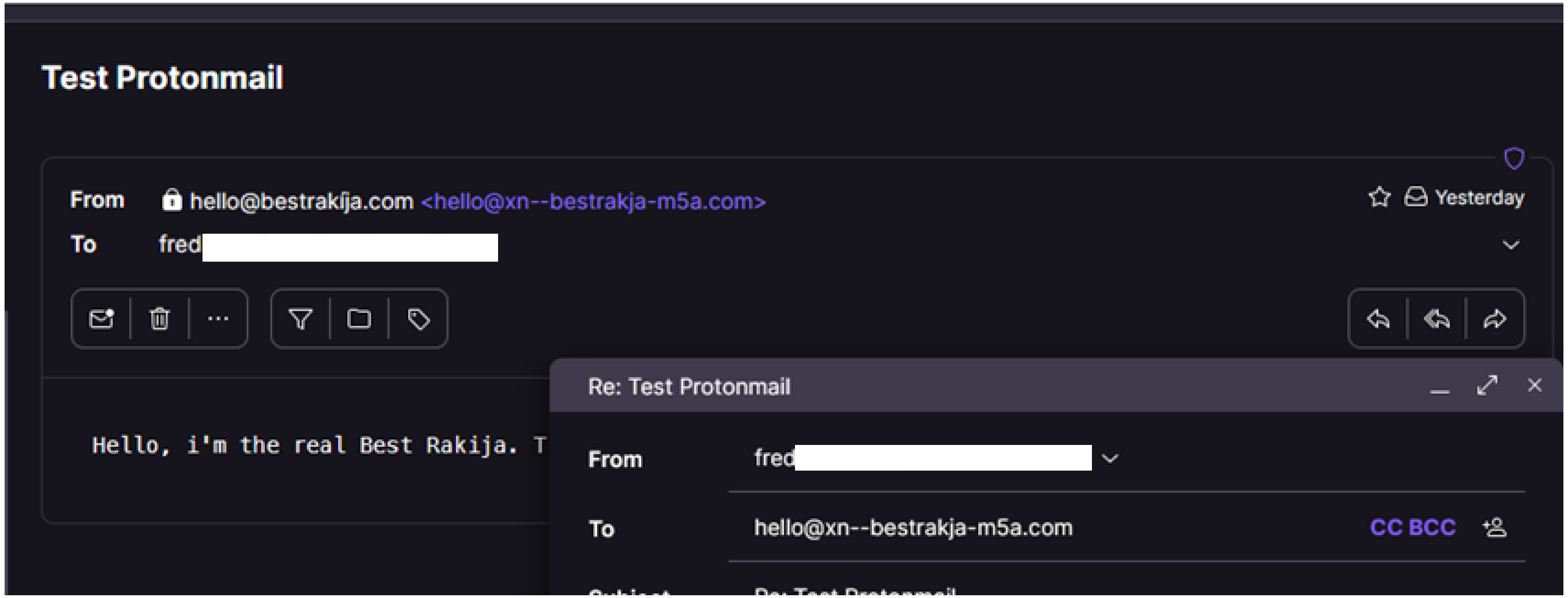
bestrakíja.com in Protonmail webmail

Preview



H hello@bestrakíja.com
Test Protonmail

Reading



Test Protonmail

From 🔒 hello@bestrakíja.com <hello@xn--bestrakja-m5a.com>

To fred[redacted]

```
Hello, i'm the real Best Rakija. T
```

Re: Test Protonmail

From fred[redacted]

To hello@xn--bestrakja-m5a.com

Subject Re: Test Protonmail

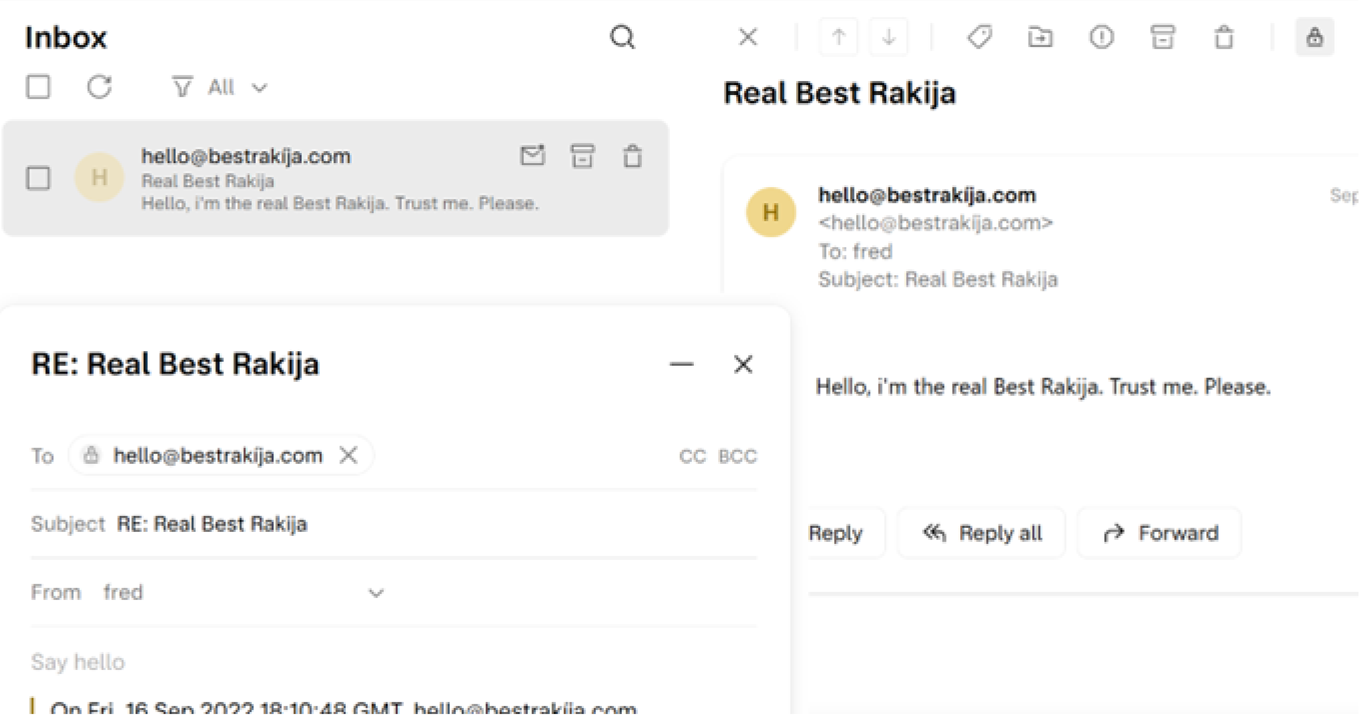
Replying

bestrakíja.com in Skiff webmail

Preview

Replying

Reading



□ H hello@bestrakija.com
Real Best Rakija
Hello, i'm the real Best Rakija. Trust me. Please.

Real Best Rakija

H hello@bestrakija.com
<hello@bestrakija.com>
To: fred
Subject: Real Best Rakija

Hello, i'm the real Best Rakija. Trust me. Please.

RE: Real Best Rakija

To hello@bestrakija.com ✕

Subject RE: Real Best Rakija

From fred

Say hello

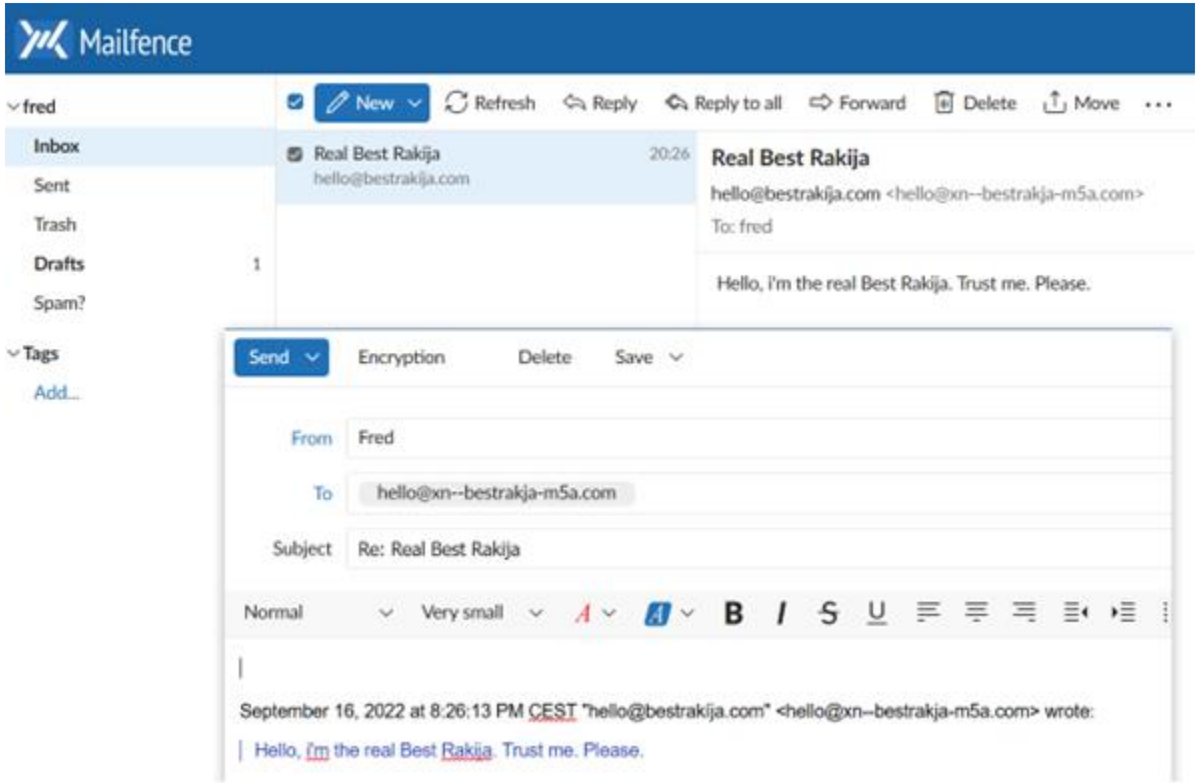
On Fri, 16 Sep 2022 18:10:48 GMT, hello@bestrakija.com

bestrakíja.com in Mailfence webmail

Preview

Reading

Replying



Real Best Rakija 20:26
hello@bestrakija.com

Real Best Rakija
hello@bestrakija.com <hello@xn--bestrakja-m5a.com>
To: fred

Hello, i'm the real Best Rakija. Trust me. Please.

From: Fred
To: hello@xn--bestrakja-m5a.com
Subject: Re: Real Best Rakija

September 16, 2022 at 8:26:13 PM CEST "hello@bestrakija.com" <hello@xn--bestrakja-m5a.com> wrote:

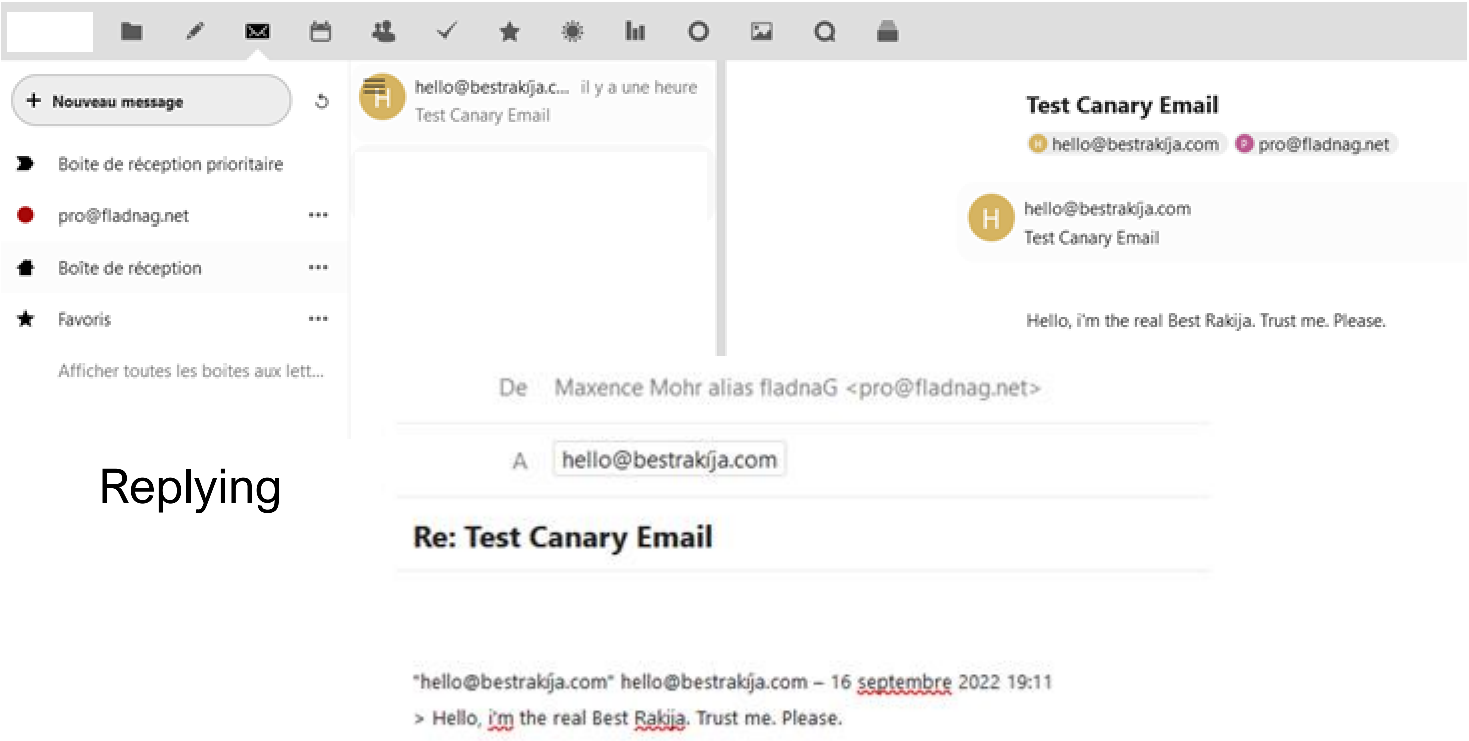
> Hello, i'm the real Best Rakija. Trust me. Please.

bestrakíja.com in Nextcloud webmail

Preview

Reading

Replying



+ Nouveau message
Boite de réception prioritaire
pro@fladnag.net
Boîte de réception
Favoris
Afficher toutes les boites aux lett...

hello@bestrakíja.c... il y a une heure
Test Canary Email

Test Canary Email
hello@bestrakíja.com pro@fladnag.net

hello@bestrakíja.com
Test Canary Email

Hello, i'm the real Best Rakija. Trust me. Please.

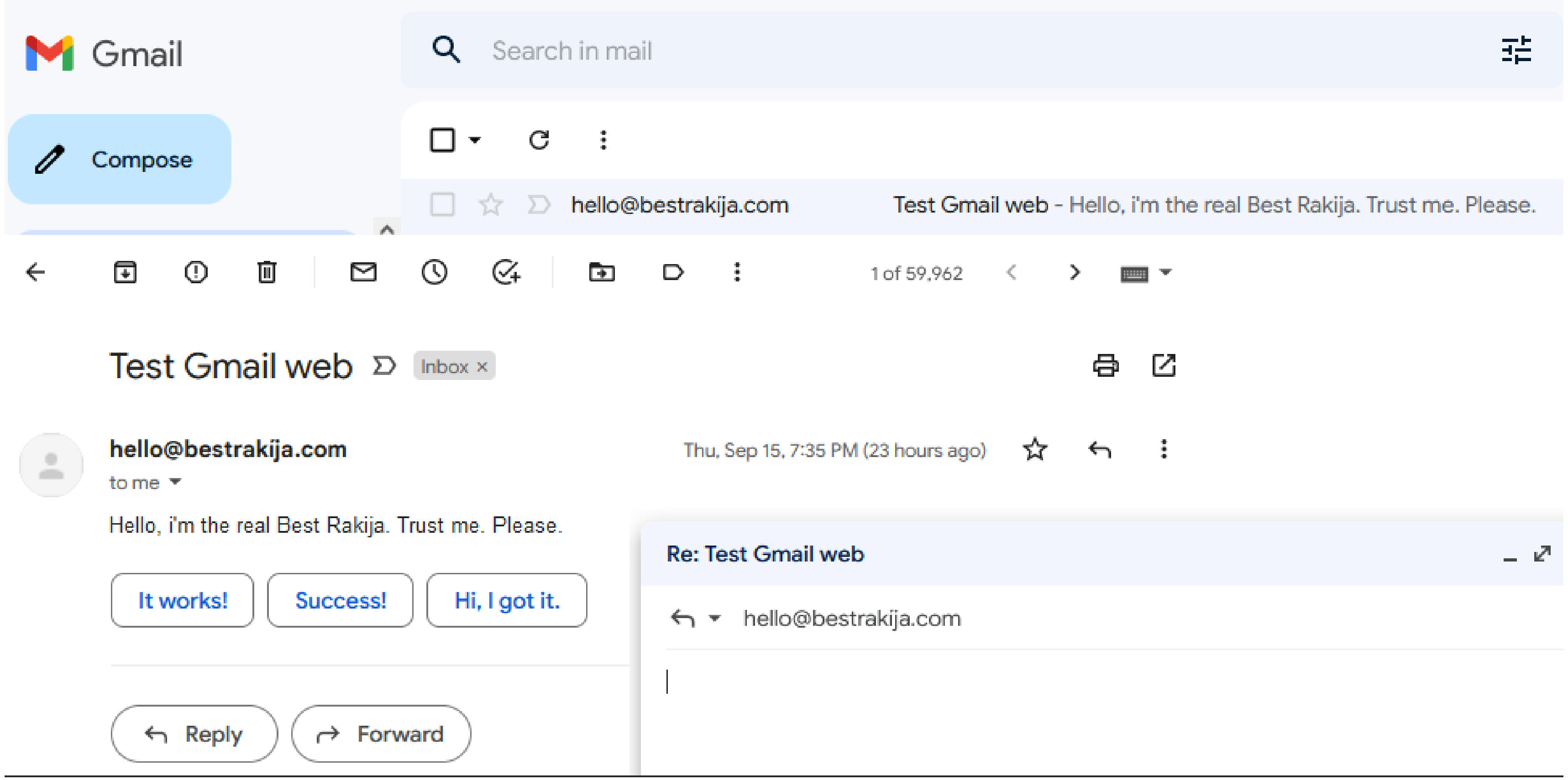
De Maxence Mohr alias fladnaG <pro@fladnag.net>

A hello@bestrakíja.com

Re: Test Canary Email

"hello@bestrakíja.com" hello@bestrakíja.com – 16 septembre 2022 19:11
> Hello, i'm the real Best Rakija. Trust me. Please.

bestrakíja.com in Gmail webmail



hello@bestrakija.com Test Gmail web - Hello, i'm the real Best Rakija. Trust me. Please.

Test Gmail web Inbox ×

hello@bestrakija.com
to me

Thu, Sep 15, 7:35 PM (23 hours ago)

Hello, i'm the real Best Rakija. Trust me. Please.

Re: Test Gmail web

hello@bestrakija.com

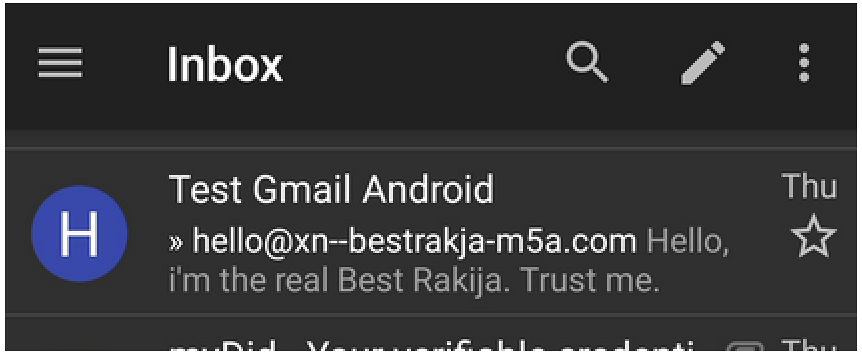
Preview

Reading

Replying

bestrakíja.com in K9-Mail

Preview



Test Gmail Android

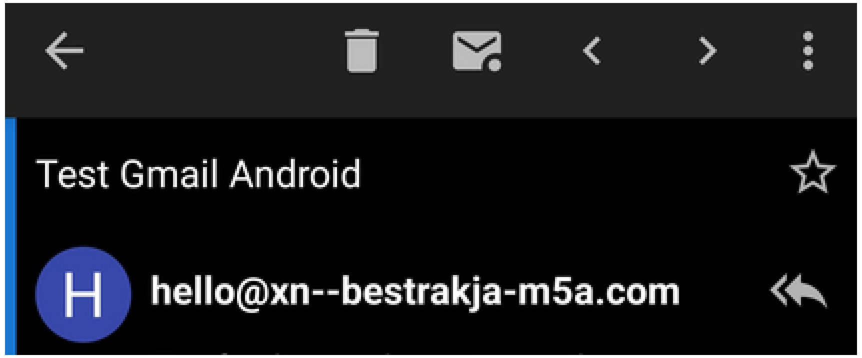
» hello@xn--bestrakja-m5a.com Hello, i'm the real Best Rakija. Trust me.

Thu

myDid - Your verifiable credenti

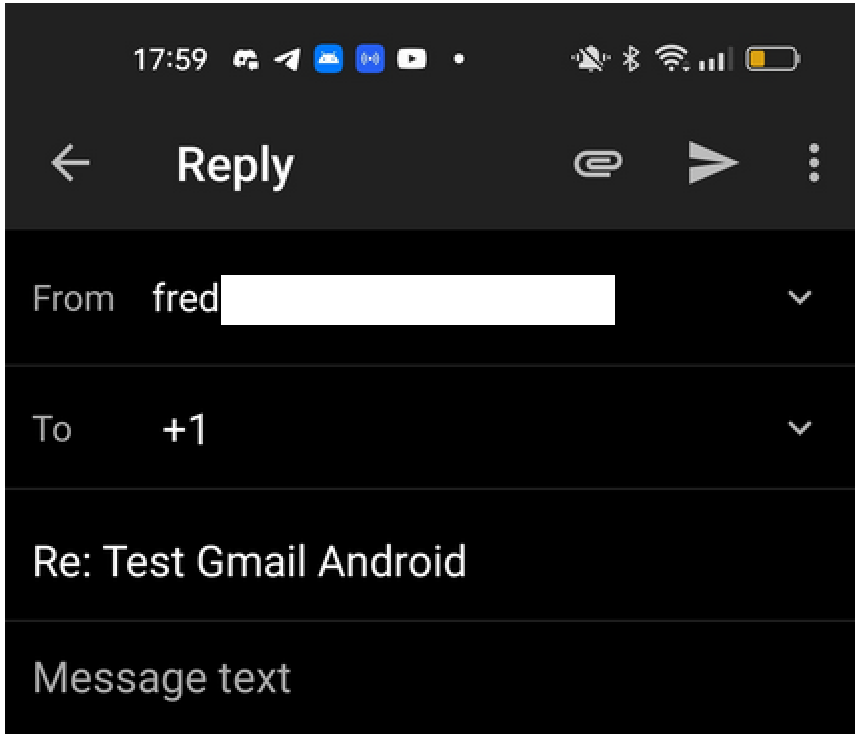
Thu

Reading



Test Gmail Android

hello@xn--bestrakja-m5a.com



From fred [redacted]

To +1

Re: Test Gmail Android

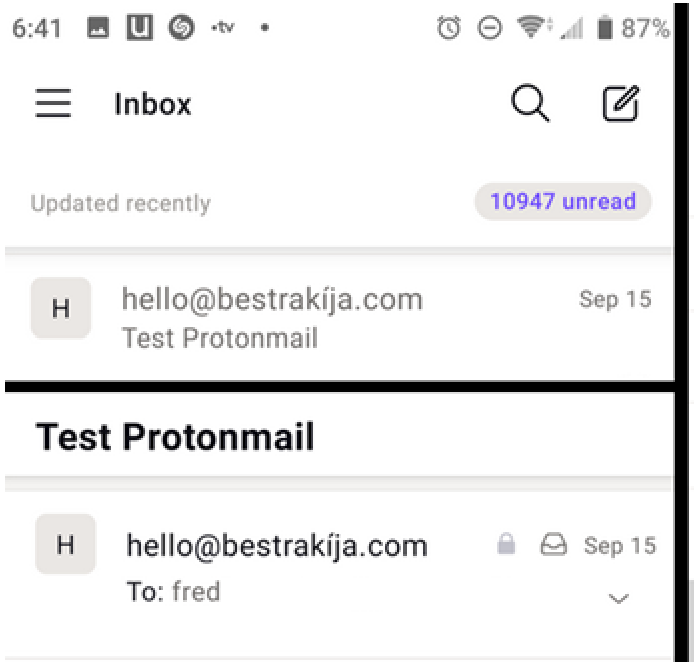
Message text

Replying

bestrakíja.com in Protonmail mobile app

Preview

Reading



6:41 87%

Inbox

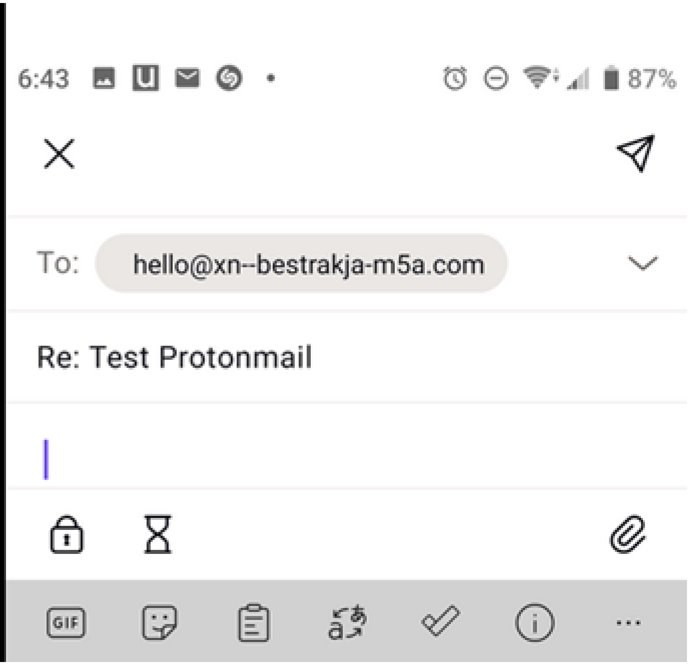
Updated recently 10947 unread

H hello@bestrakíja.com Sep 15
Test Protonmail

Test Protonmail

H hello@bestrakíja.com Sep 15
To: fred

Replying



6:43 87%

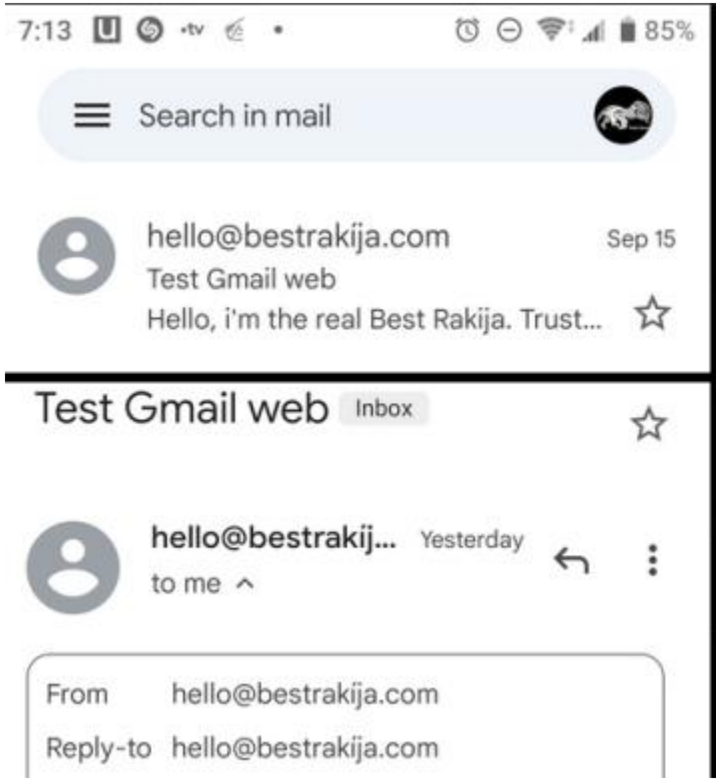
To: hello@xn--bestrakja-m5a.com

Re: Test Protonmail

bestrakíja.com in Gmail app

Preview

Reading



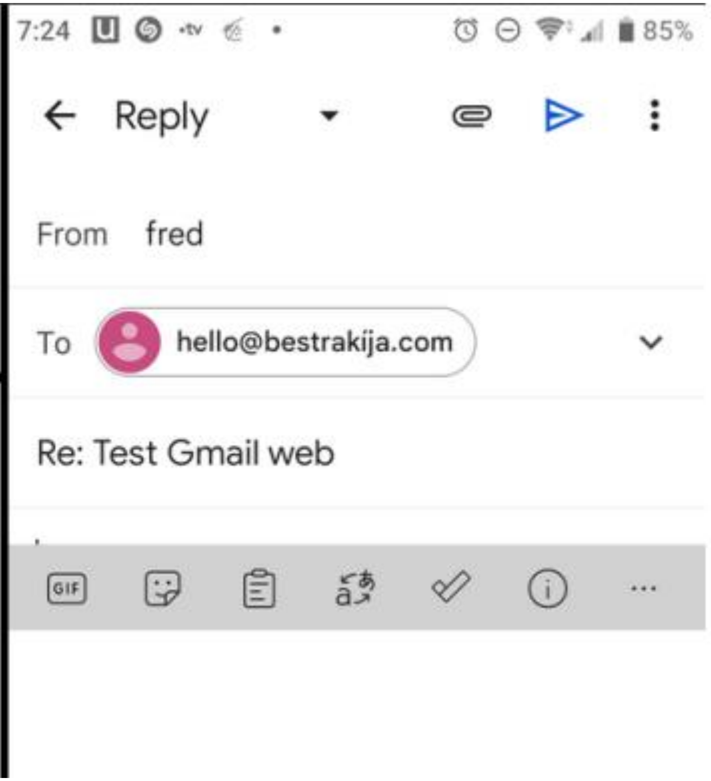
7:13 85%

hello@bestrakija.com Sep 15
Test Gmail web
Hello, i'm the real Best Rakija. Trust...

Test Gmail web

hello@bestrakij... Yesterday
to me

From hello@bestrakija.com
Reply-to hello@bestrakija.com



7:24 85%

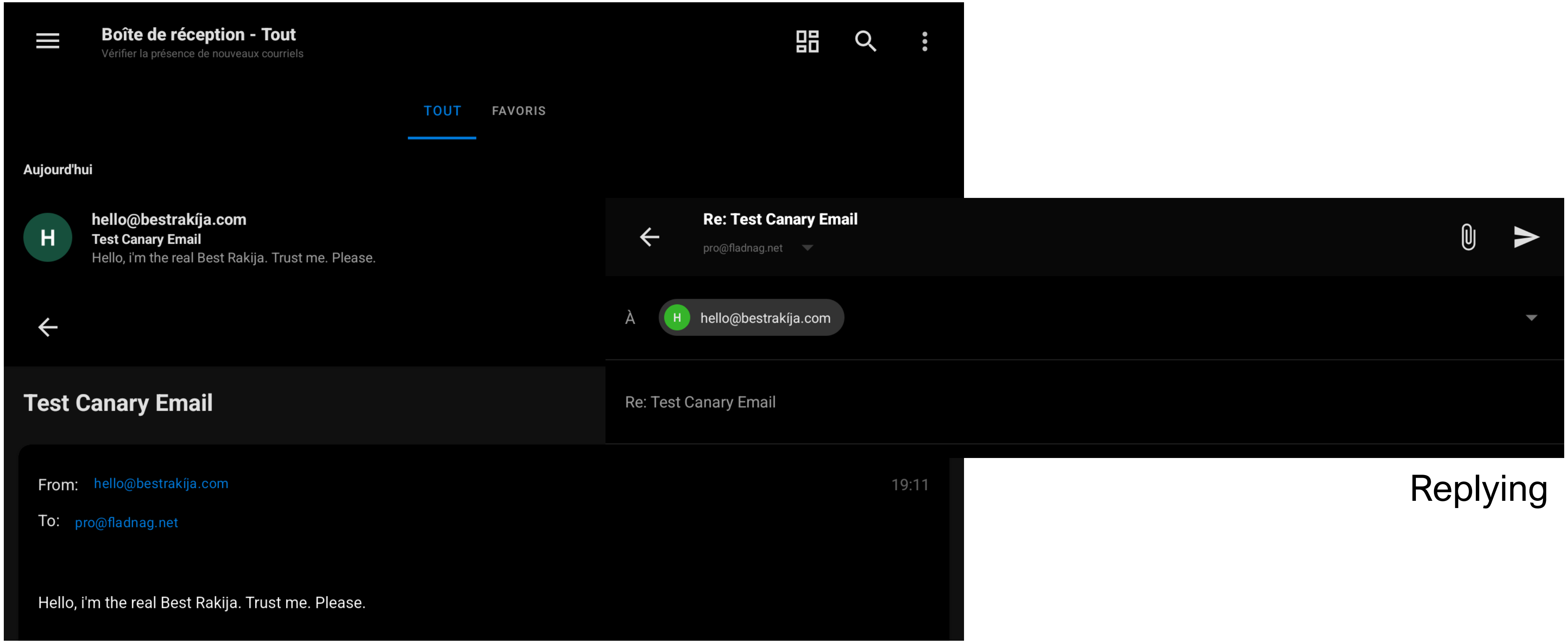
From fred

To hello@bestrakija.com

Re: Test Gmail web

Replying

bestrakíja.com in Canary Android



Preview

Reading

Replying

Boîte de réception - Tout

Vérifier la présence de nouveaux courriels

Aujourd'hui

hello@bestrakíja.com

Test Canary Email

Hello, i'm the real Best Rakija. Trust me. Please.

Test Canary Email

From: hello@bestrakíja.com 19:11

To: pro@fladnag.net

Hello, i'm the real Best Rakija. Trust me. Please.

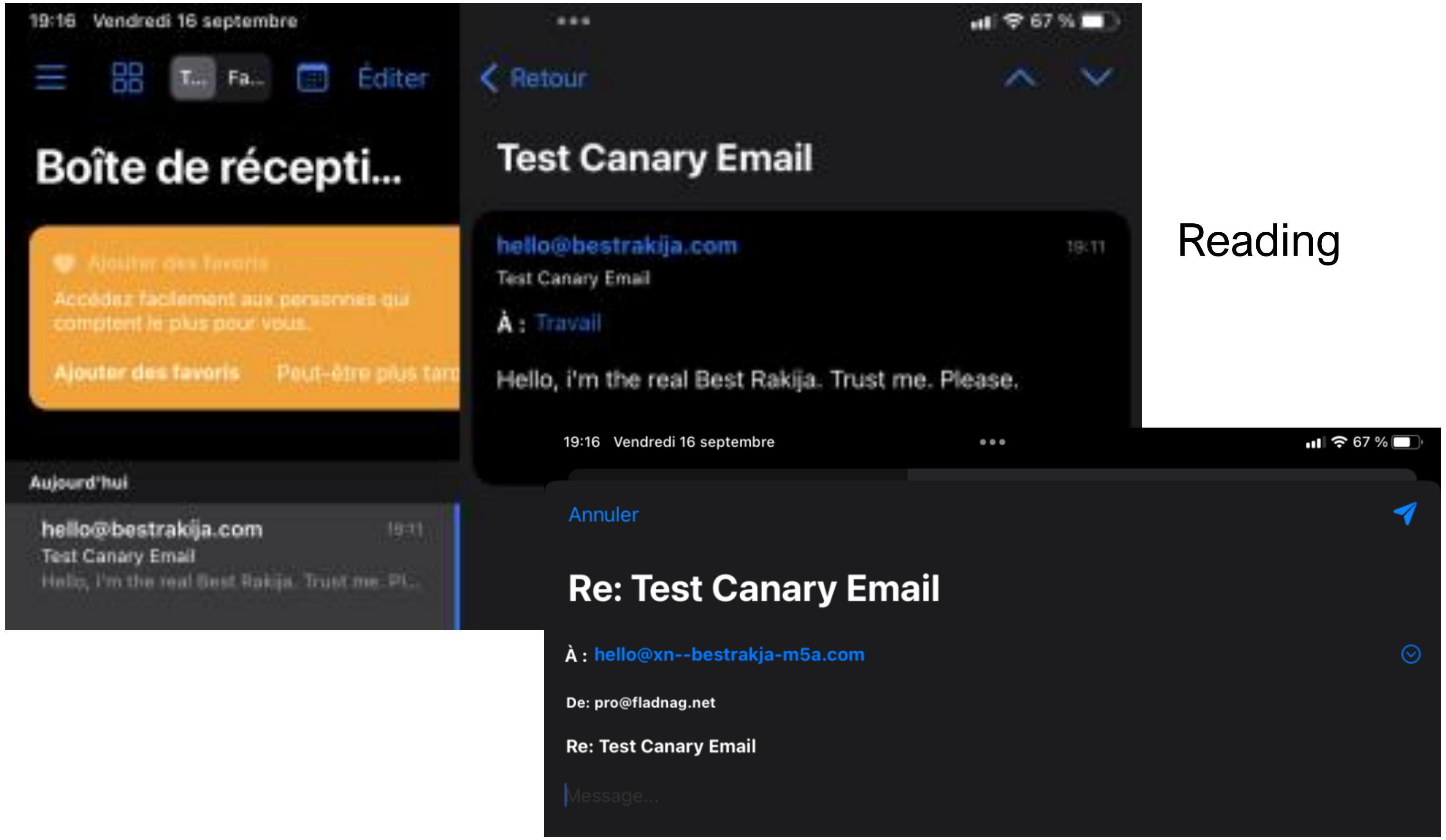
Re: Test Canary Email

pro@fladnag.net

À hello@bestrakíja.com

Re: Test Canary Email

bestrakíja.com in Canary iOS



19:16 Vendredi 16 septembre

Éditer

Boîte de récepti...

Ajouter des favoris

Accédez facilement aux personnes qui comptent le plus pour vous.

Ajouter des favoris Peut-être plus tard

Aujourd'hui

hello@bestrakíja.com 19:11
Test Canary Email
Hello, i'm the real Best Rakija. Trust me. Pl...

Retour

67 %

Test Canary Email

hello@bestrakíja.com 19:11
Test Canary Email
À : Travail

Hello, i'm the real Best Rakija. Trust me. Please.

19:16 Vendredi 16 septembre 67 %

Annuler

Re: Test Canary Email

À : hello@xn--bestrakja-m5a.com

De: pro@fladnag.net

Re: Test Canary Email

Message...

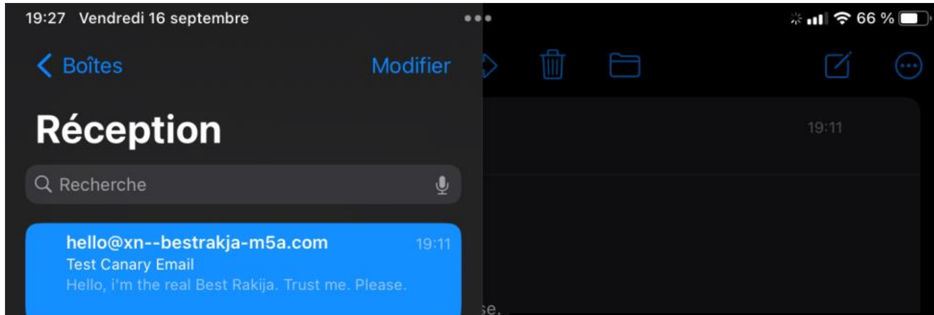
Reading

Preview

Replying

bestrakíja.com in Apple Mail iOS

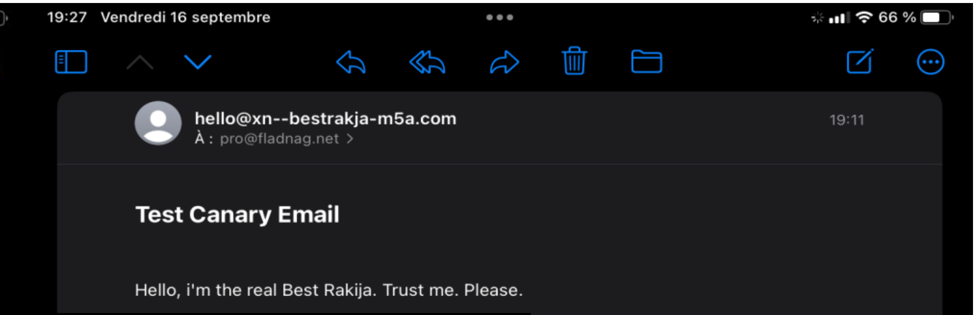
Preview



Réception

Recherche

hello@xn--bestrakja-m5a.com 19:11
Test Canary Email
Hello, i'm the real Best Rakija. Trust me. Please.

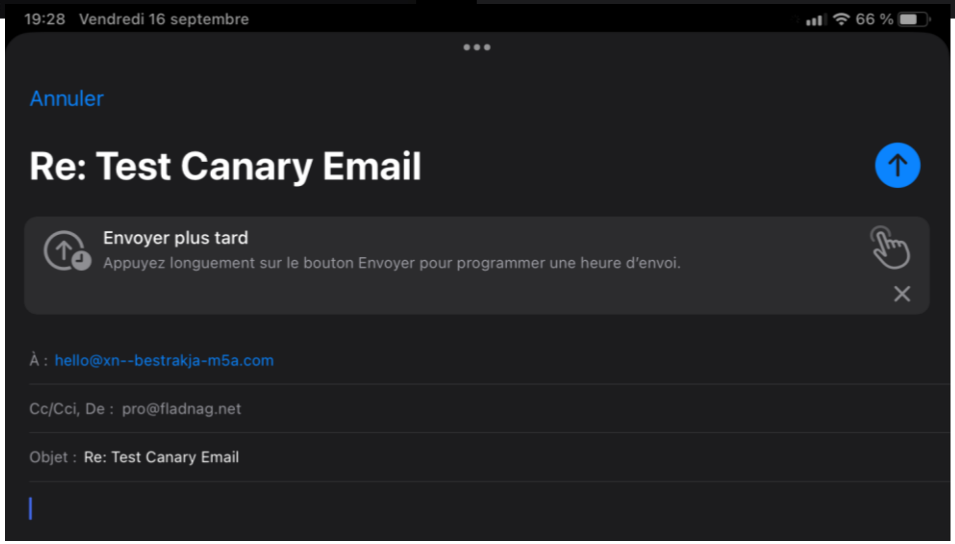


hello@xn--bestrakja-m5a.com 19:11
À : pro@fladnag.net

Test Canary Email

Hello, i'm the real Best Rakija. Trust me. Please.

Reading



Re: Test Canary Email

Envoyer plus tard
Appuyez longuement sur le bouton Envoyer pour programmer une heure d'envoi.

À : hello@xn--bestrakja-m5a.com

Cc/Cci, De : pro@fladnag.net

Objet : Re: Test Canary Email

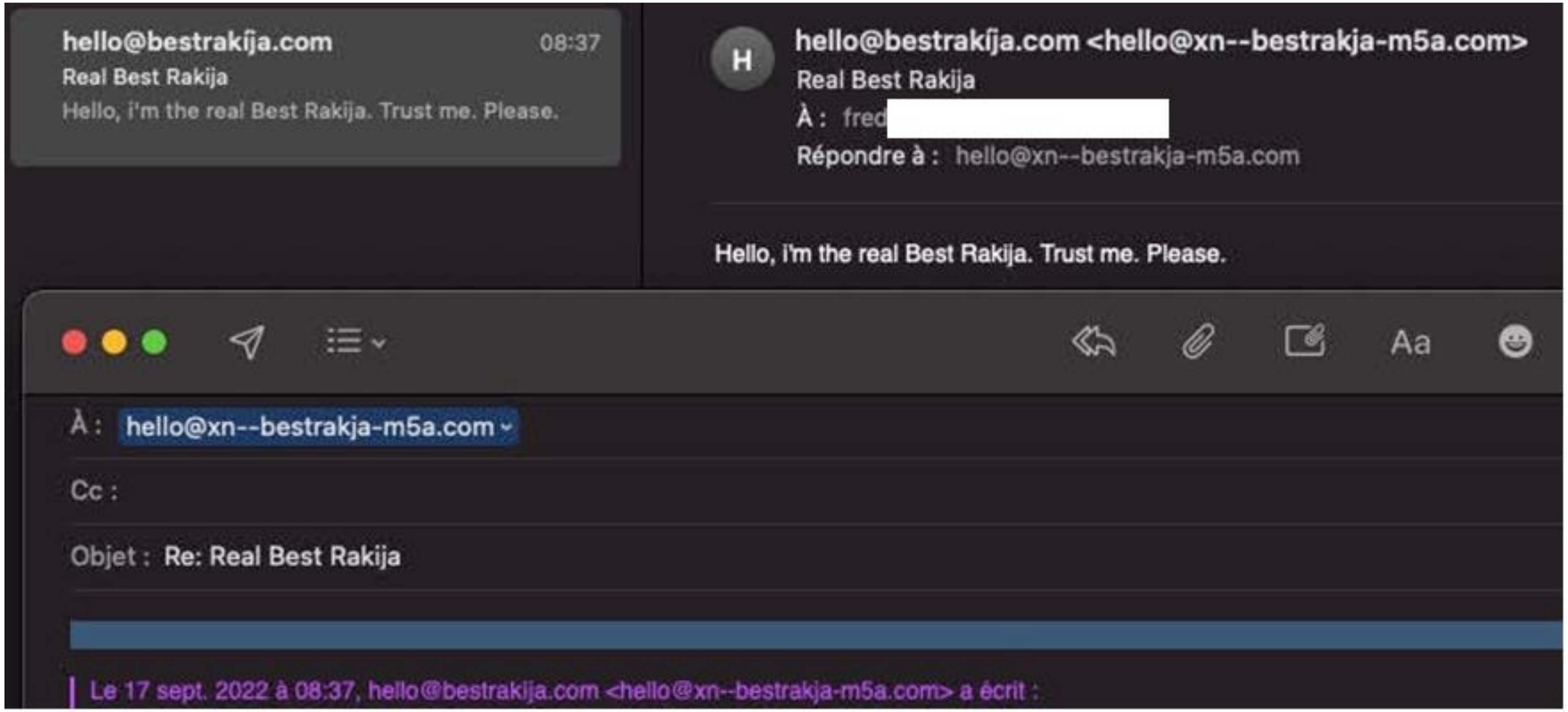
Replying

bestrakíja.com in Apple Mail macOS

Preview

Reading

Replying



hello@bestrakíja.com 08:37
Real Best Rakija
Hello, i'm the real Best Rakija. Trust me. Please.

hello@bestrakíja.com <hello@xn--bestrakja-m5a.com>
Real Best Rakija
À : fred[redacted]
Répondre à : hello@xn--bestrakja-m5a.com

Hello, i'm the real Best Rakija. Trust me. Please.

À : hello@xn--bestrakja-m5a.com
Cc :
Objet : Re: Real Best Rakija

Le 17 sept. 2022 à 08:37, hello@bestrakíja.com <hello@xn--bestrakja-m5a.com> a écrit :

Webmails - conclusion

	Preview	Reading details	Replying
SOGo (no punycode implemented?) @shiva2.inverse 202201181158	☑	☑	☑
Office 365	✕	☑	☑
Tutanota	✕	☑	☑
Protonmail	✕	☑	☑
Mailfence	✕	☑	☑
Skiff	✕	✕	✕
Roundcube	✕	✕	✕
Nextcloud Mail app	✕	✕	✕
Gmail	✕ ✕	✕ ✕	✕ ✕

Desktop mail clients - conclusion

	Preview	Reading details	Replying
Thunderbird	☑	☑	☑
Apple Mail macOS	✕	☑	☑
Windows 10 Mail	✕	☑	☑
Outlook	✕	✕	✕

Mobile mail clients - conclusion

	Preview	Reading details	Replying
Apple Mail iOS	☑	☑	☑
K9	☑	☑	—
Proton	✕	✕	☑
Canary iOS	✕	✕	☑
Canary Android	✕	✕	✕
Gmail Android	✕ ✕	✕ ✕	✕ ✕

How to patch/protecc/prevent?

Client side protection

In browsers

- Firefox, Chrome, Safari, Internet Explorer all have some kind of protection. For some domains or for some alphabets that should not be mixed, they show the raw URI, not the Unicode one. It is not perfect. At all.
- Browsers extensions will show you phishing attempts with homograph attacks if the domain name is well known. But some extensions are better than others…

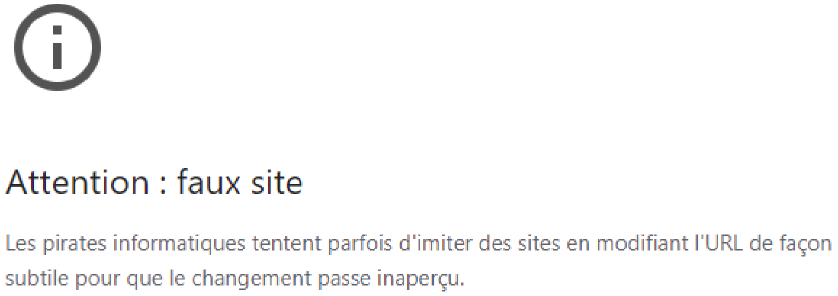
In mail clients

- A lot of mail clients don’t care about punycode. Or does stupid things (hello |\/|1cr0$0f7).

Problem

- Depends on the user…
- And require sensibilizing users, right now before its too late.

Client side protection



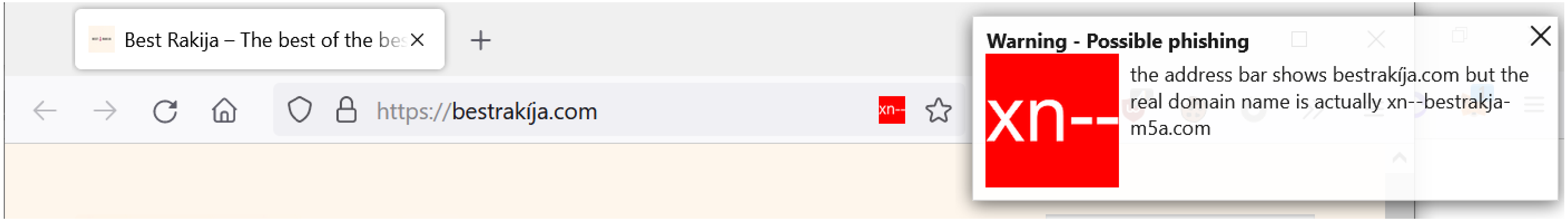
Attention : faux site

Les pirates informatiques tentent parfois d'imiter des sites en modifiant l'URL de façon subtile pour que le changement passe inaperçu.

Chrome – Avast

- Looks like a browser error.
- Clear message.

Client side protection



Warning - Possible phishing

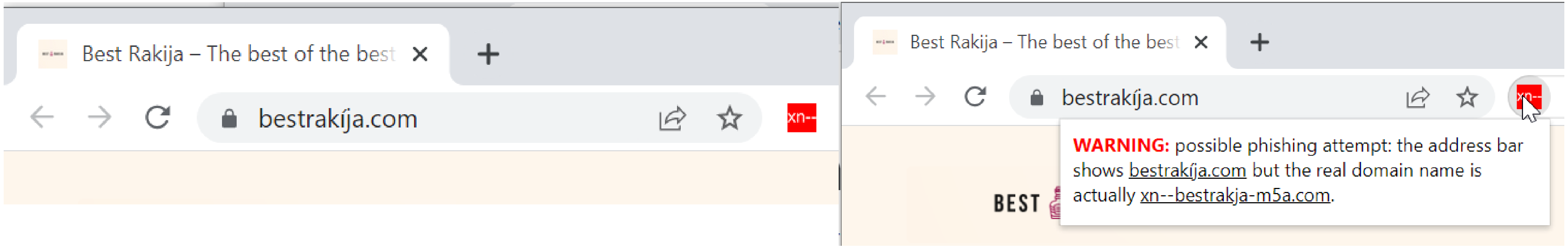
xn--

the address bar shows bestrakíja.com but the real domain name is actually xn--bestrakja-m5a.com

Firefox – PunyCode Domain Detector

- Red square in address bar
- Big unmissable and clear pop-up

Client side protection

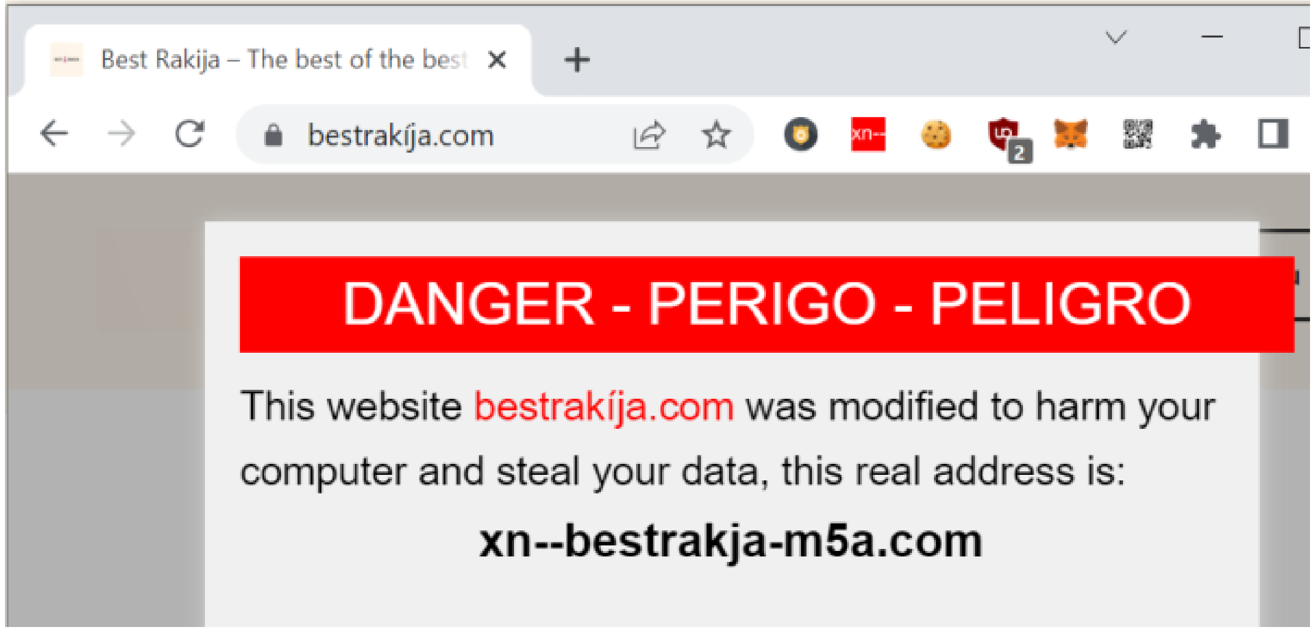

Best Rakija – The best of the best
bestrakíja.com
xn--
Best Rakija – The best of the best
bestrakíja.com
xn--
BEST

WARNING: possible phishing attempt: the address bar shows bestrakíja.com but the real domain name is actually xn--bestrakja-m5a.com.

Chrome – PunyCode Domain Detector

- Red square in address bar, you have to click on it to see details..
- Not enough for people to understand
- A LOT WORSE than the same Firefox version…

Client side protection



Best Rakija – The best of the best

bestrakíja.com

DANGER - PERIGO - PELIGRO

This website bestrakíja.com was modified to harm your computer and steal your data, this real address is:

xn--bestrakja-m5a.com

Chrome – Punyfix

- You CAN'T miss the banner ;)
- The tab is automatically closed in 10 seconds.
- A bit hardcore, but it works®.

Registry side protection

TLD

- ccTLDs should only accept correct alphabets for the country, not more than that.
    - Just like .рф only allowing cyrillic alphabet, not more.
    - AFNIC is doing a good job for that, it is really limiting the possibilities for attackers.
- Maybe some alphabets mixing cloud be banned, as not compatible with each other. But it may not protect from all homograph attacks…

Problem

- For some TLDs, it’s a bit late.
  And they are too permissive with allowed Unicode chars.

Domain owner side protection

Monitoring, monitoring, monitoring

- Some python scripts try to search for known domain names close to yours:
  - Github: `dnstwist`
  - Github: `urlcrazy`
- You can also pay a private company for this service:
  - like Nameshield (not linked or affiliated),
  - OVH (not linked or affiliated),
  - or WhoisXMLAPI (not linked or affiliated).

Problem

- Everybody monitors, right?

Laws and international cooperation

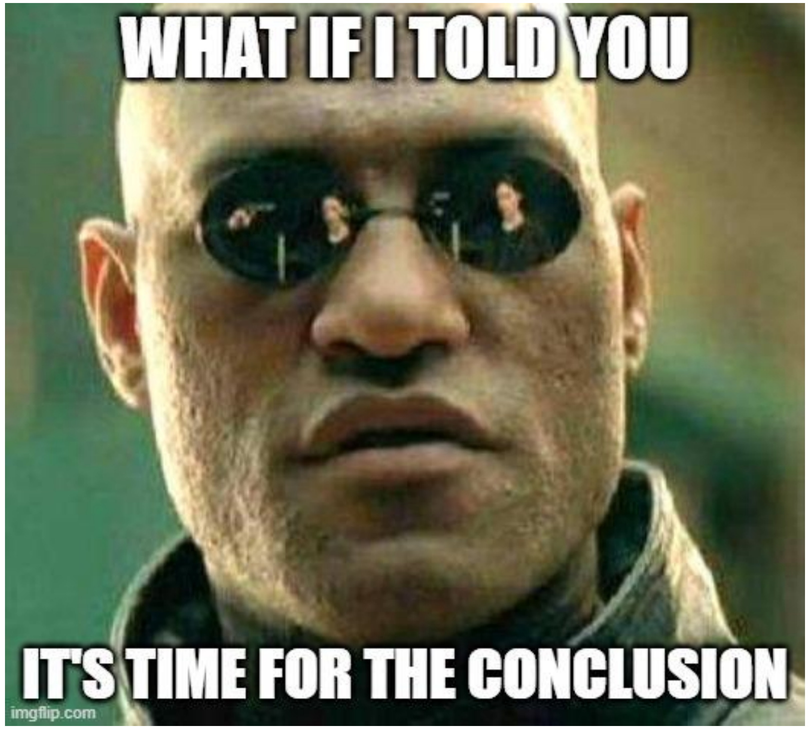
On a national level

- National laws should prevent malicious IDN homograph attacks.
  - But still allow exceptions, like parody, right to inform, etc. where applicable.

About international cooperation

- We are all in this together, so we shall unite.
  - Europe may be about to lift GDPR restrictions on Domain Name Whois for example, may be a great start for us, ITSec people to track down illegal use and report them to authorities…
- Spread the word, people!

Conclusion



Conclusion

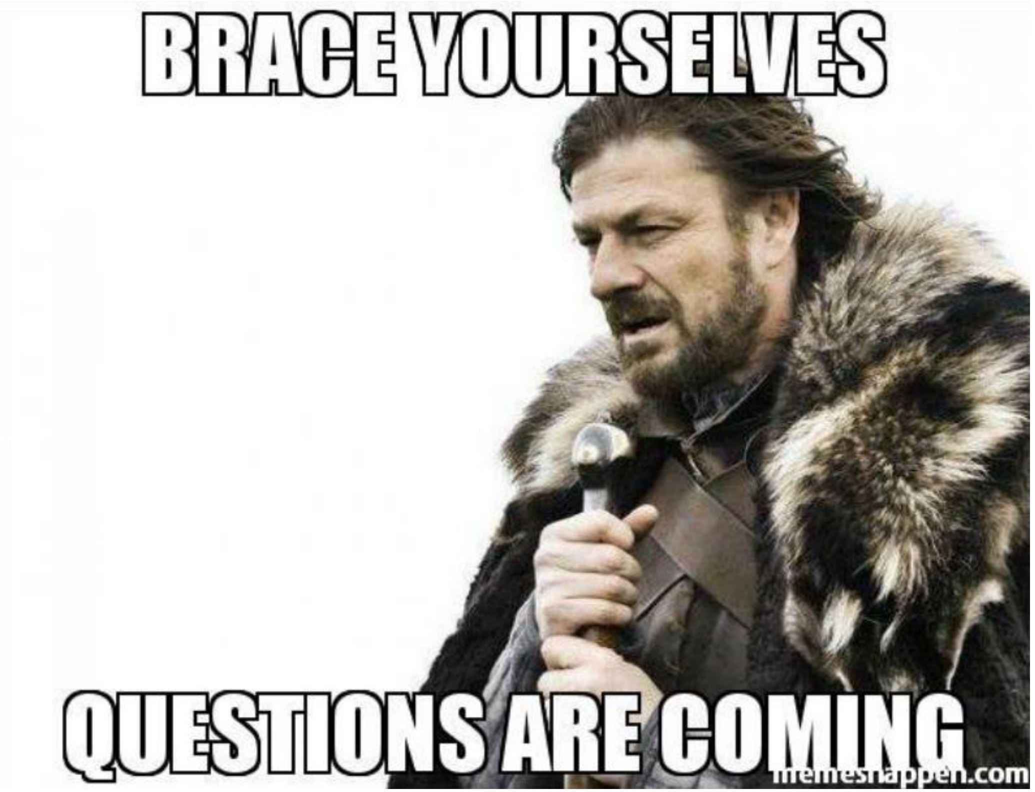
It’s time to spread the word.

- Please spread the word around you, to warn people about this technique, and protection via browser plug-ins.
- I bet a rakija bottle that in no more than 5 years, these kind of attacks will be prevalent. Let’s be ready.

Special thanks to:

- *BalCCon orga team*: you’re the best 💖
- *Fred Crypto* and *jusk*: for the bad and good advices ;)
- *You*, for listening to me talking :D

Question time…?



These slides are now available on fladnaG.net 😋

This is the end. See you at the bar 🙄

IDNs and its possible bad uses

fladnaG (Max) French independent Pentester/Sysadmin BalCCon 2k22

@fladna9 on Twitter pro@fladnag.net