

Master en Dirección de Ciberseguridad, Hacking Ético y Seguridad Ofensiva

PHISHING: 2FA? TRUST ME, I'VE PWNED YOU

Marta Barrio Marcos

Applications Security Architect

> 8 years of experience

CISA, CEH, CSX, OSCP, OSCE

Speaker at security conferences like NN2019,
C1b3rWall Academy

Trainer: ISACA, TSS, master UCLM

 <https://es.linkedin.com/in/martabarriomarcos>
 @martrudix



Carolina Gómez Uriarte



Delivery Consultant

> 3 years of experience

Head of Sh3llCON

CEH

Speaker at security conferences like NN2019,
HoneyCON, C1b3rWall Academy

 <https://es.linkedin.com/in/carolina-gomez-uriarte>
 @Carol12Gory



ÍNDICE

Section I: Introduction

- Disclaimer
- What is phishing?
- How to detect phishing?

Section II: Hands on labs

- Requirements
- GoPhish
- Evilginx2

Section III: How not to be phished

- Countermeasures

Section IV: I'm a victim, now what?

- What can we do if we are victims of phishing?

Section V: References

Section 1

Introduction

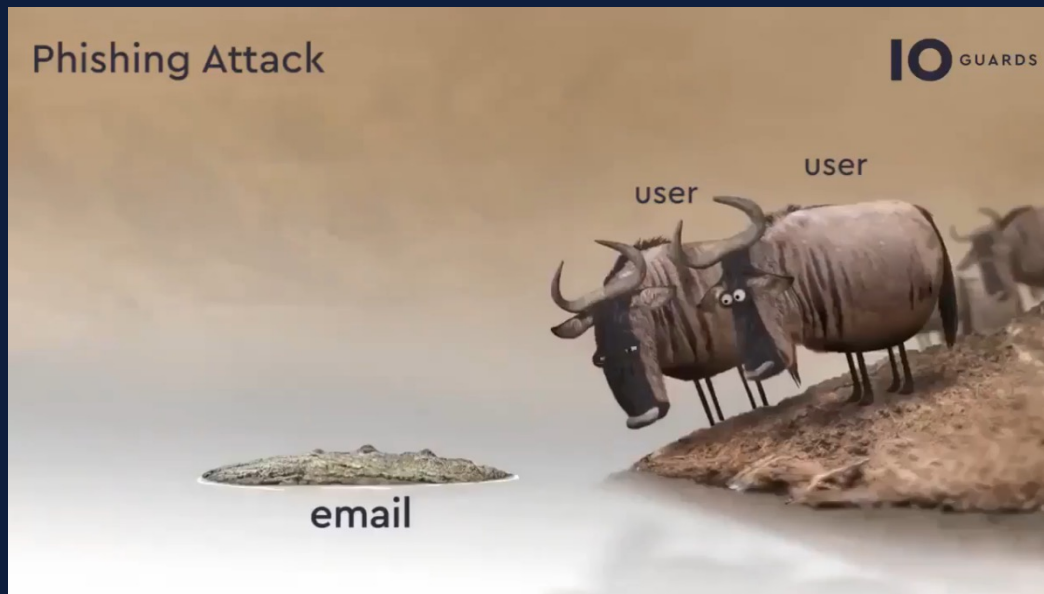
INTRODUCTION

Disclaimer

- This session is held to raise awareness and teach how cyber criminals carry out phishing attacks.
- Everything explained in this session has been done in controlled environments and without any evil purpose.
- Both speakers are not responsible for any illegitimate use for profit.

INTRODUCTION

What is phishing?



INTRODUCTION

What is phishing?

- **Impersonation** of web pages, e-mails, etc.
- Use of logos, texts, images known by the user to **mislead the user** and make him fall for the trick.
- Target: credentials, malware distribution, subscriptions to spam lists...

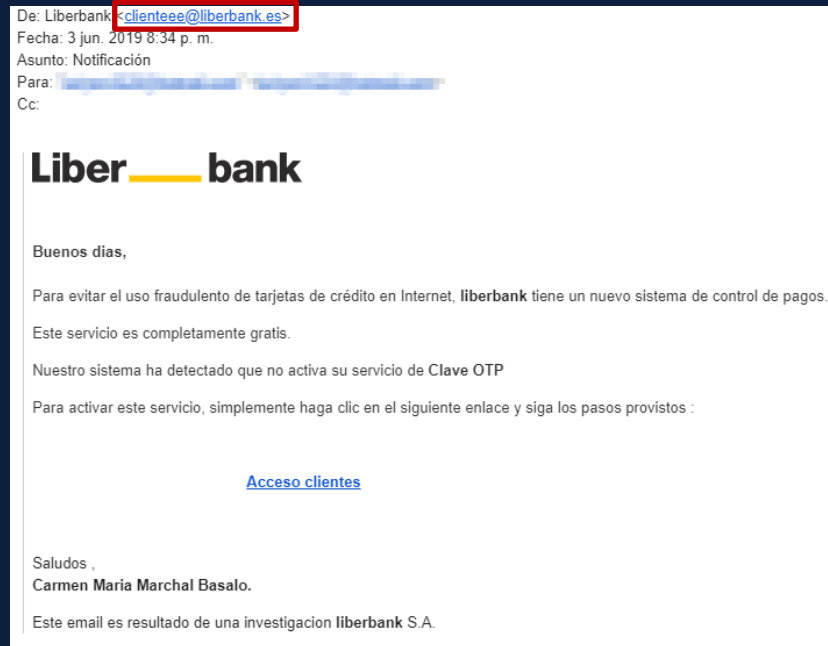
INTRODUCTION

How to detect phishing?

- Check the **sender**
- Check the **grammar of the mail**
- Where does the **link** go?
- Others checks like **Mail Headers**: IPs, domains, etc.

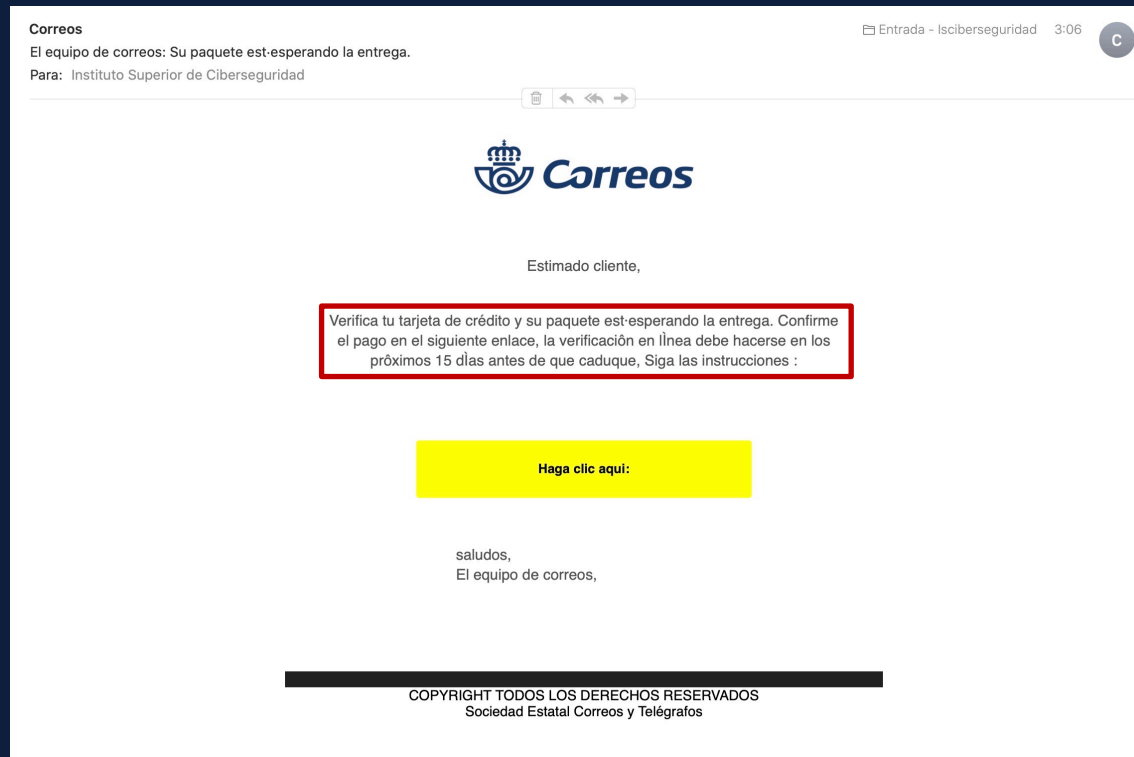
INTRODUCTION

Phishing examples



INTRODUCTION

Phishing examples



<https://twitter.com/juliocesarlop/status/1331142405052100609?s=20>

INTRODUCTION

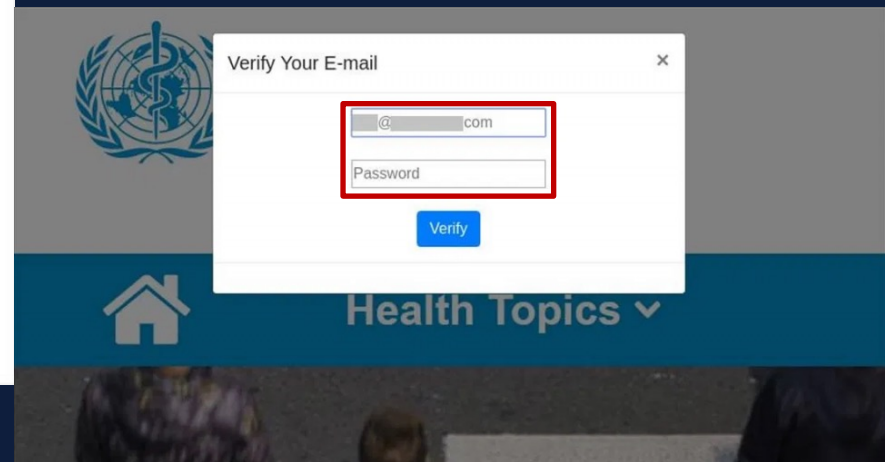
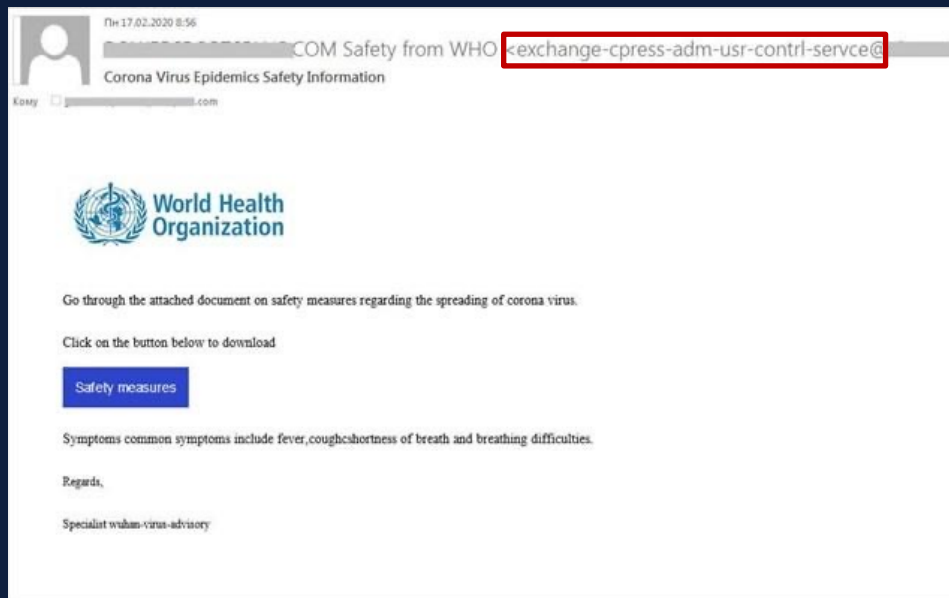
Phishing examples



<https://twitter.com/osiseguridad/status/1379052098973798400>

INTRODUCTION

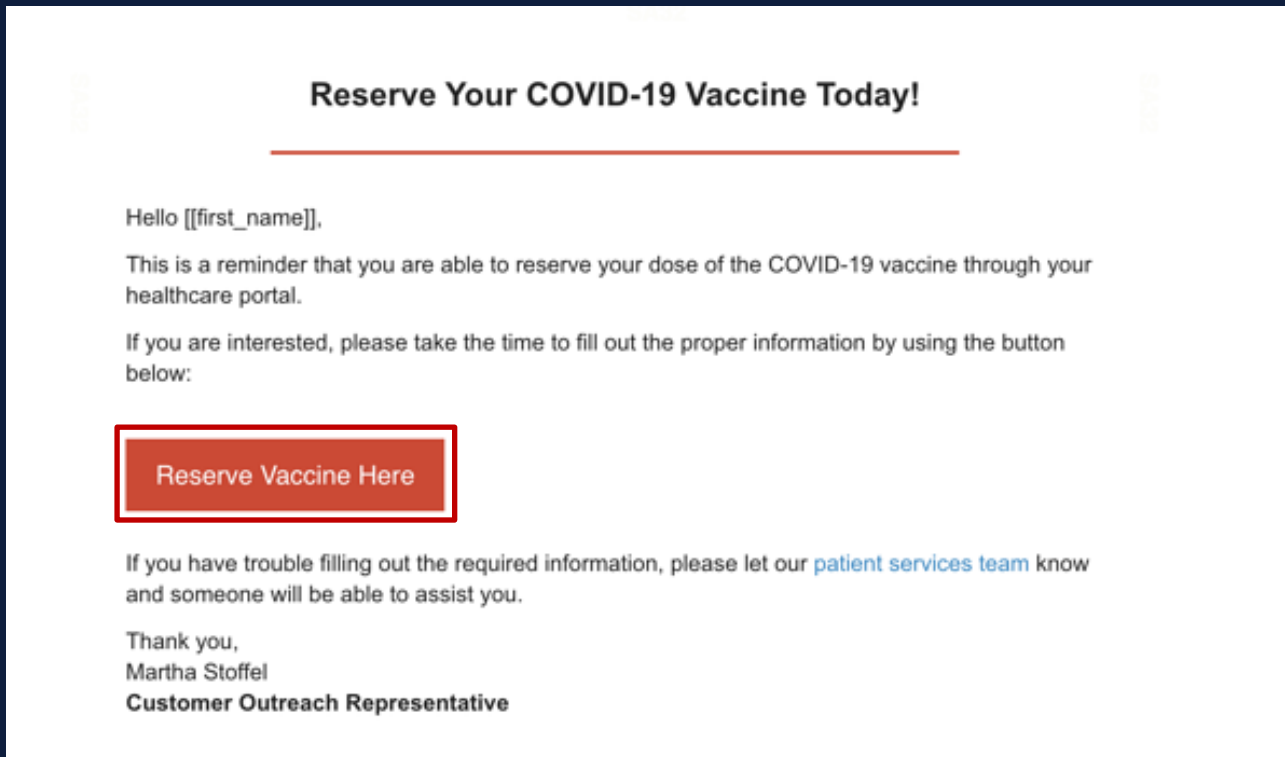
Phishing examples



<https://www.aepd.es/es/prensa-y-comunicacion/blog/campanas-de-phishing-sobre-el-covid-19>

INTRODUCTION

Phishing examples



<https://blog.knowbe4.com/the-covid-19-vaccine-the-next-wave-of-coronavirus-phishing-emails-what-you-can-do-about-it>

Section 2

Hands on labs

HANDS ON LABS

Requirements

Deployment

- **GoPhish** – Mail sender
- **Evilginx** – Manage the phishing

HANDS ON LABS

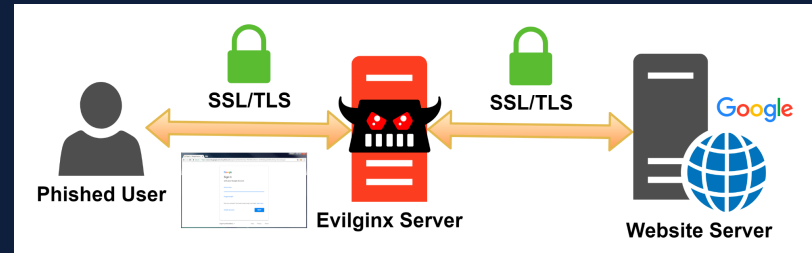
GoPhish Deployment

- *Config.json* file → IP and certificates config
- Sending Profiles → Config SMTP relay.
- ~~Landing Pages → Web that is shown to the victim when he clicks on the link~~
- Email Templates → Mail received by the victim
- Users & Groups → Destinations
- Campaigns

HANDS ON LABS

Evilginx2 Deployment

- **Phishlet** → YAML file where are defined subdomain necessary to do proxy, which strings should be replaced in relayed packets and which cookies should be captured.
- **Lure** → generation of phishing URLs
- **Config** → general configuration
- **Sessions** → sessions and captured tokens with credentials



@mrgretzky

HANDS ON LABS



HANDS ON LABS



Section 3

How not to be phished

HOW NOT TO BE PHISHED

Countermeasures

Recommendations for final users

- Check **domain** in URL bar
- Use **U2F** devices
- **DO NOT** use SMS 2FA – SIMJacking
- Common sense



HOW NOT TO BE PHISHED

Countermeasures

Recommendations for developers

- Check *window.location*
- Check *window.location* & obfuscate

```
>> window.location
< Location https://www.google.com/
  ▶ assign: function assign()
    hash: ""
    host: "www.google.com"
    hostname: "www.google.com"
    href: "https://www.google.com/"
    origin: "https://www.google.com"
    pathname: "/"
    port: ""
    protocol: "https:"
  ▶ reload: function reload()
  ▶ replace: function replace()
  search: ""
  ▶ toString: function toString()
  ▶ valueOf: function valueOf()
    Symbol(Symbol.toPrimitive): undefined
```

HOW NOT TO BE PHISHED

Countermeasures

Recommendations for developers

- Check *baseURI* property of DOM items

```
>> $("body").baseURI  
← "https://www.google.com/"
```

- Check headers: *X-Mailer: gophish*

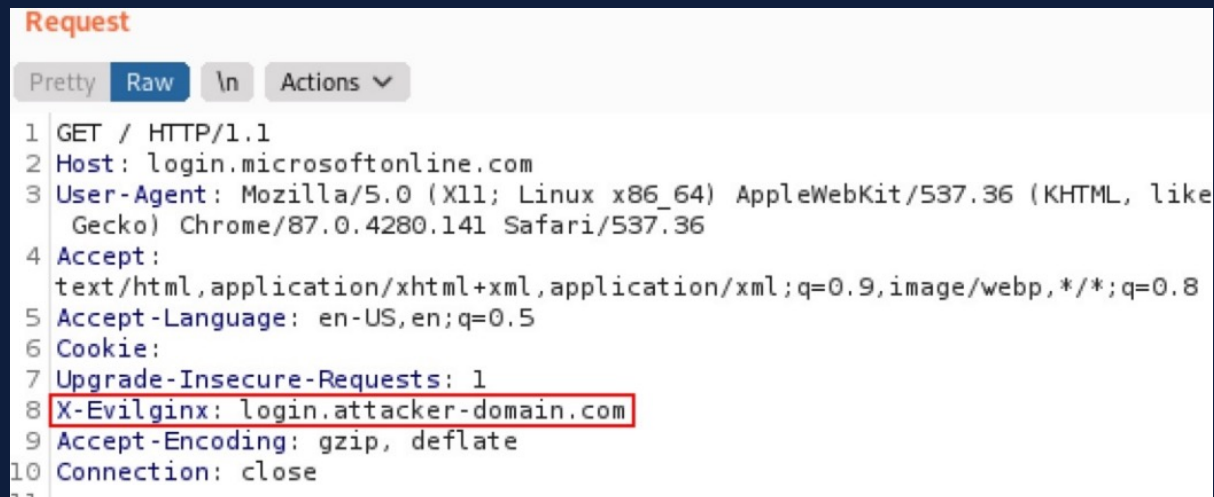
```
Date: Thu, 22 Apr 2021 10:44:29 +0200  
From: Outlook <security@microsoft-outlook.com>  
X-Mailer: gophish  
Message-Id: <1619081069784230589.14601.5364162700216065009@demophish>  
Subject: Tu cuenta de Outlook va a ser deshabilitada  
To: Marta Barrio <demophish2019@gmail.com>  
Content-Type: text/html; charset=UTF-8  
Content-Transfer-Encoding: quoted-printable
```

HOW NOT TO BE PHISHED

Countermeasures

Recommendations for developers

- Check headers: *X-Evilginx*



The screenshot shows a web browser's developer tools with the 'Request' tab selected. The 'Raw' button is highlighted. The request is a GET request to login.microsoftonline.com. The headers are listed as follows:

```
1 GET / HTTP/1.1
2 Host: login.microsoftonline.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/87.0.4280.141 Safari/537.36
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Cookie:
7 Upgrade-Insecure-Requests: 1
8 X-Evilginx: login.attacker-domain.com
9 Accept-Encoding: gzip, deflate
10 Connection: close
```

https://www.blackhillsinfosec.com/wp-content/uploads/2021/03/SLIDES_OPSECFundamentalsRemoteRedTeams-1.pdf

Section 4

I'm a victim, now what?

I'M A VICTIM, NOW WHAT?

- Collect as much information as possible: *emails, captures of conversations via email, documents sent, etc.*
- Bank phishing: contact to tour **bank office** to inform them of what happened
- Modify the password of all services where you use the same password (**but we don't use the same password for different services, right?**)
- Complaint

I'M A VICTIM, NOW WHAT?

- We can contact with (in Spain):
 - **Service or company** involved
 - Municipal Consumer Information Office (OMIC)
 - Report to the state security Forces (FCSE)
- Report to online services like Google:

Report impersonation

The page I'm reporting is:

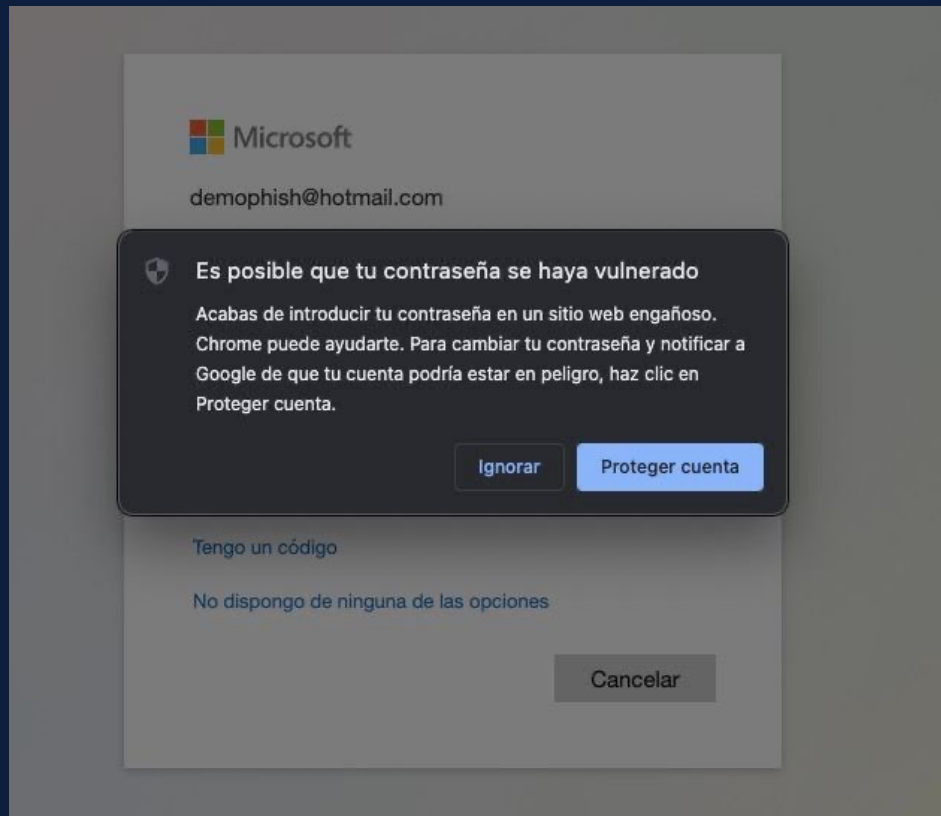
- ☐ Pretending to be me
- ☐ Pretending to be someone else, not me
- ☐ Falsely representing a company or organization

I'M A VICTIM, NOW WHAT?

Extra Tip

Are you affected by a security leak?

- Chrome:



Section 5

References

REFERENCES

Documentation and resources

- <https://github.com/kgretzky>
- <https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/>
- <https://breakdev.org/evilginx-2-3-phishermans-dream/>
- <https://breakdev.org/evilginx-2-4-gone-phishing/>
- <https://www.youtube.com/watch?v=QRyinxNY0fk>
- <https://getgophish.com/documentation/>
- <https://medium.com/@valeriyshevchenko/how-to-perform-phishing-attack-with-2fa-e9d633c66383>

MUCHAS GRACIAS POR SU ATENCIÓN



Marta Barrio Marcos

<https://es.linkedin.com/in/martabarriomarcos>

Carolina Gómez Uriarte

<https://es.linkedin.com/in/carolina-gomez-uriarte>



twitter.com/eiposgrados



facebook.com/eiposgrados



instagram.com/eiposgrados