

Seguridad frente al Phishing

Félix Fernández Peña

Basado en: Webinar “Seguridad en Tiempos de Covid-19”. David Guevara y Félix Fernández.

*“Es muy fácil ver la seguridad informática como un tema tecnológico – y uno que puede ser solucionado añadiendo más tecnología al problema. Y aún así, el elemento clave en muchos ataques es **la fragilidad humana**”.*

Mansfield-Devine, S., "Bad behaviour: exploiting human weaknesses",
Computer Fraud & Security, 2017(1), 17-20.
[https://doi.org/10.1016/S1361-3723\(17\)30008-8](https://doi.org/10.1016/S1361-3723(17)30008-8)

Hacer clic en enlaces desconocidos puede comprometer la seguridad informática.





Instalar software y/o abrir documentos de fuentes desconocidas.
puede comprometer la seguridad informática.



Utilizar contraseñas inseguras
puede comprometer la seguridad informática.

Agenda del Día

1. Estudio de casos alrededor de la ingeniería social.
 2. Orientación de práctica de laboratorio de Phishing.
 3. Autenticación de segunda fase.
 4. Generación y administración de contraseñas.
-



URGENTE ACERCARSE A LA LEGALIZAR LA BECA DE EXCELENCIA ACADEMICA

Muy buenos días

Se comunica que usted ha sido acreedor a una Beca de Excelencia Académica por lo que se le solicita de manera urgente venir a legalizar la beca de excelencia académica en el DIBESAU (**EDIFICIO NUEVO**) ubicado frente al edificio de Idiomas el lunes 13, martes 14 y miércoles 15 de Enero de 2020 en el horario del 8:30 a 12:30 y de 15:00 a 17:00 en el área de BECAS, deberán traer los siguiente requisitos:

- 2 copia a color de la cedula de identidad y papeleta de votación actualizada de marzo 2019.
- 2 copias de cuenta bancaria a color de ahorros a su nombre que este bien legible.

NOTA: CONFIRMAR SU ASISTENCIA EN EL SIGUIENTE ENLACE <https://cutt.ly/Wrfhr9S>

Reenviar Compartir en Facebook Información

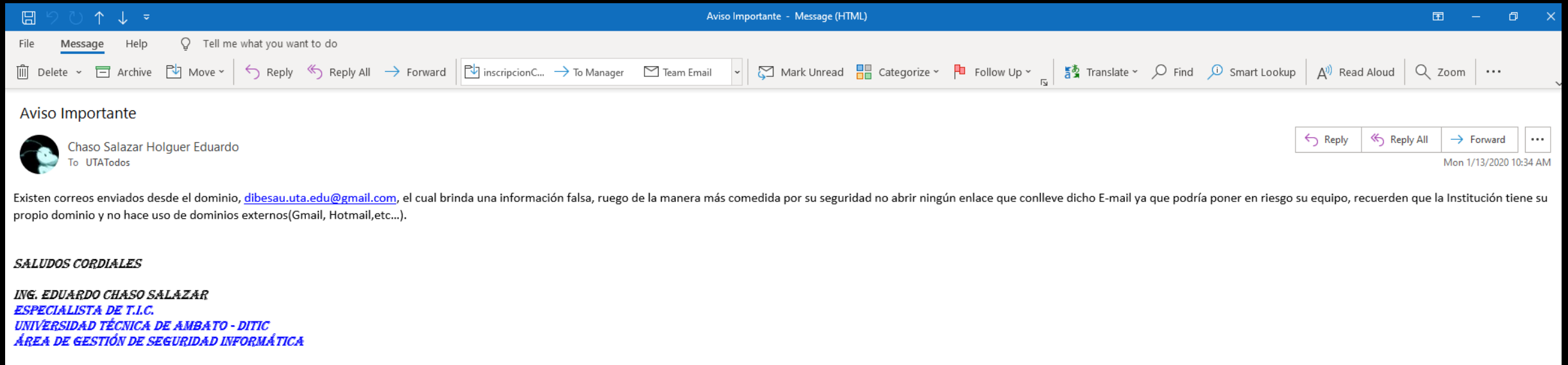
ADVERTENCIA !

Usted pudo haber sido victima de phishing al dar clic en enlace anterior y se pudieron haber capturado los siguientes datos

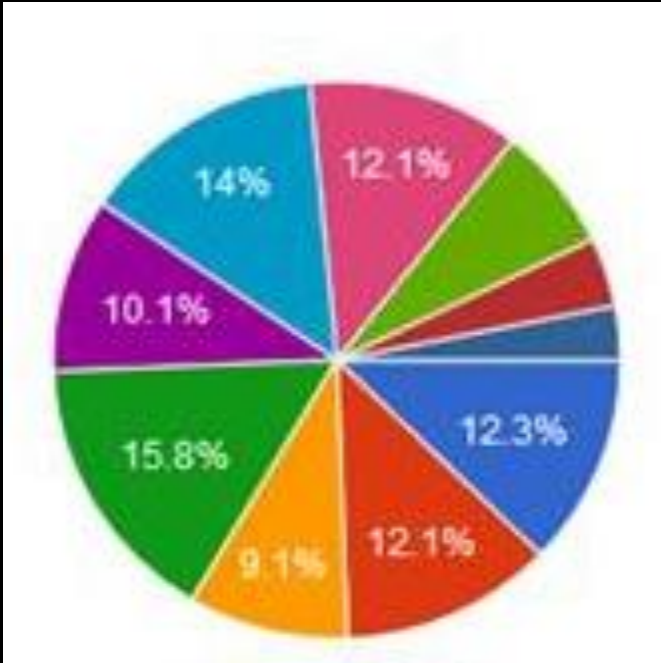
| Direccion IP | País | Ciudad | Region | Codigo ZIP | Latitud | Longitud | Zona Horaria |
|----------------|---------|--------|------------|------------|----------|----------|--------------|
| 186.46.224.151 | Ecuador | Ambato | Tungurahua | EC | -1.24908 | -78.6168 | -05:00 |

[Web hosting by Somee.com](#)

El 47.33% de estudiantes que recibieron este correo electrónico **dieron clic** al enlace que recibieron.

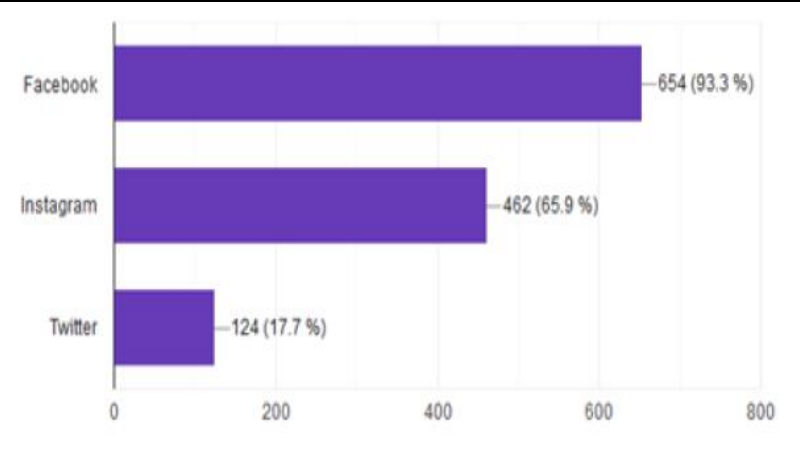


El 47.33% de estudiantes que recibieron este correo electrónico **dieron clic** al enlace que recibieron.



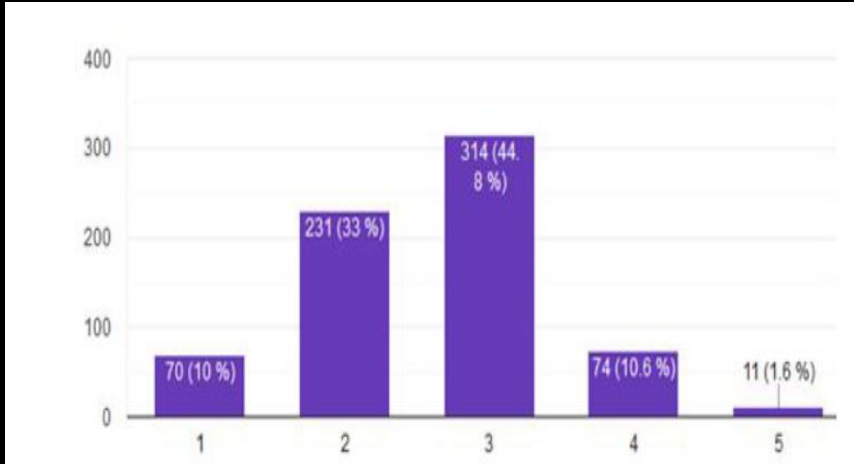
701 estudiantes

42% utiliza dispositivos de desconocidos.



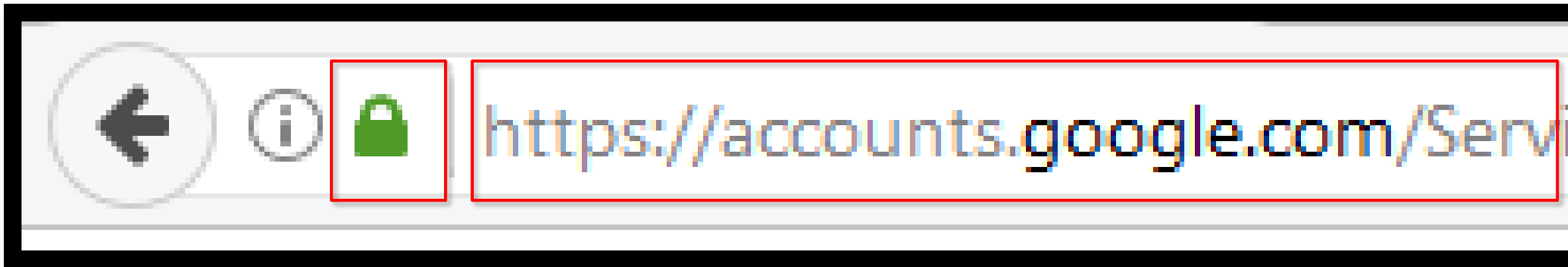
Usan redes sociales

50.4% considera que el usar celular/tablet es más seguro.



Acceden a enlaces que reciben

La seguridad ante ataques de Ingeniería Social es una asignatura pendiente.



Correo electrónico o teléfono

[¿Has olvidado tu correo electrónico?](#)

¿No es tu ordenador? Usa una ventana privada para iniciar sesión. [Más información](#)

[Crear cuenta](#) [Siguiente](#)

Español (España) ▼

[Ayuda](#)

[Privacidad](#)

[Términos](#)

Favorites

01 - Information Gathering ▶

02 - Vulnerability Analysis ▶

03 - Web Application Analysis ▶

04 - Database Assessment

05 - Password Attacks ▶

06 - Wireless Attacks ▶

07 - Reverse Engineering

08 - Exploitation Tools

09 - Sniffing & Spoofing ▶

10 - Post Exploitation ▶

11 - Forensics ▶

12 - Reporting Tools

13 - Social Engineering Tools

14 - System Services ▶



backdoor-f...



beef xss fr...



ghost phis...



maltego



msf payloa...



social engi...



u3-pwn

Aplicaciones ▾

Lugares ▾

Firefox ESR ▾

mié 13:44

1

es ▾



Gmail - Mozilla Firefox (Private Browsing)



GUÍA DE PRACTICAS - 5... x

Gmail x

Gmail x

x



172.21.107.190/signin/v2/identifer?flowName



Search



Most Visited ▾



Offensive Security



Kali Linux



Kali Docs



Kali Tools



Exploit-DB



Aircrack-ng

Google

Acceder

Ir a Gmail

Correo electrónico o teléfono

|

¿Olvidaste el correo electrónico?

¿Esta no es tu computadora? Usa el modo de invitado para navegar de forma privada. [Más información](#)



Escribe aquí para buscar

12:05

24/4/2019


```
Terminal -
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your d
irectory structure is.
Press {return} if you understand what we're saying here.
[+] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.21.107.185 - - [24/Apr/2019 12:05:05] "GET / HTTP/1.1" 200 -
[+] WE GOT A HIT! Printing the output:
PARAM: utf8=✓
PARAM: authenticity_token=iN3ex0wQ2vZa4hg44I0z6nDCaY9CM/OT8/bSTXf5DaMubPfuGcbW4Z
wBb0uv0Ih0FIofZirDq/qa7FkBMfnTDw==
POSSIBLE USERNAME FIELD FOUND:
POSSIBLE PASSWORD FIELD FOUND:
PARAM: remember_me=1
[+] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Aplicaciones ▾

Lugares ▾

Firefox ESR ▾

mié 13:44

1



es ▾



Gmail - Mozilla Firefox (Private Browsing)



GUÍA DE PRACTICAS - 5... x



Gmail



Gmail



<http://accounts.google.com/ServiceLogin/>

Search



Most Visited ▾



Offensive Security



Kali Linux



Kali Docs



Kali Tools



Exploit-DB



Aircrack-ng

Google

Acceder

Ir a Gmail

Correo electrónico o teléfono

|

[¿Olvidaste el correo electrónico?](#)

¿Esta no es tu computadora? Usa el modo de invitado para navegar de forma privada. [Más información](#)



Escribe aquí para buscar



12:05

24/4/2019



Making over a billion long URLs usable! Serving billions of redirects per month.

[Home](#)[Example](#)[Make Toolbar
Button](#)[Redirection](#)[Preview Feature^{cool!}](#)[Link to Us!](#)[Terms of use](#)[Articles](#)[Contact Us!](#)

Welcome to TinyURL!™

Are you sick of posting URLs in emails only to have it break when sent causing the recipient to have to cut and paste it back together? Then you've come to the right place. By entering in a URL in the text field below, we will create a tiny URL that ***will not break in email postings*** and ***never expires***.

Enter a long URL to make tiny:

Make TinyURL!

Custom alias (optional):

<https://tinyurl.com/>

May contain letters, numbers, and dashes.

An example

Turn this URL:

`http://www.amazon.com/Kindle-Wireless-Reading-Display-Globally/dp/B003FSUDM4/ref=amb_link_353259562_2?pf_rd_m=ATVPDKIKX0DER&pf_rd_s=center-10&pf_rd_r=11EYKTN682A79T370AM3&pf_rd_t=201&pf_rd_p=1270985982&pf_rd_i=B002Y27P3M`

into this TinyURL:

<http://tinyurl.com/KindleWireless>

Which one would you rather cut and paste into your browser? That's the power of TinyURL!

Cómo prevenir ataques de Ing. Social

Sé cauteloso(a). Revisa críticamente los mails que recibes.

Revisa el contenido. Podría incluso haber un registro de ataque de suplantación de identidad con el mail que has recibido.

Si crees que has recibido una solicitud legítima que requiere que confirmes credenciales, intenta hacerlo por un medio convencional.

Revisa las URL. Garantiza que utilicen HTTPS.

No compartas tus contraseñas.