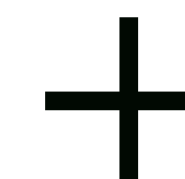


LET'S SPREAD PHISHING AND ESCAPE THE BLOCKLISTS

Tecniche sfruttate dai criminali per protrarre una campagna di phishing



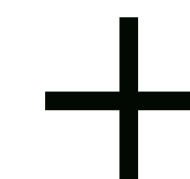
Photo by Nahel Abdul Hadi on Unsplash





Andrea Draghetti

- + Phishing Analysis and Contrast @ D3Lab
- + Python Developer
- + Team Member @ BackBox Linux



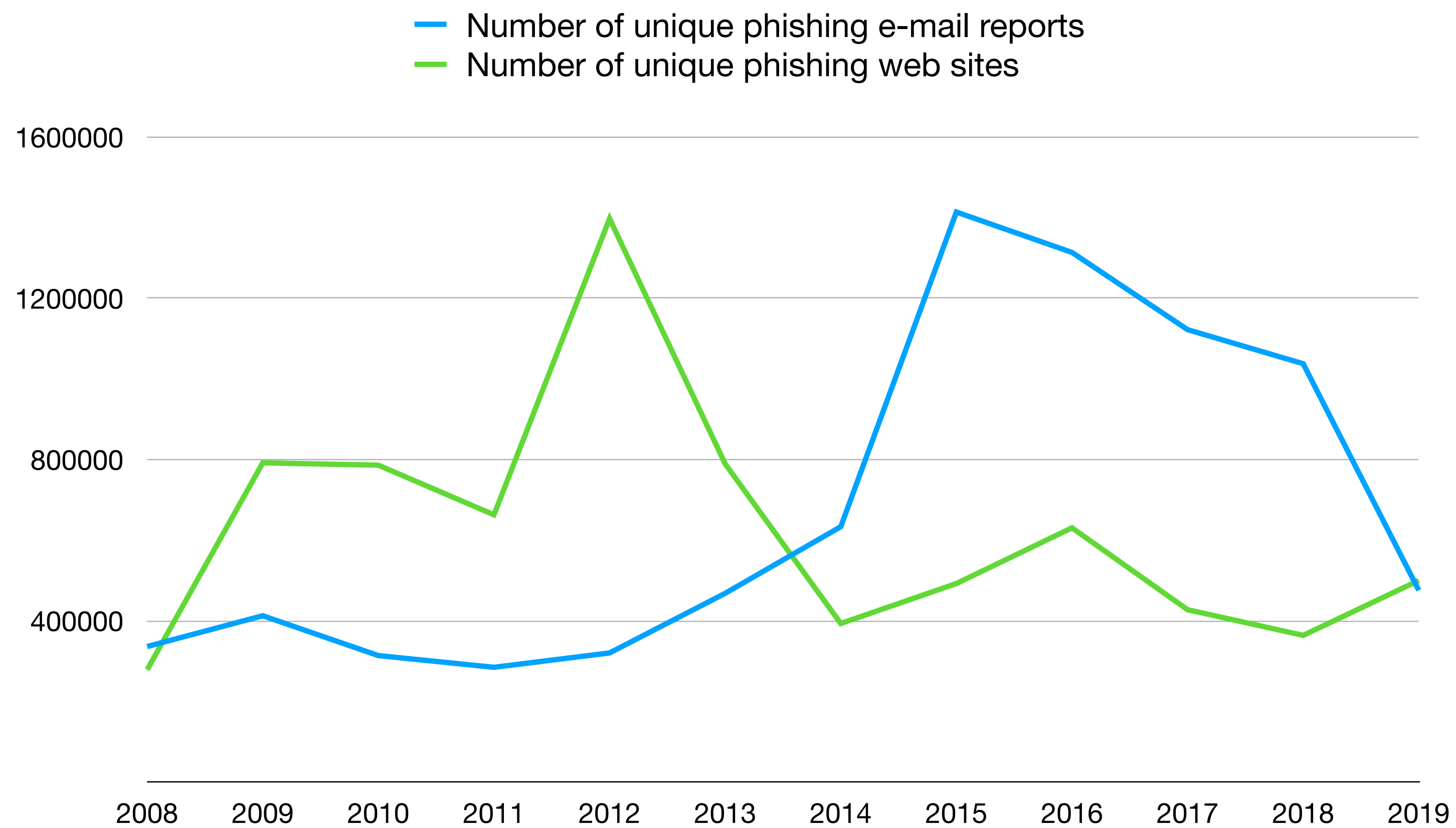
+ PHISHING

Il Phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

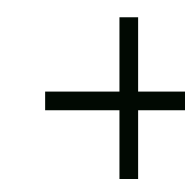
{Wikipedia}



+ STATISTICHE

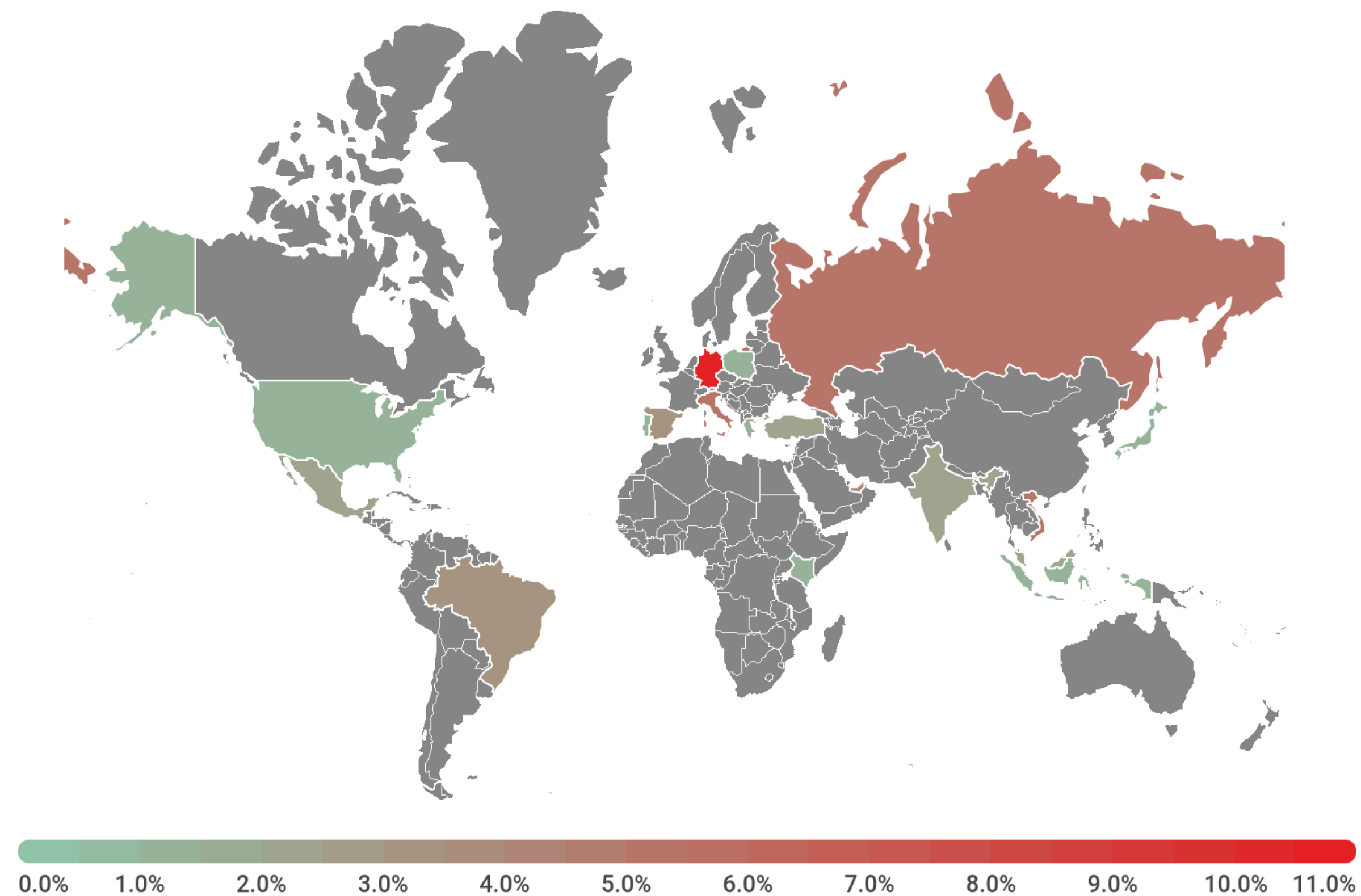


Fonte: Anti-Phishing Working Group

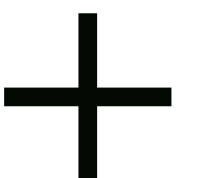


+ STATISTICHE

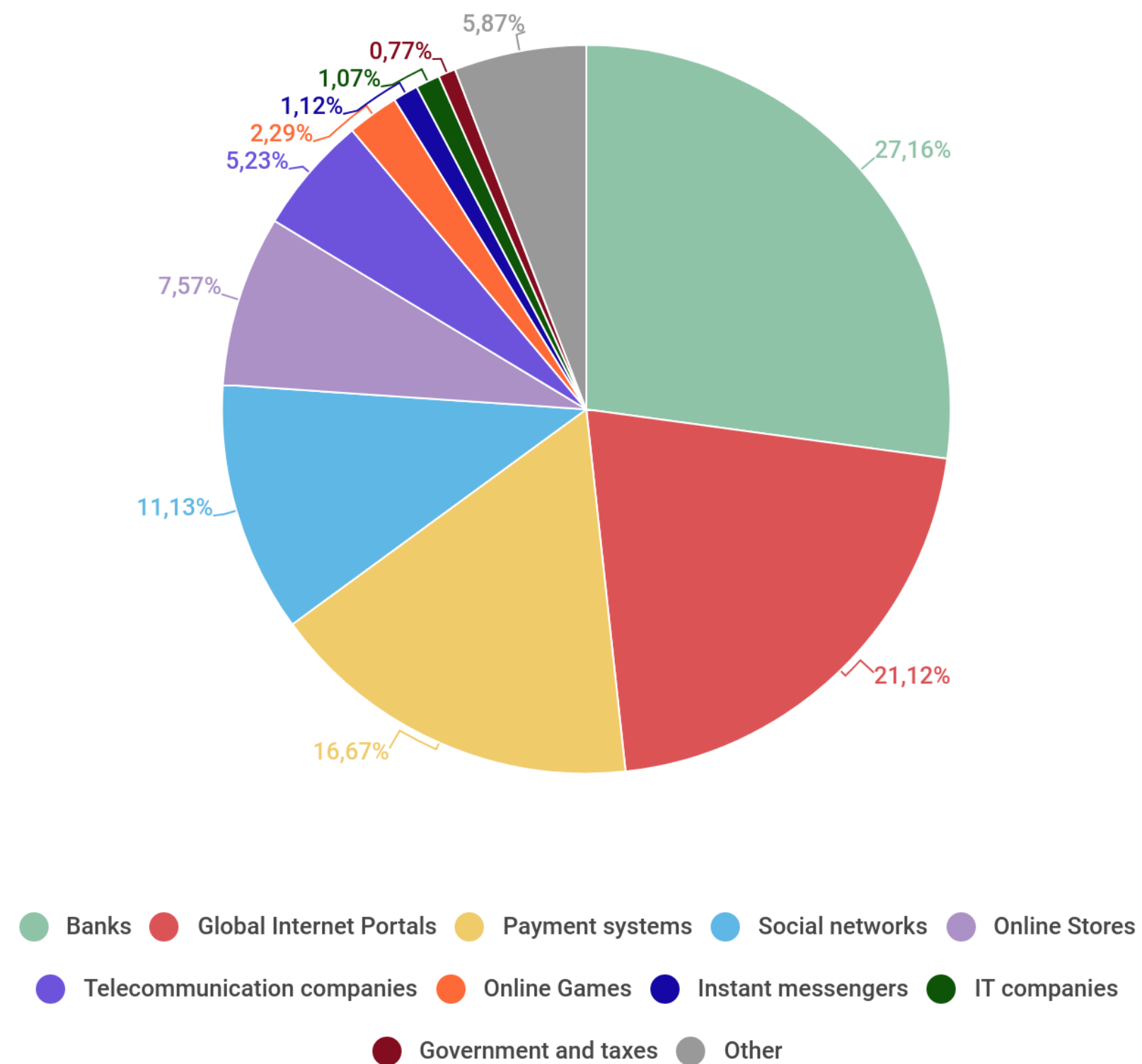
Countries targeted by malicious mailings



Fonte: Securelist

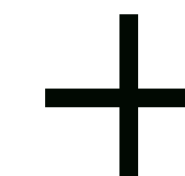
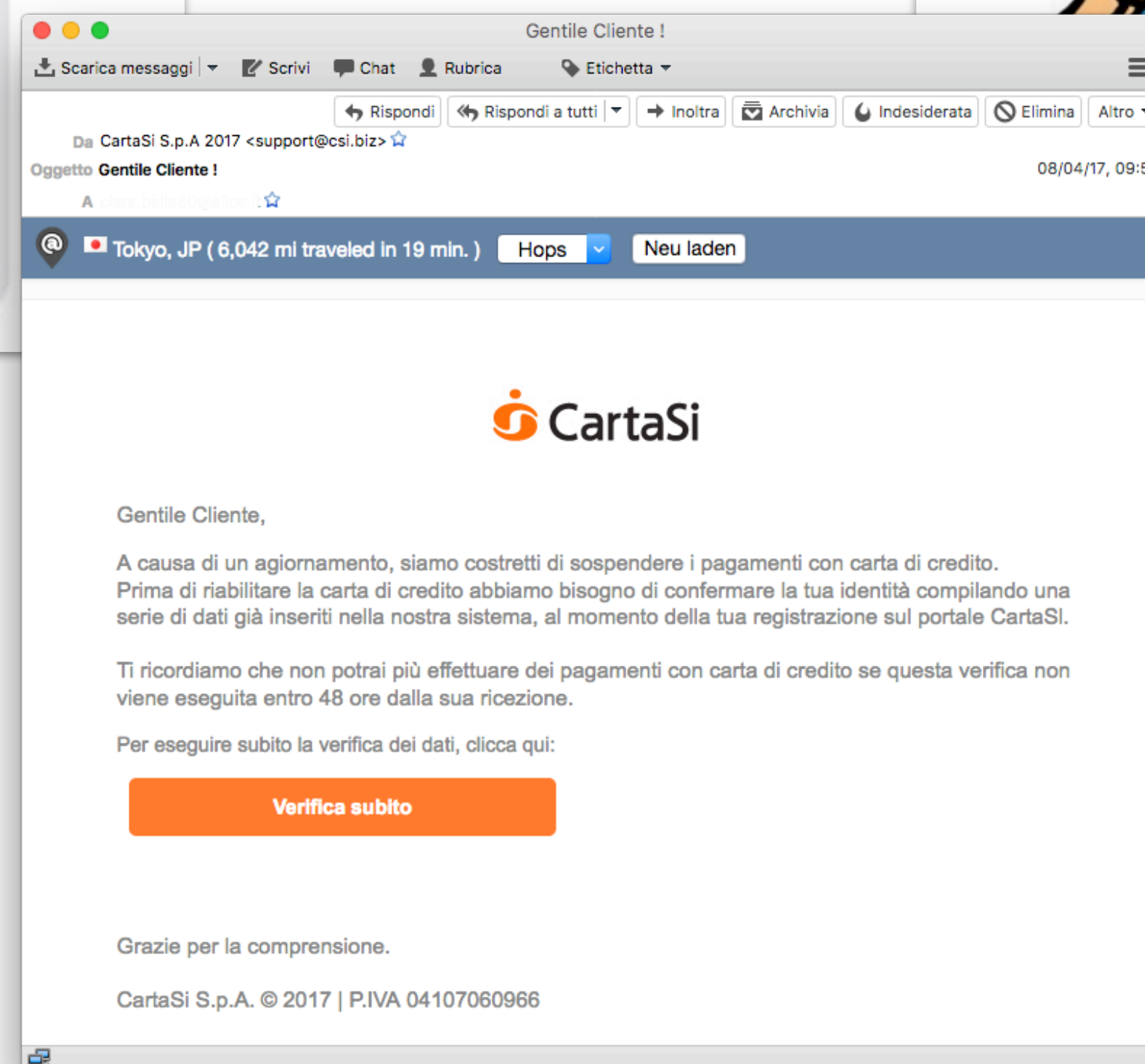


Rating of categories of organizations attacked by phishers



Fonte: Securelist

+ VETTORI: EMAIL, SMISHING, VISHING, ADS, ETC..

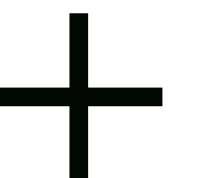


+ CONTRASTO

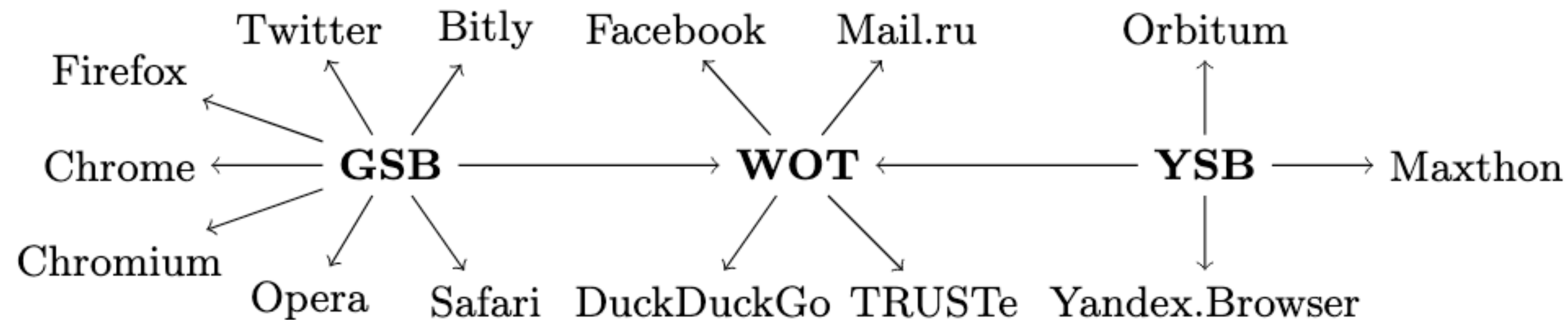
Blocklist



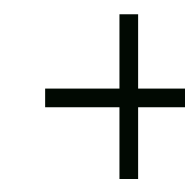
Abuse Team



+ CONTRASTO: BLOCKLIST



Fonte: <https://www.inrialpes.fr/planete/people/amkumar/papers/gsb-security.pdf>



+ CONTRASTO: GOOGLE SAFE BROWSING

Segnalazione di una pagina di phishing


Ti ringraziamo per il tuo contributo al debellamento dei siti di phishing dal Web. Se ritieni di aver trovato una pagina che ne simula un'altra allo scopo di acquisire informazioni personali degli utenti, compila il seguente modulo per segnalare al team per la navigazione sicura di Google.

Quando ci invii siti, alcuni dati dell'account e del sistema vengono inviati a Google. Useremo le informazioni da te inviate per proteggere i prodotti, l'infrastruttura e gli utenti di Google da contenuti potenzialmente dannosi. Se stabiliamo che un sito viola le norme di Google, potremmo aggiornare lo stato del sito nel nostro Rapporto sulla trasparenza, nonché condividere l'URL e il relativo stato con terze parti. Puoi trovare ulteriori informazioni relative al Rapporto sulla trasparenza [qui](#). Le informazioni relative alla tua segnalazione verranno gestite nel rispetto delle [Norme sulla privacy](#) e dei [Termini di servizio](#) di Google.

URL:

☐ Non sono un robot 
reCAPTCHA
Privacy - Termini

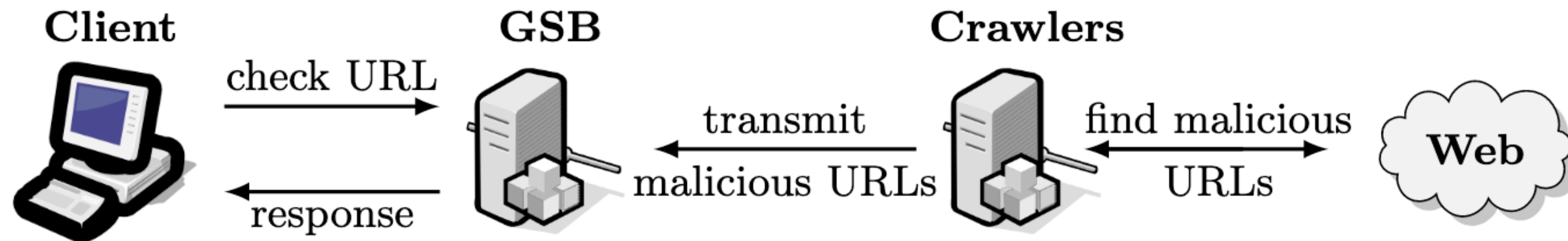
Ulteriori informazioni sulla violazione relativa a phishing:
(Facoltativo)



https://safebrowsing.google.com/safebrowsing/report_phish/



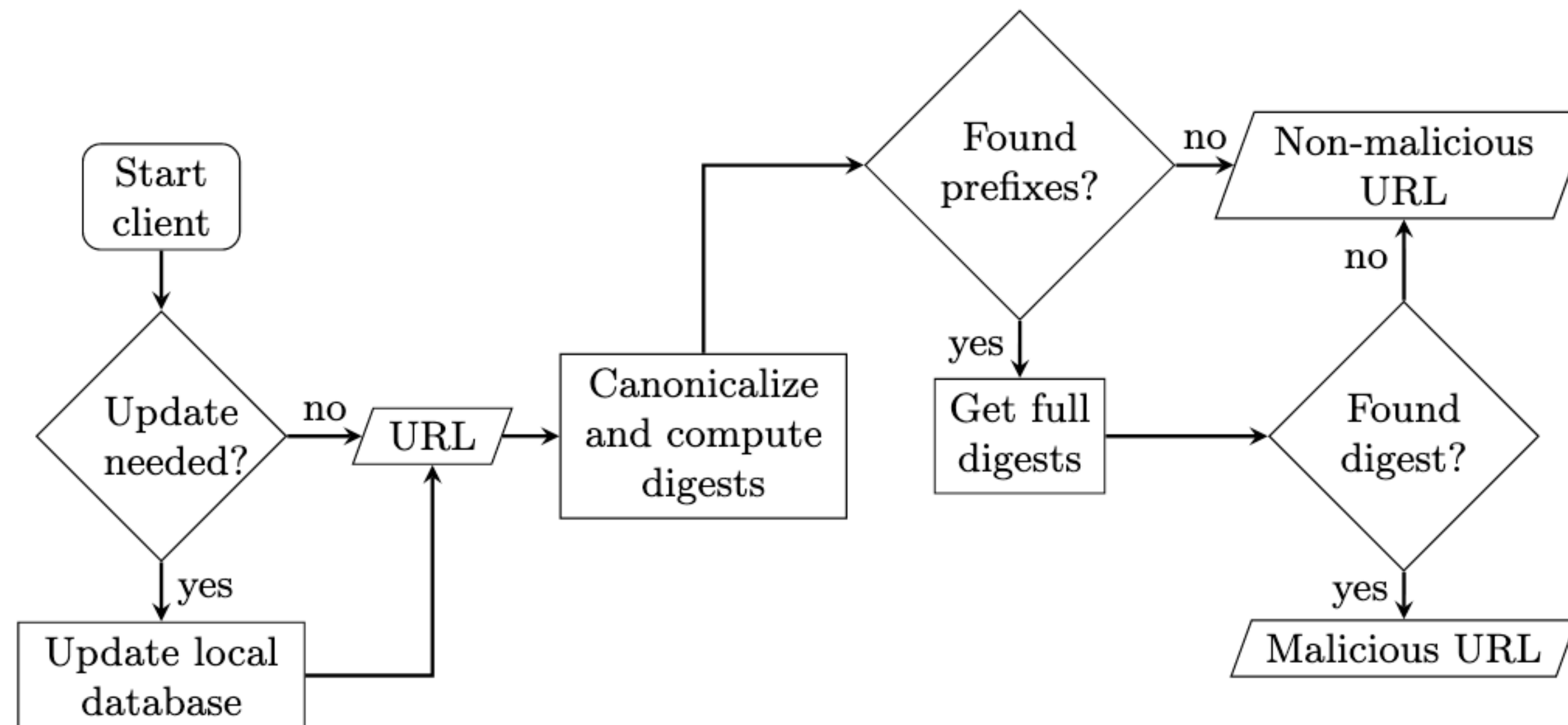
+ CONTRASTO: GOOGLE SAFE BROWSING



Fonte: <https://www.inrialpes.fr/planete/people/amkumar/papers/gsb-security.pdf>



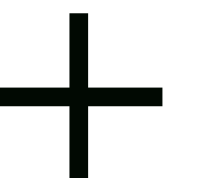
+ CONTRASTO: GOOGLE SAFE BROWSING



Fonte: <https://www.inrialpes.fr/planete/people/amkumar/papers/gsb-security.pdf>

+ BLOCKLIST E TECNICHE DI EVASIONE: GEO-BLOCKING

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js"></script>
<script>
  $.getJSON('https://api.ip.sb/geoip?callback=?', function (data) {
    if (data.continent_code == "EU"){
      $(location).attr('href', 'http://example.xsph.ru/phishing-page/')}
    else {
      $(location).attr('href', 'https://google.it/')}
  });
</script>
```



+ BLOCKLIST E TECNICHE DI EVASIONE: IP-BLOCKING

```
$ip_blocking_array = ["^192.168.*.*"]
```

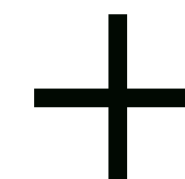
```
foreach ($ip_blocking_array as $ip) {  
    if (preg_match("/" . $ip . "/", $ipaddress_visitor)) {  
        header("HTTP/1.0 404 Not Found");  
        die("<h1>404 Not Found</h1>The page that you have requested could not be found.");  
    }  
}
```



+ BLOCKLIST E TECNICHE DI EVASIONE: HOSTNAME BLOCKING

```
$blocked_hostname = array( "google", "phishtank", "netcraft", "yandex", ...);

foreach($blocked_hostname as $word) {
    if (substr_count(gethostbyaddr($_SERVER['REMOTE_ADDR']), $word) > 0) {
        header("HTTP/1.0 404 Not Found");
        die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
    }
}
```



+ BLOCKLIST E TECNICHE DI EVASIONE: USER-AGENT BLOCKING

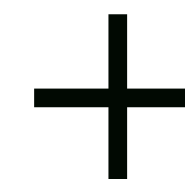
```
$useragent = $_SERVER['HTTP_USER_AGENT'];
```

```
if (strpos($useragent, "google") OR strpos($useragent, "phishtank") !== false ) {  
    header("HTTP/1.0 404 Not Found");  
    die("<h1>404 Not Found</h1>The page that you have requested could not be found.");  
}
```



+ BLOCKLIST E TECNICHE DI EVASIONE: USER-AGENT BLOCKING

```
$useragent = $_SERVER['HTTP_USER_AGENT'];  
if (strstr($useragent, "iPhone") === false ) {  
    header("HTTP/1.0 404 Not Found");  
    die("<h1>404 Not Found</h1>The page that you have requested could not be found.");  
}
```

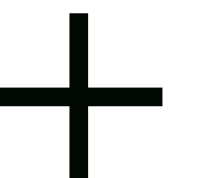


+ BLOCKLIST E TECNICHE DI EVASIONE: RANDOM PATHS

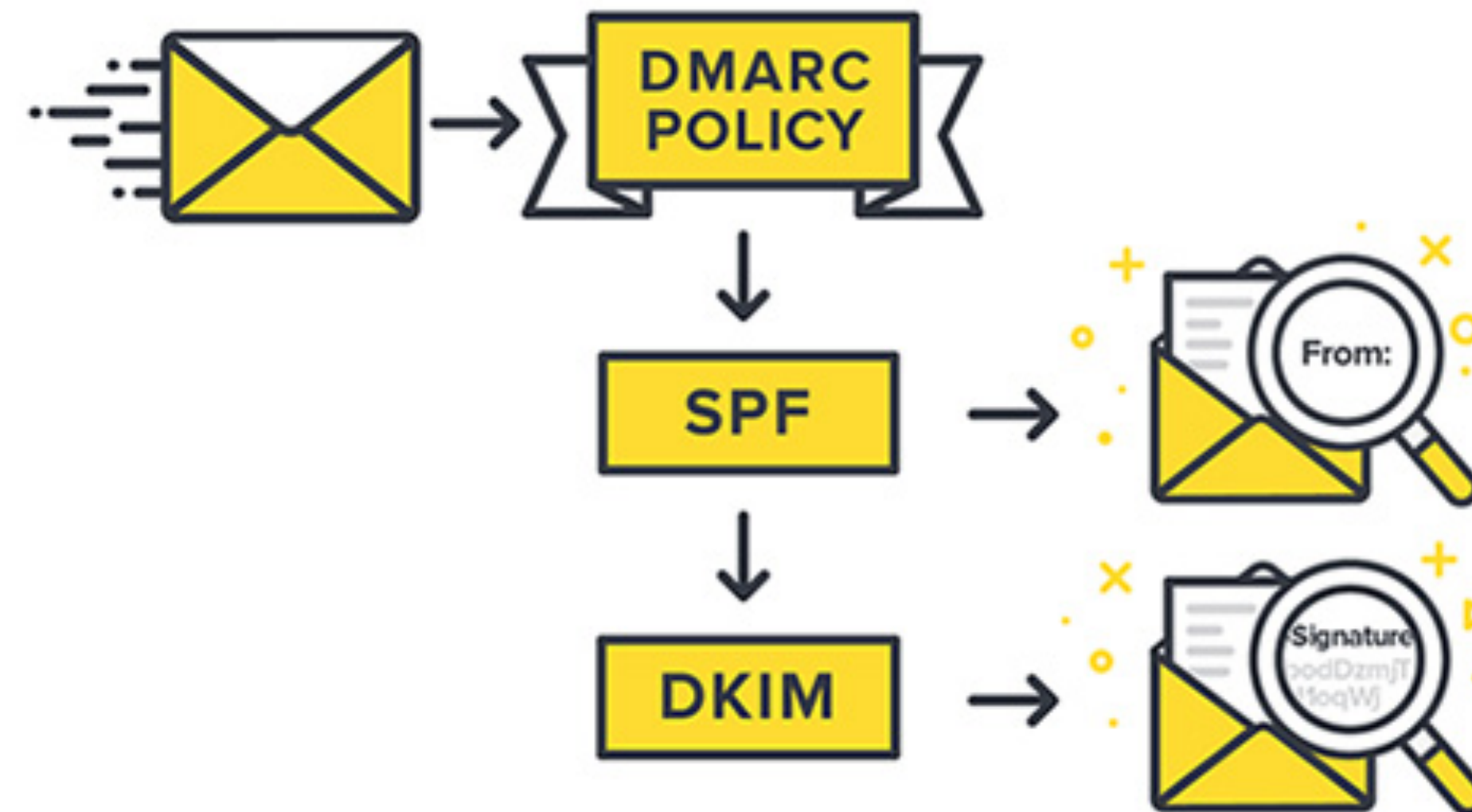
<https://www.officialsite.it.examplesite.com/login/caf93d0f225c7a59d52ad3c4a0afc575/>

<https://www.officialsite.it.caf93d0f225c7a59d52ad3c4a0afc575.examplesite.com/login/>

<https://www.officialsite.it.caf93d0f225c7a59d52ad3c4a0afc575.examplesite.com/login/caf93d0f225c7a59d52ad3c4a0afc575/>



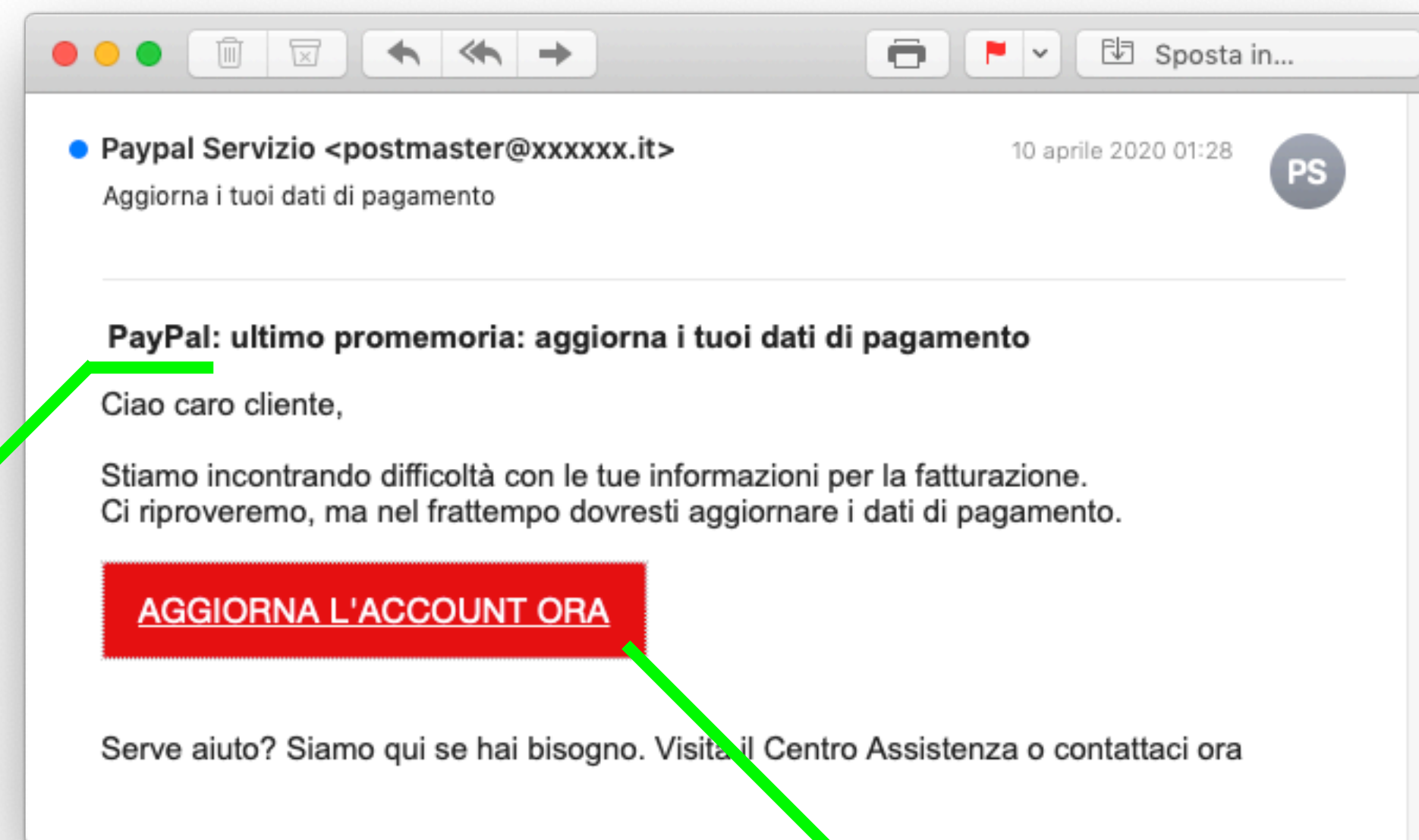
+ ANTI-SPAM E TECNICHE DI EVASIONE



mail-tester.com



+ ANTI-SPAM E TECNICHE DI EVASIONE



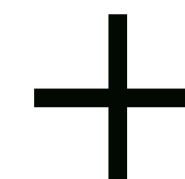
Invisible characters:

```
<style>span.hc {font-size:0;}</style>
```

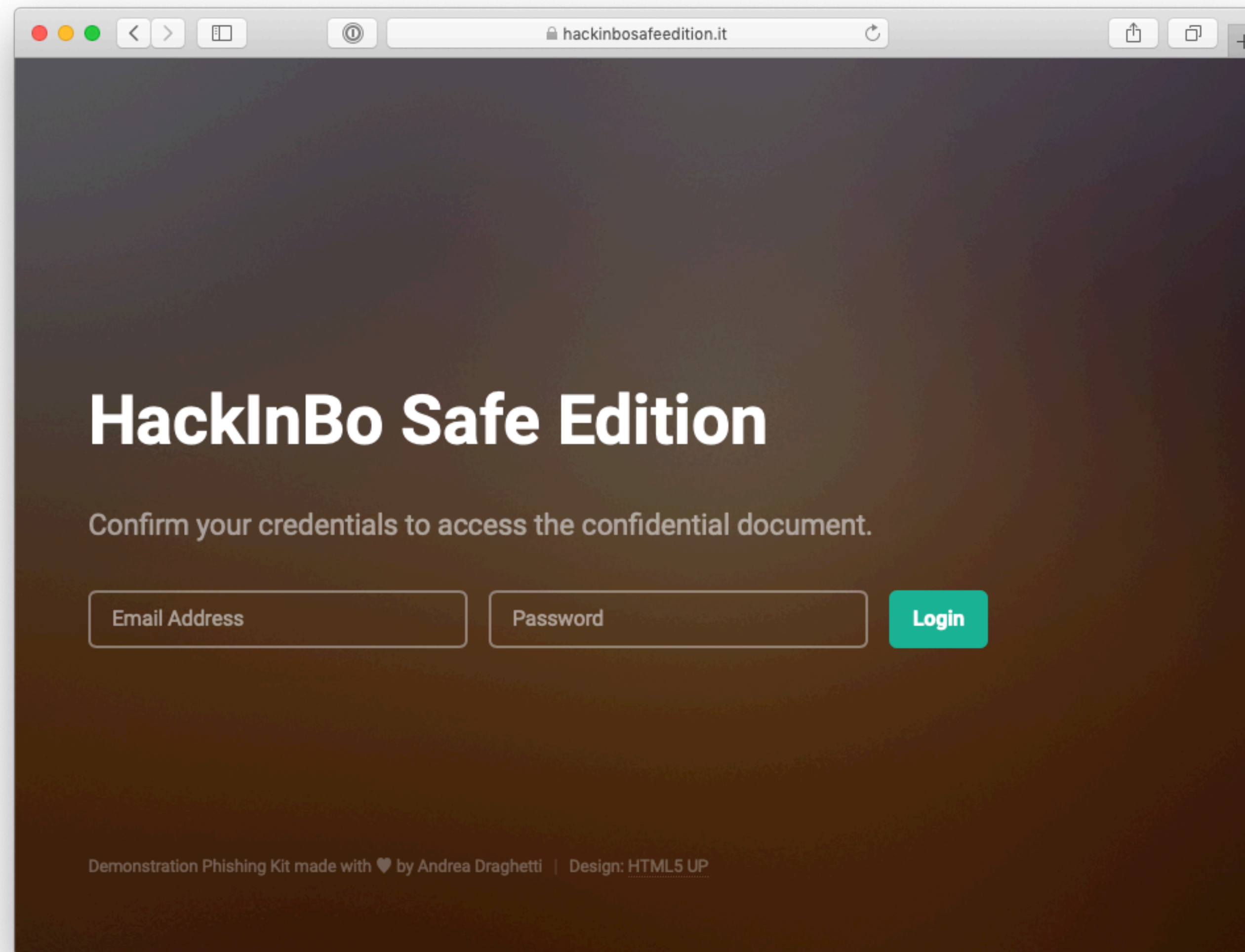
```
P<span class='hc'>1</span>a<span class='hc'>2</span>y<span class='hc'>3</span>P<span class='hc'>4</span>a<span class='hc'>5</span>l<span class='hc'>6</span>.....
```

Allowed URL:

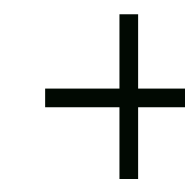
<https://bit.ly/2WwFPyB>



+ DEMO



<https://github.com/drego85/HackInBoSafeEdition/>



+ CONCLUSIONE



Photo by NeONBRAND on Unsplash

