

# DNS-PROJECT COMPETITION

Joint Initiative of NASSCOM CoE— IoT & AI and ICANN



## TEAM NETWORK

### TEAM MEMBERS :

FARHAN P MOHAMMED ([19epci019@skcet.ac.in](mailto:19epci019@skcet.ac.in))  
ALEN MORRES ([19epci004@skcet.ac.in](mailto:19epci004@skcet.ac.in))  
KEERTHI T M ([19epci017@skcet.ac.in](mailto:19epci017@skcet.ac.in))  
III M.Tech CSE

### TEAM MENTOR:

Ms. V.R.AZHAGURAMYAA, ME.,(Ph.D)  
([azhaguramyaa@skcet.ac.in](mailto:azhaguramyaa@skcet.ac.in))  
Assistant Professor / CSE



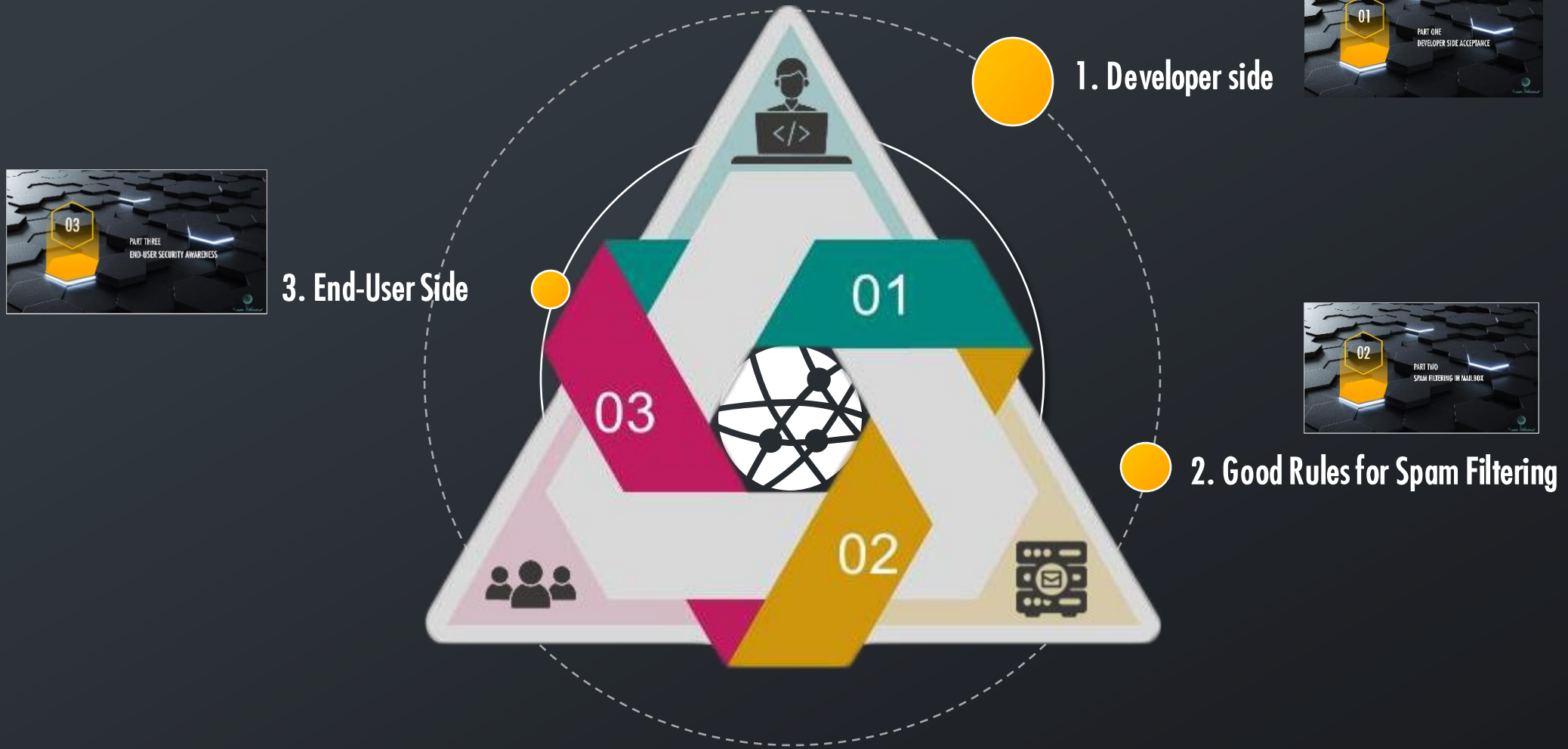
**SRI KRISHNA**  
COLLEGE OF ENGINEERING AND TECHNOLOGY  
An Autonomous Institution, Accredited by NAAC with 'A' Grade.



Team Network

# ADDRESSING PROBLEMS

We have identified and classified the problem statements in these three categories



# • CHALLENGES IN WEB-FORMS •

- Web development languages use outdated identifiers for validation.
- Developers use regex from open-source code repositories for their websites.
- Regex deployed, show no commonality in terms of validating email.

## JAVASCRIPT

JavaScript regular expression:

(Eg.) : `result=str.match(/^ w+((- w+)(. w+))*@[A-Za-z0-9]+((.|-)((com)|(net)|(cn))+)$/)`

## HTML 5

HTML input type="email">

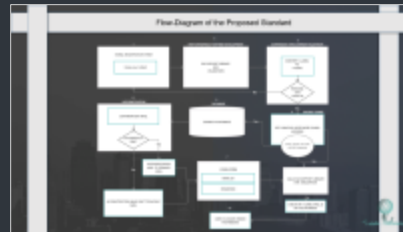
(Eg.) : `<input autocomplete="on" class="form-control input-xxlarge input-validation-error" data-val="true" data-val-maxlength="Email address must be under 256 characters." data-val-maxlength-max="255" data-val-regex="Email does not appear to be a valid format." data-val-regex-pattern="^[w-]{1,}@([da-zA-Z-]{1,}){1,}[da-zA-Z-]{2,3}$" data-val-required="Please enter your email address." id="Email" maxlength="255" name="Email" placeholder="Enter your e-mail address" title="Please enter your e-mail address (required)" type="text" value="">`



# PROPOSED APPROACH

- Our approach is to develop a standard client side library, that will accept email in all the categories listed below.

- `ascii@ascii.newshort`
- `ascii@ascii.newlong`
- `ascii@idn.ascii`
- `unicode@ascii.ascii`
- `unicode@idn.idn`
- `arabic.arabic@arabic (RTL)`

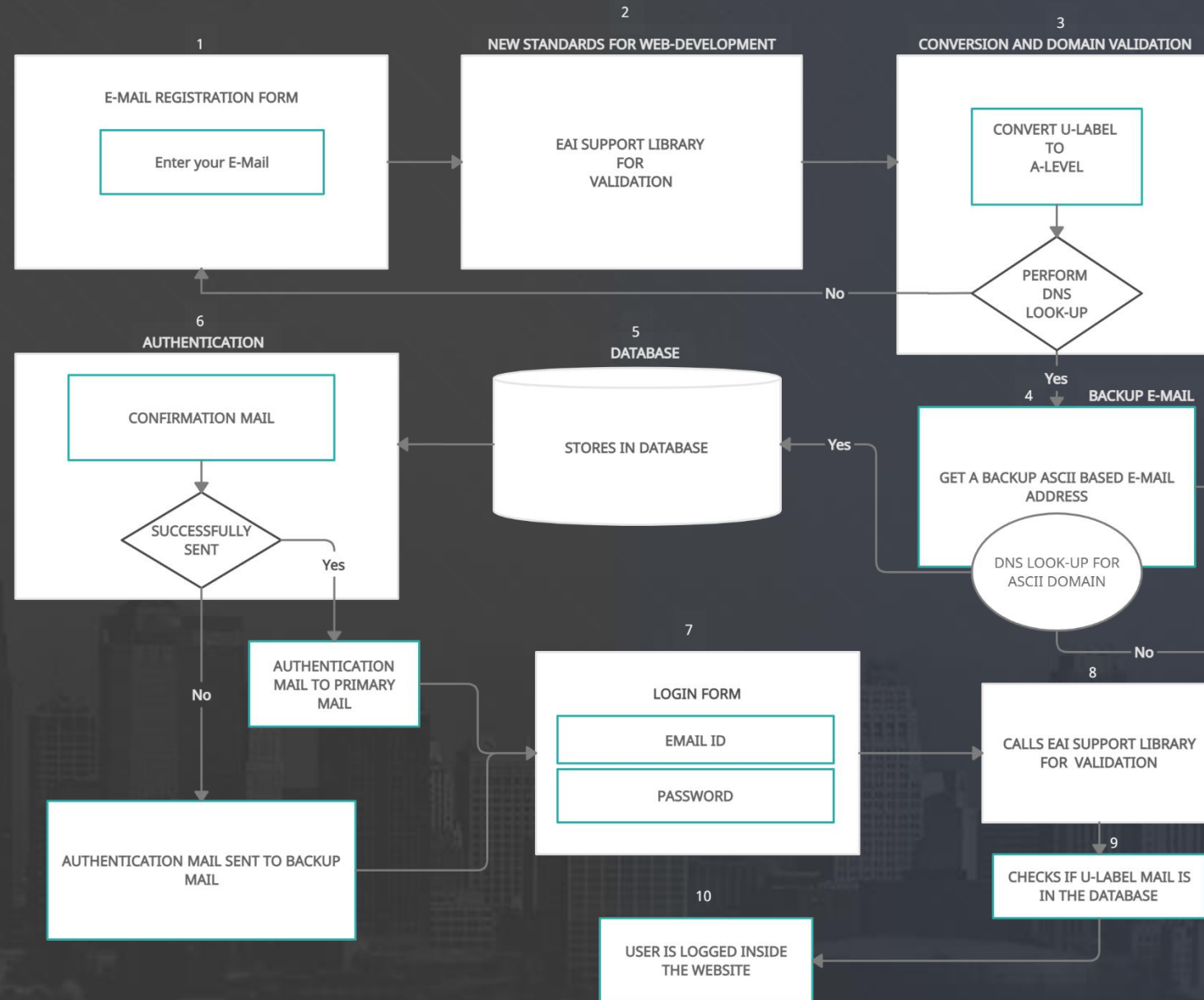


Note : `ascii@ascii.idn` was dropped from the test case due to lack of support for that format.

Ref [UASG25](#)



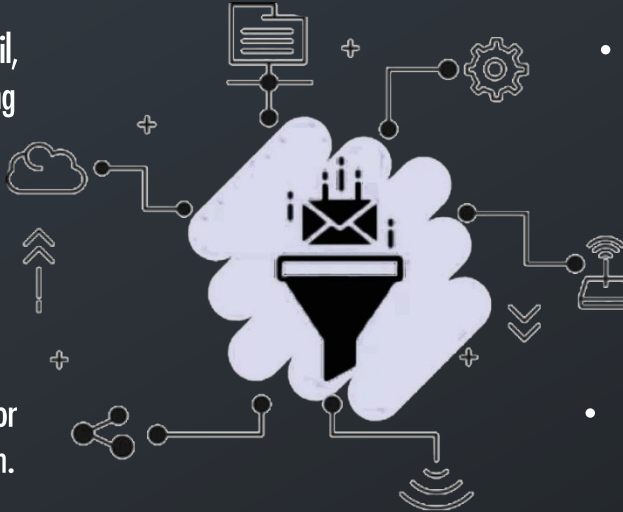
# Flow-Diagram of the Proposed Standard



# SPAM FILTERING

SPAM RULES FOR SYSTEM ADMINISTRATORS AND USERS

- Keep an address book for EAI with a backup ASCII mail, At admin level to allow those mails without any filtering inside the private network.



- It is advised not to look-up the header of an E-Mail for non-ASCII characters and filter it or label it as spam. Instead content filtering should be promoted.

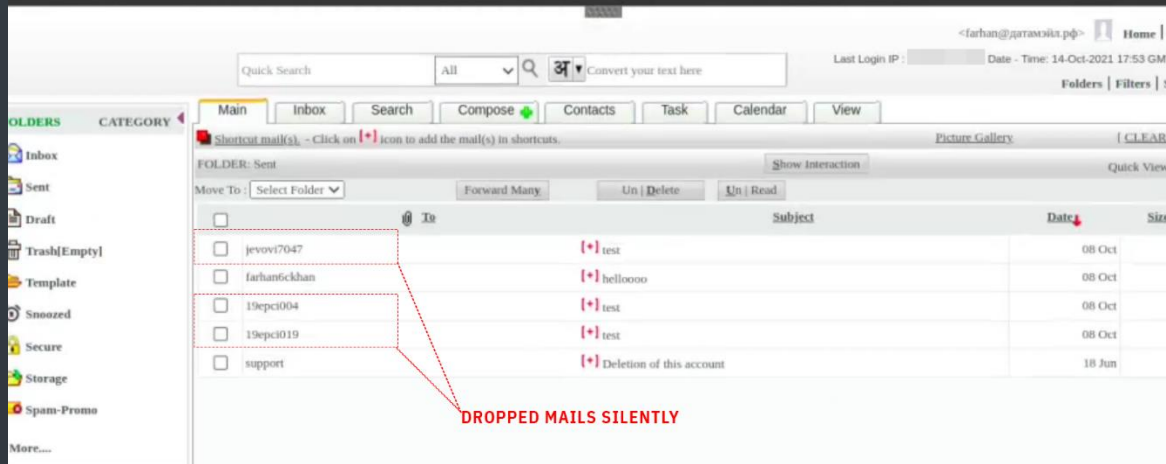
- If EAI is received from an unknown sender, put it in an entirely separate spam folder and inform the recipient of the mail.

- If the recipient of the mail recognizes that the mail address is legitimate, Add that EAI to the address book with backup ASCII mail.

## Test Case

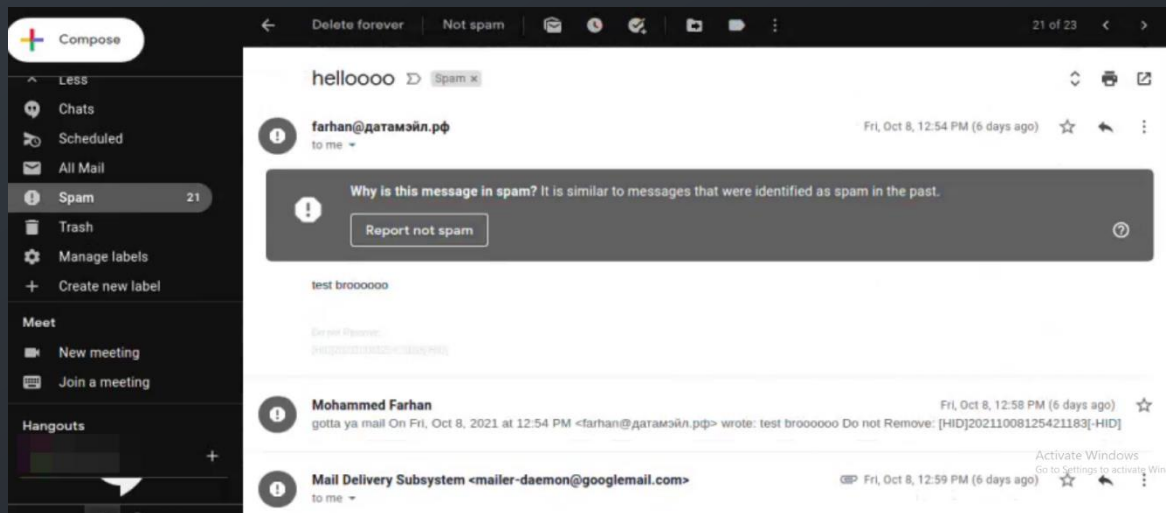


# TEST CASE



SENDER

- To test, four emails were sent, three of which were dropped and one of which was marked as spam.



RECEIVER






# COUNTERMEASURES TO IDN HOMOGRAPH ATTACKS

IDN HOMOGRAPH ATTACKS : Usage of homoglyphs from Unicode characters for spoofing with ASCII identical characters to create phishing domains and end-user confusion.



COUNTERMEASURES TO IDN HOMOGRAPH ATTACKS  
BROWSER SECURITY MECHANISM



When a valid Cyrillic only domain was constructed as example similar to an ASCII domain, Chrome forced it to display in A-label. This restriction will limit UA readability...

Microsoft Firefox also added guards for not performing this forced conversion, instead advising users to double IDN support in their browser settings and advising that such spoofing deeds are the domain registry's responsibility.

COUNTERMEASURES TO IDN HOMOGRAPH ATTACKS  
BROWSER SECURITY MECHANISM

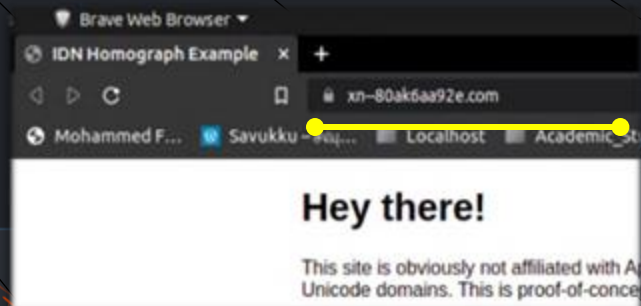
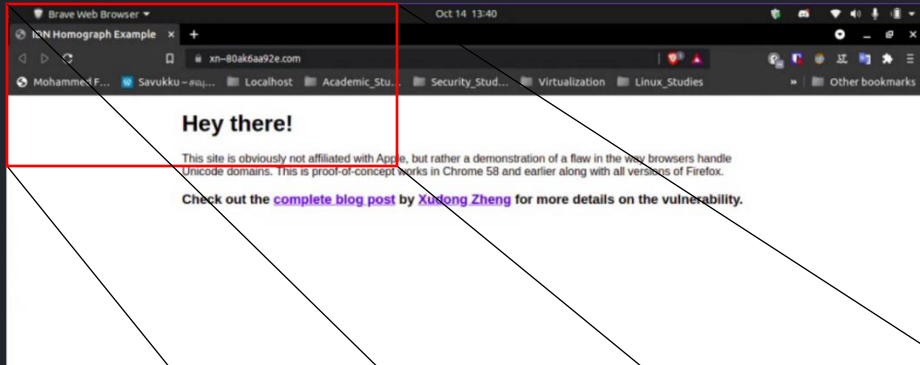


- Browsers show a secure domain with a padlock in the address bar by default.
- We are suggesting browsers to provide an IDN language icon in the address bar, alerting visitors that the website URL contains International characters.
- Browsers can be more considerate on any unwanted discrimination of languages. By using this approach, rather than just forcing valid Unicode domains to be displayed in A-label.

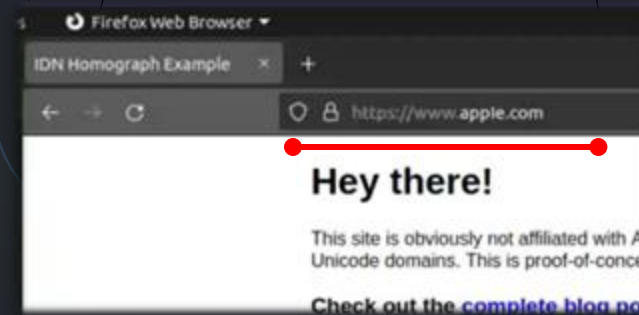
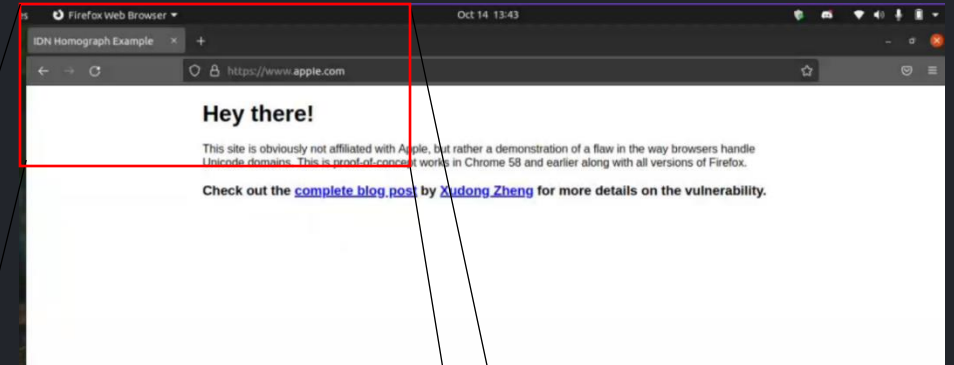


# COUNTERMEASURES TO IDN HOMOGRAPH ATTACKS

## BROWSER SECURITY MECHANISM



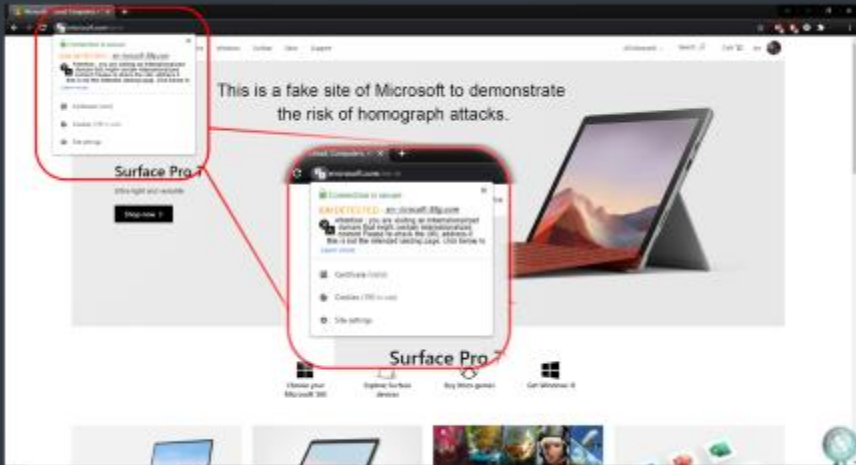
When a valid Cyrillic only domain was constructed as example similar to an ASCII domain, Chrome forced it to display in A-Label. This restriction will limit UA readiness.



Mozilla Firefox cites ethical grounds for not performing this forced conversion, instead advising users to disable IDN support in their browser settings and claiming that such spoofing checks are the domain registry's responsibility.

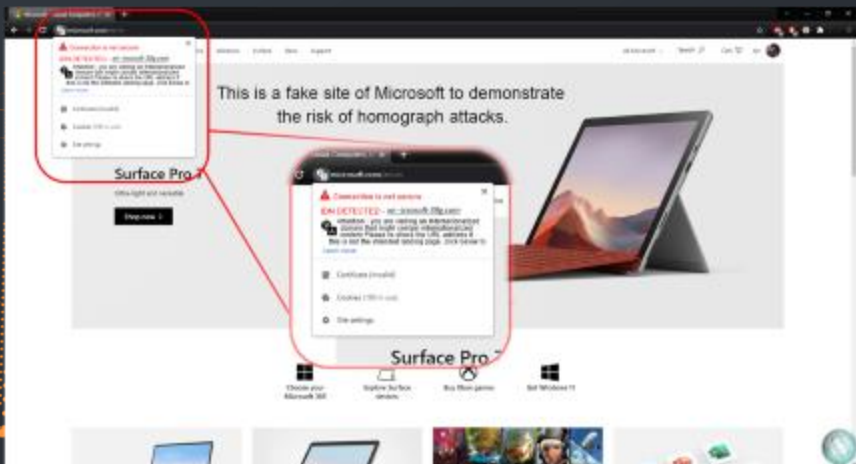
# COUNTERMEASURES TO IDN HOMOGRAPH ATTACKS

## BROWSER SECURITY MECHANISM

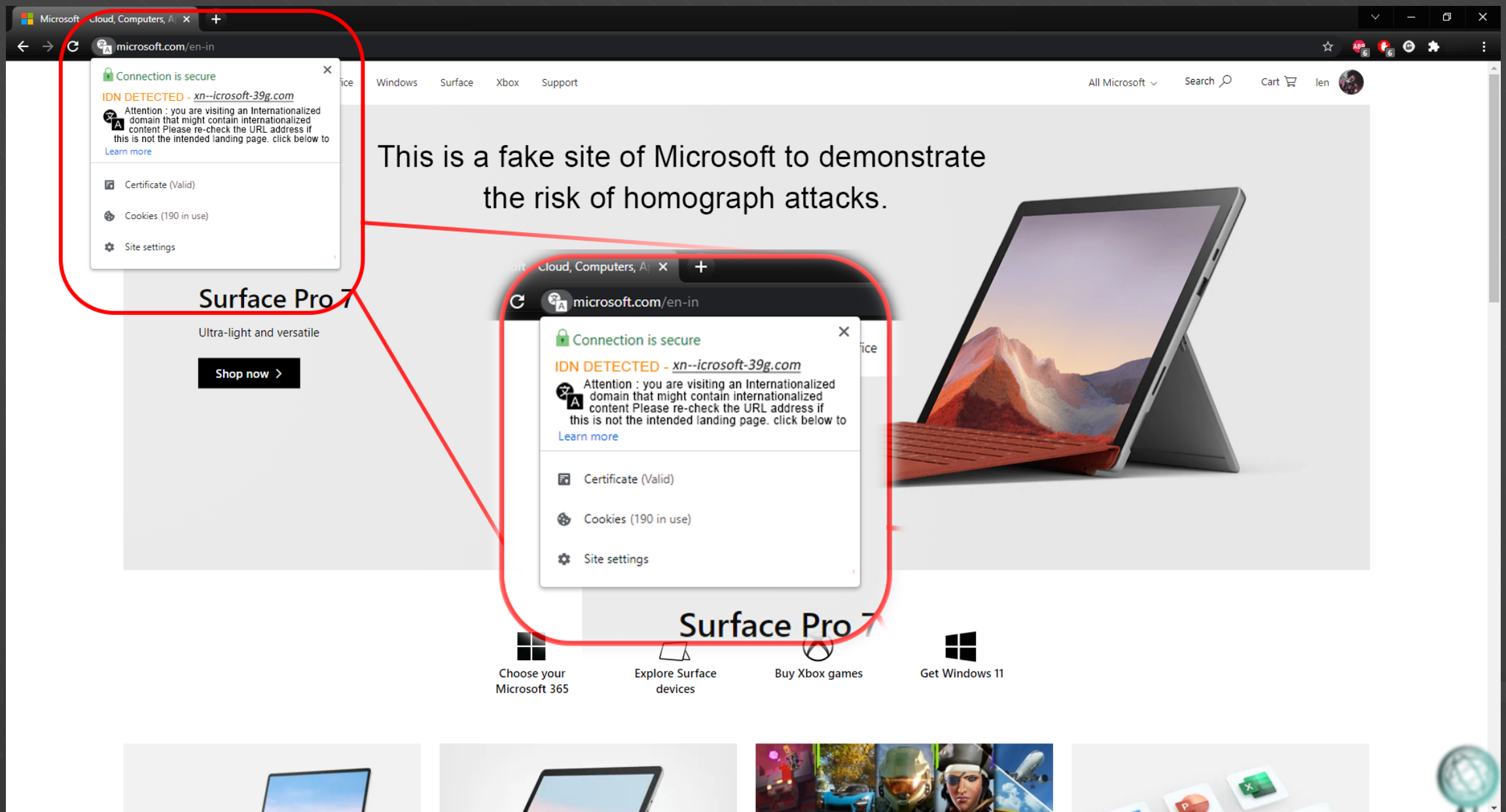


- Browsers show a secure domain with a padlock in the address bar by default.

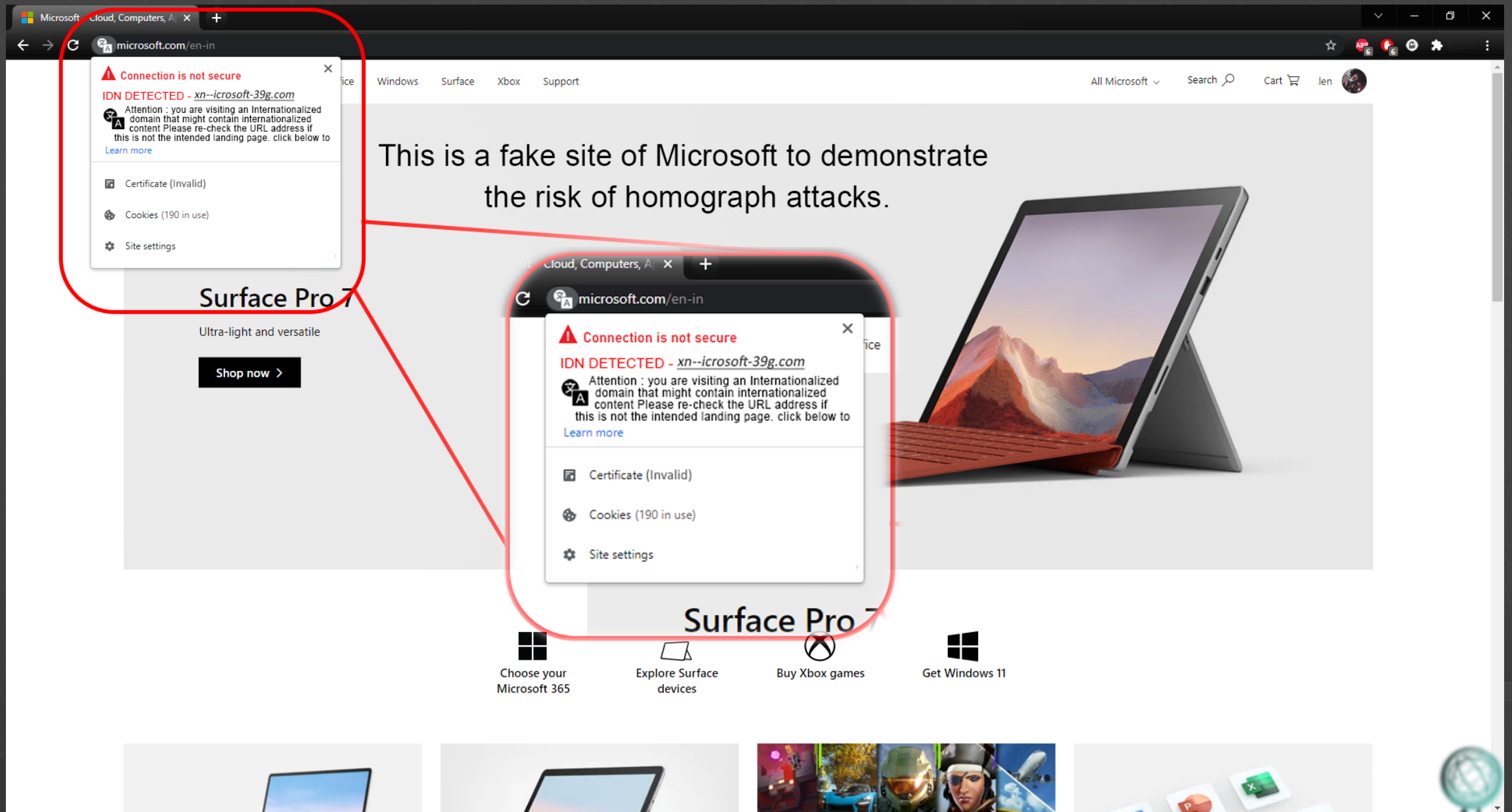
- We are suggesting browsers to provide an IDN language icon in the address bar, alerting visitors that the website URL contains International characters.



- Browsers can be more considerate on any unwanted discrimination of languages, By using this approach, rather than just forcing valid Unicode domains to be displayed in A-label.



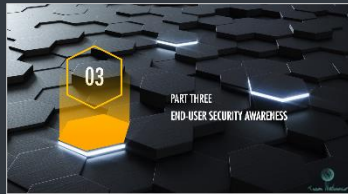
Team Network





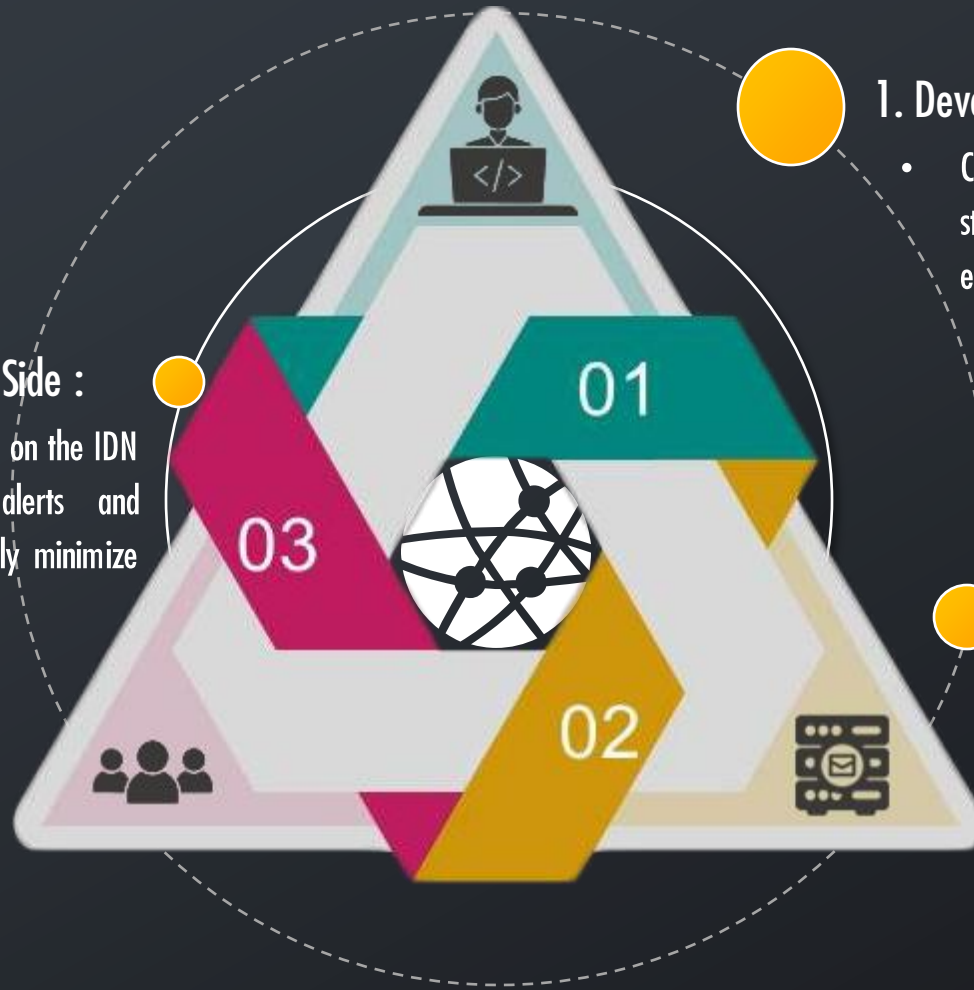
# FUTURE IMPACTS

We have identified and classified the problem statements in these three categories



## 3. End-User Side :

- Relaying information on legitimacy on the IDN website through appropriate alerts and notifications to caution and possibly minimize the risk of homograph attacks.



## 1. Developer side :

- Common library would help developers to use standardised form of REGEX, which makes it easier for validating a genuine e-mail.



## 2. Good Rules for Spam Filtering

- Effective rules for spam filtering of International email addresses in the mailbox would help those mails to be recognized as genuine mail better

# TEAM SKILLSET



## Projects

- Web development
- Tinder Clone
- Amazon clone
- Game development



## Tech Stack

- React-Js, node-Js
- Java Script
- PHP
- HTML
- CSS
- EJB
- SQL
- Python
- C,C++



## Certifications

- Cisco Cybersecurity essentials
- Palo alto network cybersecurity
- Pursuing EJPT from e-learn security and security+ from COMPTIA
- RESTful API with HTTP and JavaScript
- Oracle Cloud Infrastructure Architect Professional certifications
- JavaScript animation for websites



# REFERENCES

Chrome IDN policy :

[https://chromium.googlesource.com/chromium/src/+main/docs/idn.md](https://chromium.googlesource.com/chromium/src/+/main/docs/idn.md)

Chrome Source code for IDN spoof check :

[https://source.chromium.org/chromium/chromium/src/+master:components/url\\_formatter/spoof\\_checks/idn\\_spoof\\_checker.cc;l=422](https://source.chromium.org/chromium/chromium/src/+master:components/url_formatter/spoof_checks/idn_spoof_checker.cc;l=422)

The security researcher who identified this vulnerability :

<https://www.xudongz.com/blog/2017/idn-phishing/>

Bug reports for Mozilla and chrome :

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=1332714](https://bugzilla.mozilla.org/show_bug.cgi?id=1332714)

<https://bugs.chromium.org/p/chromium/issues/detail?id=683314>

Security tool for Homoglyphs :

<https://www.irongeek.com/homoglyph-attack-generator.php?encoded=%E2%80%AE%E2%85%BC&decode=%3C%3C+Decode>

Relevant RFC's :

<https://uasg.tech/wp-content/uploads/documents/UASG006-en-digital.pdf>

UASG reports :

<https://uasg.tech/wp-content/uploads/documents/UASG025-en-digital.pdf>

<https://uasg.tech/wp-content/uploads/documents/UASG017-en-digital.pdf>

# THANK YOU

