

**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

> 2 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



#index

Part I: Introduction

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

Part II: Hands on labs

- Requirements
- GoPhish
- Evilginx2

Part III: How not to be phished

- Countermeasures

Part IV: References

1.

Part I

Introduction

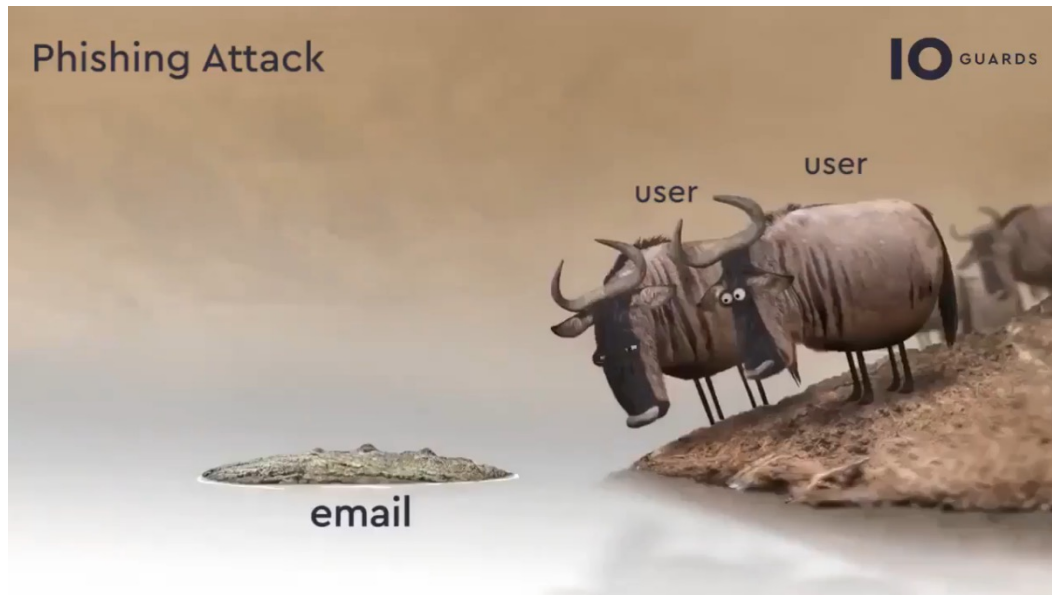
Disclaimer

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.

What is phishing?



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...

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.

Phishing examples

De: Liberbank <cliente@liberbank.es>

Fecha: 3 jun. 2019 8:34 p. m.

Asunto: Notificación

Para:

Cc:

Liber bank

Buenos días,

Para evitar el uso fraudulento de tarjetas de crédito en Internet, **liberbank** tiene un nuevo sistema de control de pagos.

Este servicio es completamente gratis.

Nuestro sistema ha detectado que no activa su servicio de **Clave OTP**

Para activar este servicio, simplemente haga clic en el siguiente enlace y siga los pasos provistos :

[Acceso clientes](#)

Saludos ,

Carmen Maria Marchal Basalo.

Este email es resultado de una investigacion **liberbank** S.A.

<http://nuevadigital.co.vu/?ref=9809C51RO2M5BB3908H8SY1HXTFRLW3D0998D7H897>

Phishing examples

Correos

El equipo de correos: Su paquete est-esperando la entrega.

Para: Instituto Superior de Ciberseguridad

Entrada - Isciberseguridad 3:06

C



Estimado cliente,

Verifica tu tarjeta de crédito y su paquete est-esperando la entrega. Confirme el pago en el siguiente enlace, la verificación en línea debe hacerse en los próximos 15 días antes de que caduque, Siga las instrucciones :

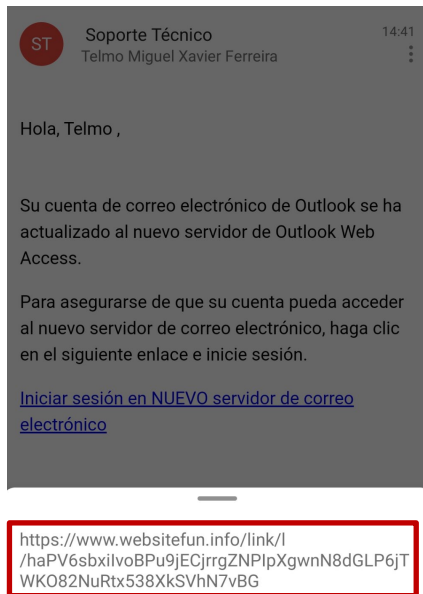
Haga clic aquí:

saludos,
El equipo de correos,

COPYRIGHT TODOS LOS DERECHOS RESERVADOS
Sociedad Estatal Correos y Telégrafos

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

Phishing examples



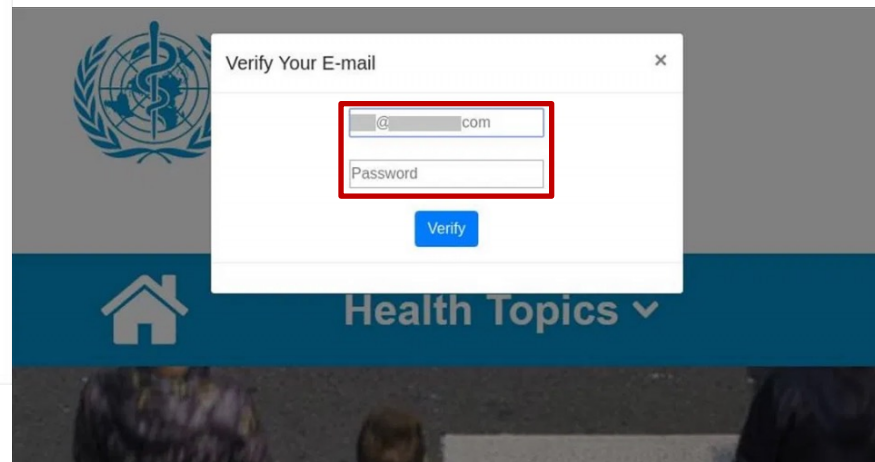
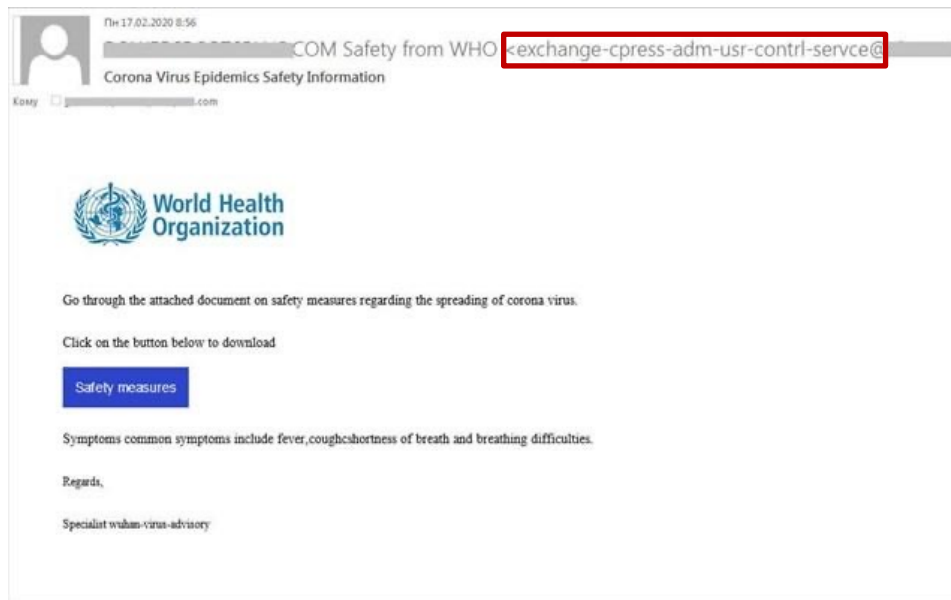
Copiar dirección del vínculo



Abrir vínculo

<https://twitter.com/t31m0/status/1331957527395831808?s=20>

Phishing examples



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

Phishing examples



2.

Part II

Hands on labs

Requirements

Deployment

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

GoPhish

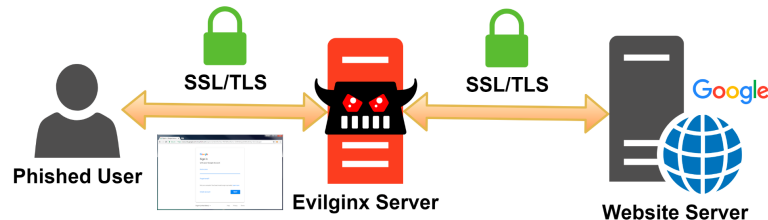
Deployment

- *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

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



OMG

DEMO TIME





3.

Part III

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



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
```

Countermeasures

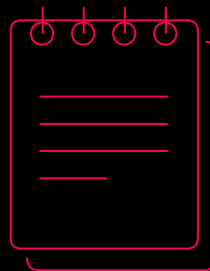
Recommendations for developers

- Check *baseURI* property of DOM items

```
>> $("body").baseURI
```

```
← "https://www.google.com/"
```

- Check headers: *X-Evilginx*



4. References

Documentation and resources

4.1 References

- <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>



Thanks!

Any questions?

You can find us at [@martrudix](#) & [@Carol12Gory](#)