

# Seguridad Preventiva en Internet - Parte 2

...

¡Defiéndete ante las nuevas amenazas!

# Por repasar un poquito...

(continuamos desde el último día)

- ~~Phishing y estafas online~~
- ~~Malwares~~
- Contraseñas y buenas prácticas
- Privacidad y seguridad en internet

---

# Contraseñas y buenas prácticas



# Las contraseñas

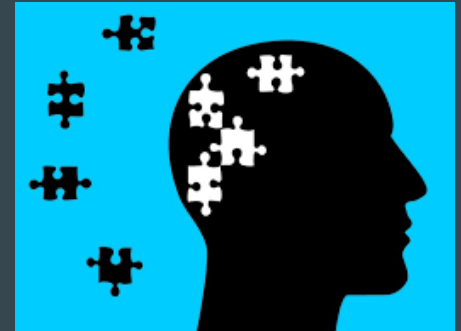
“Una contraseña o clave es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso.” ([Wikipedia](#))

En nuestro día a día utilizamos las contraseñas para acceder a cualquier servicio o dispositivo. Y, al final, acabamos autenticando nos en decenas de ellos.

Es por ello que es importante definir unas buenas políticas para elegir y manejar nuestras contraseñas.

# Características de una “buena” contraseña

- Tiene que ser lo suficientemente ROBUSTA
- No tiene que ser predecible = IMPREDECIBLE
- Debe de ser fácilmente RECORDABLE por el usuario



# Características de una “buena” contraseña

- Robustez

- Longitud deseada: > 10 caracteres ('caracteres' == 10)
- Case Sensitive: Mayúsculas y Minúsculas
- Numérica: al menos un par de números
- Y si ya, le pones algún carácter especial... pues fantástico!

L0Us0P4r4Cr1tlc@r

Lo\_del\_p4jaro\_azul!



- Impredecible

- Mi contraseña es: Katniss12
- El nombre de mi gata es: Katniss
- El mes en el que nació mi gata es: Diciembre (12)



- Recordable:

- Mi contraseña es: sAHtp8LQxY



¿Dónde se puede generar una buena contraseña?

LastPass 



# Ataques a contraseñas

Algunos ataques que se pueden realizar utilizando contraseñas son los siguientes:

- Ataques de Fuerza Bruta
- Ataques de Password Spraying
- Ataques de Password Reuse
- Ataques de Predicción
- Ataques de Permutación y Combinatoria





# Password Leaks

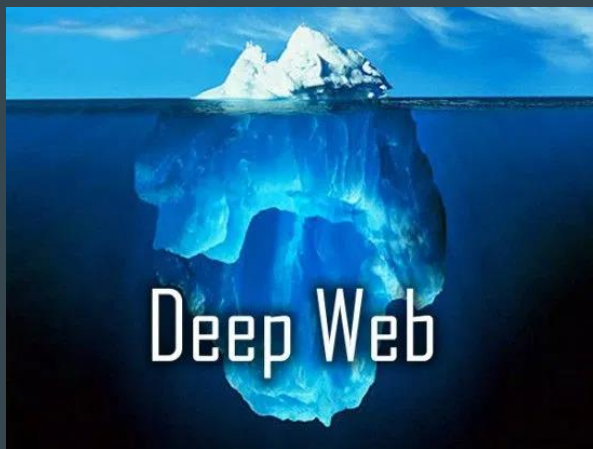
En ocasiones, cuando un servicio es comprometido, sino se han guardado correctamente las credenciales en la base de datos estás, por extensión, se ven comprometidas también.

Cuando este conjunto de credenciales o contraseñas, se extraen del servicio comprometido y se publican en Internet, pasan a conocer como LEAK.



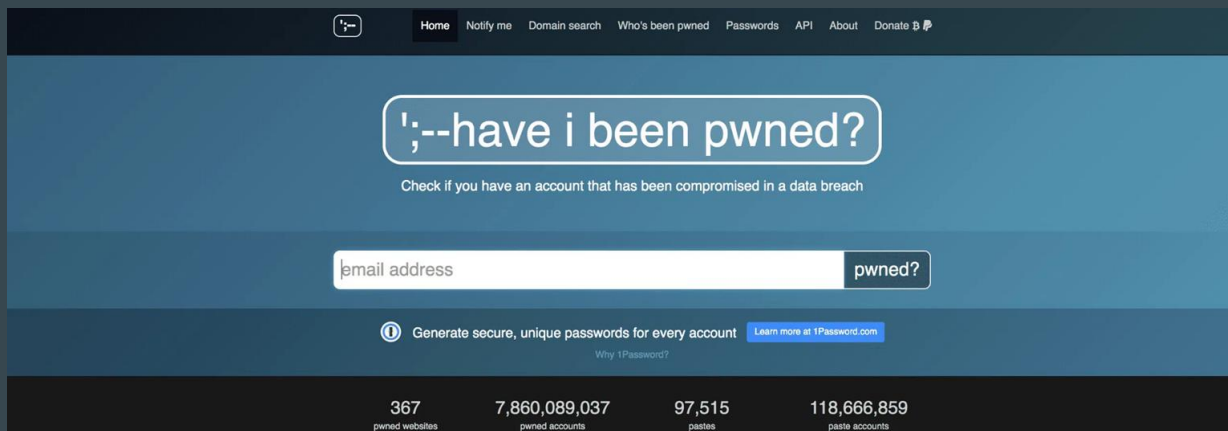
# ¿Dónde se publican los Leaks de Credenciales?

En sitios como: Raidforums, Pastebin, en servicios .onion\* y no tan onion.



# ¿Cómo combatir esta amenaza?

1. Usa “one-use passwords” o “mails temporales” en determinados servicios web.
2. No uses contraseñas predecibles o variaciones de otras contraseñas
3. En caso de querer saber si alguno de tus correos ha sido comprometido y está en algún leak público, puedes usar el servicio de [HaveIbeenPwned](#)



The screenshot shows the homepage of the HaveIbeenPwned website. At the top is a dark navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area has a blue background with a large white rounded rectangle containing the text "'--have i been pwned?". Below this is a subtitle: "Check if you have an account that has been compromised in a data breach". A search form consists of a white input field labeled "email address" and a dark button labeled "pwned?". Below the form is a blue banner with an information icon, the text "Generate secure, unique passwords for every account", and a link "Learn more at 1Password.com". At the bottom is a dark footer with four statistics: 367 pwned websites, 7,860,089,037 pwned accounts, 97,515 pastes, and 118,666,859 paste accounts.

Statistic	Value
pwned websites	367
pwned accounts	7,860,089,037
pastes	97,515
paste accounts	118,666,859

# El que nunca falla... Password Reuse

Escenario:

1. Atacante fija a un usuario como su objetivo.
2. Comienza buscando credenciales en Leaks de contraseñas. Y consigue un par de credenciales de un servicio web de... 2018
3. El atacante prueba las credenciales obtenidas en una red social, como por ejemplo, twitter. Y consigue entrar!
4. Tras esto, el atacante utiliza esa misma contraseña para entrar en el Instagram, Facebook, BBVA y Gmail de la víctima. PORQUE ES LA MISMA
5. Finalmente, el atacante consigue acceso a todos sus servicios utilizando una sola contraseña. Resultado: TAKEOVER total.

# ¿Medidas?

1. No utilices la misma contraseña para todo.
2. Tampoco vale utilizar combinaciones sobre tu contraseña original. Ejemplo: si tu contraseña es: Pepito2020, no vale usar Pepito1, 123Pepito, Pe123pito...
3. Utiliza un gestor de contraseñas como Keepass.
4. Utiliza un segundo factor de autenticación (2FA)



¿Preguntas?

# Privacidad y Seguridad en Internet



# ¿Qué es la Privacidad?

Entiendo la privacidad como aquel contexto o espacio, propio del individuo y en el cual toda información queda reservada y se mantiene confidencial para sí mismo.

¿Por qué es importante la privacidad?

- ¿Dejarías la puerta de tu casa abierta?
- ¿Permitirías que cualquier persona pueda ver todas tus conversaciones?
- ¿Compartirías tu geolocalización para cualquier persona en todo momento?













# Redes Sociales y Datos

Las aplicaciones saben mucha información sobre ti, algunos datos son imprescindibles, pero muchos otros... ponen en jaque tu privacidad.

clarío.

The companies that know most about you

#	Company	% of personal data collected	Email	Name	Age	Gender/Sex	Sexual Orientation	Marital Status	Race	Religious Belief	Live Location	Home Address	Employment Status	Job Title	Pet/Animal Ownership	Mobile Number	Landline Number	Type of Phone/Device	Hobbies	Interests	Height	Weight	Next of Kin	Mother's Maiden Name	Current Employers	Past Employers	Bank Account Details	Salary	Social Profile (Friends)	Social Profile (Hobbies)	Social Profile (Interests)	Country of Birth	Allergies/Intolerances	Health & Lifestyle Info
1	 Facebook	70.59%	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
2	 Instagram	58.82%	•	•	•	•					•	•	•	•	•	•	•	•	•	•	•			•	•			•	•	•	•			
3	 Tinder	55.88%	•	•	•	•	•	•			•		•	•	•	•			•	•	•					•		•	•	•	•			
4	 Grindr	52.94%	•	•	•	•	•	•			•		•	•	•	•			•	•	•							•	•	•	•			
5	 Uber	52.94%	•	•	•	•					•	•	•	•		•	•	•	•	•					•	•			•	•	•			
6	 Strava	41.18%	•	•	•	•					•	•				•	•			•	•	•				•		•	•	•	•			
7	 Tesco	38.24%	•	•	•	•		•			•					•	•	•								•		•	•	•	•			
8	 Spotify	35.29%	•	•	•						•					•	•	•	•	•						•		•	•	•	•			
9	 MyFitnessPal	35.29%	•	•	•						•					•	•	•			•	•				•							•	
10	 Jet2	35.29%	•	•	•	•		•	•		•					•	•	•								•							•	

# Y también servicios de mensajería...

SEGURIDAD Y PRIVACIDAD EN APPS DE MENSajerÍA							
	Whatsapp	Telegram	Signal	FB messenger	Wire	Wickr Me	Delta chat (App que envía mensajes por correo electrónico)
Verificación de 2 pasos	Sí	Sí	Sí	Sí desde inicio de sesión de Facebook	No	En Wickr Pro	Depende de tu correo electrónico
¿Se puede bloquear el acceso a la app?	Solo con huella dactilar	Sí	Sí	No	Sí	Sí	No
Cifrado de extremo a extremo	Sí	- Cifrado simple en chats convencionales - Cifrado fuerte en chat secreto	Sí	Solo en chat secreto	Sí	Sí	Sí
¿Pueden leer mis conversaciones?	Aseguran que no, pero potencialmente podría hacerlo * Hace falta mayor información al respecto	Aseguran que no, pero potencialmente podría hacerlo * Hace falta mayor información al respecto	No	Sí	No	No	No
Está relacionado a tu número de teléfono	Sí	Sí, pero puedes ocultarlo para que no se muestre	Sí	Parcialmente, depende de la configuración de Facebook (si inicias por correo o número telefónico)	Inicialmente al correo, pero se puede asociar el número telefónico	No	No
Almacena información en sus servidores	Parcialmente (Datos de la cuenta)	Sí, excepto la información de chats secretos	Parcialmente (Datos de la cuenta)	Sí	Sí, pero está cifrado	Sí, pero está cifrado	No, depende del proveedor de correo con el que te registres
¿Recaba y comparte información internamente o con terceros?	Sí comparte con empresas de FB	Sí	No	Sí	No	No	No
Autodestrucción de mensajes	Sí, después de una semana	Solo en chat secreto	Sí	Dice que temporal	Sí	Sí	No
Bloqueo de captura de pantalla	No	Solo en chat secreto	Sí	No	No	En Wickr Pro	No
Bloqueo de reenvío de mensajes	No	Solo en chat secreto	No	No	No	No	No
OTROS ASPECTOS							
Código abierto	No	Solo la app, los servidores no	Sí	No	Sí	Solo una parte de la app, los servidores no	Sí
Tiene reportes de transparencia	Sí	No	Sí	Sí	Sí	Sí	Depende del proveedor de correo
Tiene herramientas para reporte y bloqueo de contactos y grupos	Sí	Sí y también para stickers	Solo bloqueo	Sí	Solo bloqueo	Solo bloqueo	Solo bloqueo
Stickers y gifs	Sí	Sí	Sí	Sí	Sí	No	No

## ¿Son seguras tus aplicaciones de mensajería instantánea?

\*Las aplicaciones resaltadas en rojo, al no ser de código abierto, no nos permiten estar del todo seguros de que su garantía de seguridad sea máxima

	¿Viaja cifrado el mensaje?	¿Está encriptado de extremo a extremo?	¿Se puede verificar la identidad del contacto?	Si te quitan las claves, ¿están a salvo tus mensajes?	¿Es código abierto?	¿Se ha revisado el código últimamente?
Snapchat	✓	✗	✗	✗	✗	✓
Google Hangouts	✓	✗	✗	✗	✗	✓
Telegram	✓	✗	✗	✗	✓	✓
WhatsApp	✓	✓	✓	✓	✗	✓
Signal	✓	✓	✓	✓	✓	✓
Facebook Chat	✓	✗	✗	✗	✗	✓
Skype	✓	✗	✗	✗	✗	✗
ChatSecure	✓	✓	✓	✓	✓	✓
Pidgin	✓	✓	✓	✓	✓	✓

Fuente: Electronic Frontier Foundation

# Riesgos en redes sociales

Al utilizar las redes sociales nos encontramos expuestos a determinados riesgos que, sino no conocemos o pasamos por alto, pueden exponer mucha información acerca de nosotros y de nuestro entorno:

- Exposición mediante perfiles públicos
- Exposición al compartir archivos
- Metadatos
- Tracking a partir de los datos expuestos



# ¿Qué puede pasar si tenemos el perfil público?

En primer lugar, depende de la red social, pues cada una maneja un conjunto de información diferente. No obstante, el riesgo es obvio: si tu perfil es público significa que **CUALQUIER PERSONA PUEDE ACCEDER A LA INFORMACIÓN.**

¿Y cómo lo hacen los atacantes para acceder a esa información pública?

Pues, uno de los métodos que se suele utilizar para encontrar y obtener esa información, es utilizar técnicas de web scraping.



# Una cara desconocida: Información que subes a las redes

En ocasiones, no percibimos el peligro que tiene subir información a las redes sociales. Información que un actor malicioso puede utilizar para su propio beneficio:

- Foto de vacaciones en Salou: “...ya se que no estás en casa”
- Foto de clase online aburrida: “...ya se que sistema operativo y software tienes”
- Captura de pantalla de una conversación: “...ya se quién es tu operador”
- Foto lavando el coche: “...si sale la matricula, ya se quién eres”

Y así un sin fin de posibilidades... dime una cosa...

¿eras consciente de alguna de estas?



# Cuando subes una imagen...

Cuando subes una imagen... sin darte cuenta estás dando la posibilidad de que tu cara o la de quien salga, se utilice para:

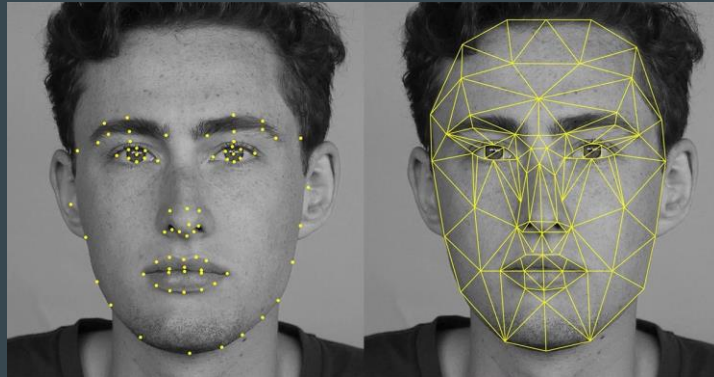
- Hacer extorsión a otras personas o a ti mism@
- Como complemento en Scams
- Sexting y extorsiones relacionadas
- Suplantación de identidad
- Publicidad sin tu autorización



# Rizando el rizo: reconocimiento facial

Otra cosa en la que no caemos cuando subimos una imagen nuestra o de una persona a internet, es que esta persona queda expuesta. Y con ello me refiero a que, es posible, utilizar las herramientas que algunos servicios te brindan para desvelar su identidad.

Es posible utilizar el reconocimiento de imágenes de servicios como: Google, Yandex, Pimeyes, TinEye, etc.



# Busca y encontrarás: los metadatos

Los metadatos se conocen como “los datos de los datos”, es decir, es la información relacionada con un archivo. ¿Y por qué son importantes? Porque esa información acerca del archivo, nos puede servir para trabajar en inteligencia.

Algunos ejemplos de información que se puede obtener de los metadatos (varía en función del tipo de archivo):

- Fechas relacionadas con el documento
- Usuarios relacionados con el documento
- Información referente a la geolocalización
- Software y/o programas utilizados sobre el archivo





# Tracking

En ocasiones, una amenaza potencial que podemos llegar a sufrir es el tema del “tracking”. Pero no hablo del seguimiento que pueden realizar empresas con fines publicitarios o de marketing, sino del que puede realizar un atacante para recopilar información de un objetivo (que podrías ser tú).

¿Cómo lo haría un atacante?

- **IPgrabber**: recopilación de información sobre tu IP y tu dispositivo.
- **Sniffing**: descubrimiento de información al analizar tu tráfico de red.



**GRABIFY IP LOGGER**

Create or Track URLs



**Wireshark**

# Pelando cebollas: Tor Browser y red TOR

La red TOR es una red de comunicación distribuida cuyo objetivo es aportar una cierta privacidad al usuario y permitir una comunicación fuera de censuras y otras restricciones.

Para poder acceder a la red TOR se puede utilizar el navegador Tor Browser. A pesar de que TOR se diseñó para un fin positivo. Los cibercriminales lo han utilizado para aprovechar la descentralización y cometer sus delitos a través de esta red.



# Otros recursos útiles

Algunos recursos que puedes utilizar para mejorar tu privacidad son:

- **Mail Temporal**: servicios de mail temporal como 10minutemail
- **Mail “Seguro”**: servicios de mensajería “anónimos” como protonmail o tutanota.
- Servicios para **compartir archivos de forma anónima** como onionshare.
- **Generadores de contenido falso**:
  - Para whatsapp: <http://www.fakewhats.com/generator>
  - Para twitter: <https://www.tucktools.com/spoof-tweet>
  - Para facebook: <https://simitator.com/>
  - Para instagram: <https://generatestatus.com/fake-instagram-direct-message/>

¿Preguntas?

*The End*



Curso de Seguridad Preventiva en Internet