



INTRO A LA CIBERSEGURIDAD PREVENCIÓN DE ATAQUES DE INGENIERÍA SOCIAL

A S O C I A C I Ó N U R U G U A Y A
D E C O M P L I A N C E

2 8 D E J U N I O - 9 A M



¿Qué es la ciberseguridad?





Estadísticas relacionadas

Fuente: Cybersecurity Ventures Data. 2023

8 Billones
de USD

Costo de **daños**
hechos por
cibercrímenes en el
2023.

Fuente: Stanford Research 2020

88%
de los
incidentes

De los **incidentes** de
ciberseguridad que
terminan en pérdida
de datos, **se originan**
en errores humanos

Fuente: 2023 Data Breach Report

425
Millones

Personas que han
sido afectadas por la
filtración de datos
en el año 2023.



Estadísticas sobre la Ingeniería Social

Fuente: Anti-phishing Working Group - 2023

5
Millones

Ataques de phishing
que han sido
detectados en el año
2023.

Fuente: Stanford Research 2020

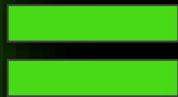
41% de las
personas

De las personas
**hace click en un
correo electrónico**
cuando parece venir
de un **alto ejecutivo**

40% de las
personas

De las personas hace
**click en un correo
electrónico** cuando
parece venir de una
empresa reconocida

¿Qué es un “Hacker”?



El término **HACKER** es aplicado a **cualquier sujeto que intente acceder a DATOS o SISTEMAS INFORMÁTICOS** de manera **no autorizada**.

Tipos de Hackers



White Hat

Fines: Protección

Este tipo de hacker se dedica a **testear** los sistemas informáticos de las compañías con **previa autorización** con el fin de mejorar la seguridad en sus sistemas.

Grey Hat

Fines: Acceso a Datos

Este grupo de hackers busca el **acceso a datos confidenciales** ya sea por consumo personal, con el fin de hacer los datos públicos, o de entregarle los datos a la competencia.

Black Hat

Fines: Ganancias personales

Este grupo busca **usar su conocimiento** para generar dinero ilícito ante la **extracción de datos o infiltración a un sistema informático.**



¿Qué es exactamente la **INGENIERÍA SOCIAL?**

Los ataques por **ingeniería social** se basan en un **conjunto de técnicas** dirigidas a nosotros, los usuarios, con el objetivo de conseguir que **revelemos información personal** a través del uso de **engaños y manipulación**.

MODUS OPERANDI

¿Cómo realizan los **hackers** un ataque?



Investigación

En la primera etapa los Hackers buscan ganar la **mayor información posible** sobre todos los **puntos de accesos** a los **sistemas informáticos** y seleccionan los **puntos más débiles**.

Mucha de la información que usan viene de **páginas web** de las empresas y **redes sociales de sus empleados**.



Generación de Acceso

Después de haber finalizado su plan de acción, los hackers usan **múltiples vectores de ataque para engañar a sus objetivos (los usuarios) o al sistema**. Los vectores de ataque son distintos caminos por los que los hackers generan su acceso.

Algunos ejemplos de las estrategias más comunes de los **atacantes son ataques de fuerza bruta, phishing, ataques troyanos, o incluso ataques por las redes de conexión**.



Explotación

Una vez los hackers logran el acceso al sistema informático, utilizan diversas **herramientas para explotar este acceso**. El término explotar se refiere al hacer uso del acceso para lograr su objetivo planeado. Una vez este acceso es explotado las consecuencias pueden ser tanto la **extracción de datos, como la denegación de servicio**.

Algunos de los “exploits” (herramientas) son malware, ransomware, y spyware.



Limpieza

Al finalizar con su objetivo los hacker hacen una limpieza de sus rastros en el sistema o aplicaciones corrompidas. Para esto alteran el **registro de entrada**, en caso de ser phishing, **eliminan las comunicaciones** que se hayan mantenido, en caso de haber descargado algún tipo de malware **desinstalan este mismo con el propósito de no dejar rastros**.

¿Cómo nos defendemos?

**Aprender a diferenciar ataques y
asegurar nuestras contraseñas**



¿Qué es un ataque de fuerza bruta?



Consiste en **adivinar** nuestra contraseña a base de **ensayo y error**. Los atacantes prueban varias **combinaciones alfanuméricas** secuencialmente hasta dar con la combinación exacta. Por eso cuanto **más caracteres se haya utilizado más se tardará** en dar con la contraseña correcta

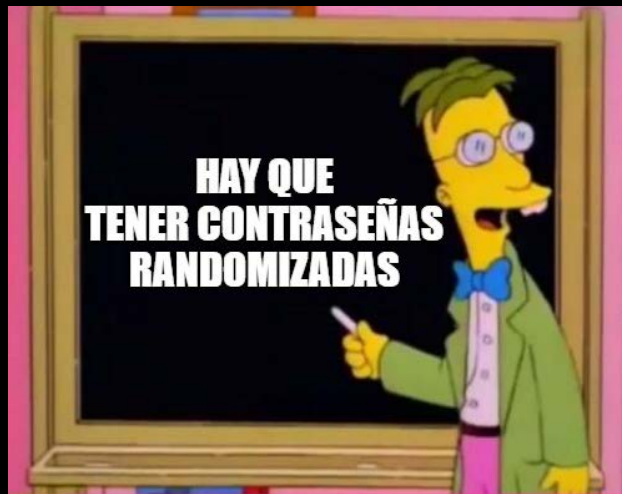
Por ejemplo en un candado de 3 dígitos se prueba el 000, 001 ... hasta llegar al 999, encontrando así la combinación correcta.

¿Qué es un ataque de diccionario?



Los ciberdelincuentes utilizan un software que, de forma automática, trata de averiguar nuestra contraseña. Para ello, realiza diferentes comprobaciones, **empezando con letras simples** y progresivamente, va cambiando a **palabras más complejas**.

Muchas veces se utilizan **palabras relacionadas al usuario y la entidad** a la que está relacionada la cuenta, por eso es importante **no usar información personal** como contraseña.





Construyendo contraseñas seguras

- Menor cantidad de caracteres posibles
- Sólo se utiliza un tipo de carácter alfanumérico
- Incluye palabras relacionadas al usuario o entidad

- Uso de frases o conjuntos de palabras
- Combinaciones de letras en mayúscula, minúscula, número, y símbolos

- Se utiliza al menos 12 caracteres
- Secuencia de caracteres aleatoria
- En caso de usar palabras, usar símbolos para representar letras



Recomendaciones **claves** para las claves

Uso repetido de la misma contraseña

Además de cumplir con los estándares para crear contraseñas fuertes, es importante **no repetirlas** en distintos servicios o cuentas. De este modo si nuestra contraseña es comprometida no estamos dando **acceso a todas nuestras cuentas**.

Bóveda de contraseñas

Las bóvedas o “managers” de contraseñas son documentos que cuentan con encriptación y/o contraseña, con el fin de limitar su acceso. Dentro de él se guardan contraseñas para todos los servicios que si no estuviesen es esta bóveda serían imposibles de recordar.

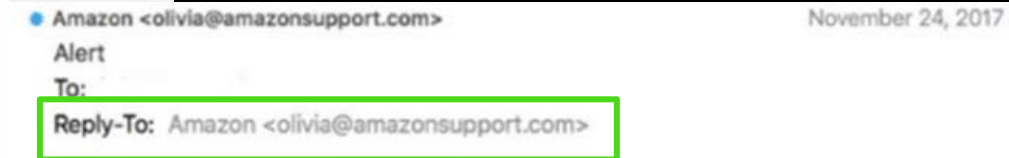
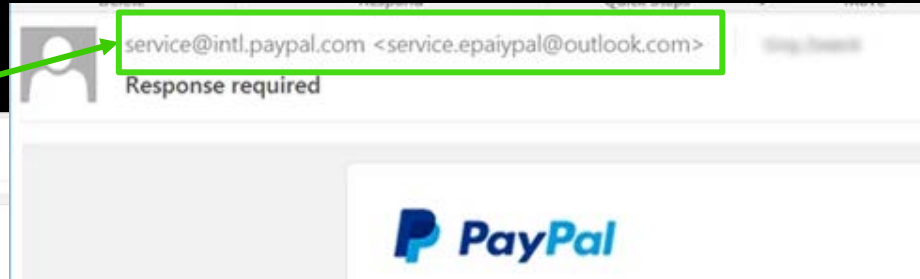
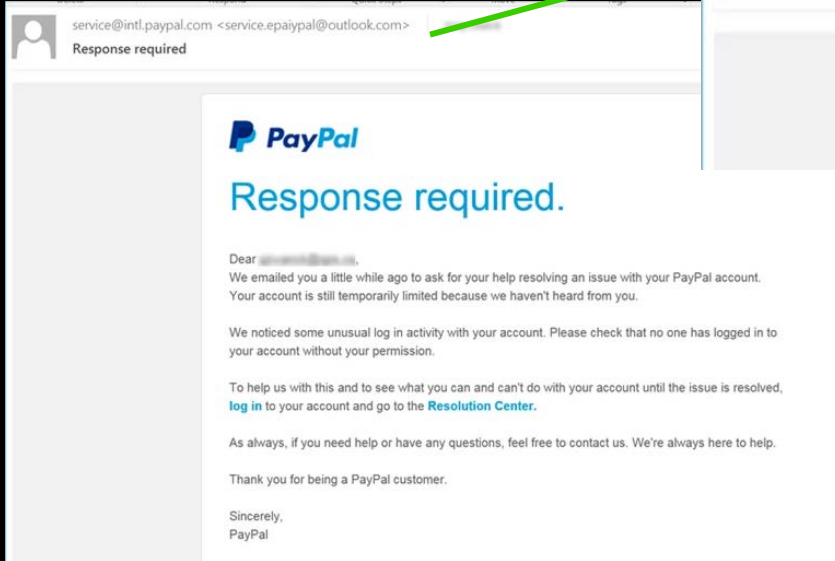
¿Qué es el phishing?



El phishing es un ataque de ingeniería social, en el cual el atacante intenta **engañar** a los usuarios **a través de correos electrónicos**. Usualmente el objetivos de estos ataques son los de **adquirir información personal de los usuarios, infectar a través de distintos tipos de malware o estafar a la víctima**.

Algunos de los derivados del phishing son el whaling, smishing, y vishing.

Ejemplos de Phishing



Password assist

Someone tried to reset your password from **Dayton, Ohio**, If you have not requested this code

Please Call Us on [1-800-801-5811](tel:1-800-801-5811)

Please provide below mentioned code with your Email address to verify

161145

¿Qué es un ataque de troya?



Los ataques troyanos son ataques en los que los hackers intentan **camuflar algún tipo de malware** en algún software legítimo que sea de **interés de los usuarios**.

Estos ataques pueden ser acompañados de **“typosquatting”**, este término se refiere a los **dominios que contienen errores tipográficos usuales**. Un ejemplo sería “gnail.com”.

¿Qué es el malware?



El malware (derivación de software malicioso) es **cualquier tipo de software** desarrollado por un cibercriminal con el **fin de generar daños o destrucción** tanto de computadoras como sistemas de computación.

Los virus son un claro ejemplo de malware aunque el malware no se limita únicamente a virus, por lo que **no todo malware es un virus**.

Virus	programa auto-replicable que va infectando distintos archivos o aplicaciones para propagarse
Ransomware	programa que encripta los archivos de las víctimas con el propósito de que los ciberdelincuentes exijan un pago por la liberación de los archivos
Spyware	programa que se dedica a grabar las actividades de los usuarios con el fin de acceder sus datos personales y/o credenciales.

Medidas físicas de seguridad de la información



Shoulder Surfing

Este término se refiere al “mirar por arriba del hombro”, muchas veces no nos damos cuenta de que la gente de nuestro alrededor nos esta observando. Es importante que al estar en lugares públicos no hagamos uso de nuestras contraseñas o divulguemos datos personales o de la entidad.

Dumpster Diving

Este término se refiere a la técnica de buscar en nuestros residuos. Muchas veces tanto la información (en papel), como los componentes de hardware no son desechados de una manera segura. Para asegurarnos de que nuestra información no sea expuesta, necesitamos usar técnicas seguras.

Casos de estudio

**Análisis de casos recientes, técnicas
para su detección y prevención**

Caso: Hospital Clínic de Barcelona



Resumen

En marzo de 2023, el Hospital Clínic de Barcelona sufrió un ciberataque en el que **se utilizó un virus y un ransomware** con el propósito de dejar **inoperativo su sistema informático y extraer sus datos**.

Si bien este ataque no logró paralizar la totalidad de la actividad del hospital, sí **provocó la interrupción de servicios básicos** como urgencias. Más allá del impacto en la operativa diaria, cabe señalar que el incidente también **supuso la filtración de datos personales sensibles**, con los que los ciberatacantes intentaron extorsionar al Hospital Clínic por una suma de 4,2 Millones de euros.

Caso: Hospital Clínic de Barcelona



Aprendizaje

Los vector de ataque utilizado por los hackers de la organización RansomHouse fue la explotación de la debilidad de una contraseña en las credenciales de autenticación de un trabajador. A esta contraseña se le hizo un **ataque de diccionario**, y se logró dar con la contraseña porque esta misma **contenía una palabra ligada al hospital**.

Como consecuencia de este ataque se adoptaron medidas de ciberseguridad que integren todo el sistema sanitario. Además se adoptaron políticas de contraseñas que incluyen la **prohibición del uso de palabras relacionadas al hospital y el uso de símbolos**. Como medida extra se colocó una **doble autenticación** para acceder al sistema.

Caso: Snowflake



Resumen

Snowflake es una empresa que ofrece el **servicio de almacenamiento de datos en la nube**. A principios de este año sufrió un ciberataque resultando en que las bases de datos de sus clientes fueron expuestas a los cibercriminales. Algunos 165 clientes son el Banco Santander y la empresa americana Ticketmaster

Según algunas de las entrevistas que se han hecho a miembros de la organización responsable por el hackeo, pudieron generar este acceso a través de un **ataque troyano**. Luego de la ejecución del mismo hicieron movimientos laterales en los servidores de la empresa y dieron con **toda la información de sus clientes**.

Caso: Snowflake



Aprendizaje

En este caso, si bien la víctima de el ataque fue la empresa Snowflake, los **datos filtrados pertenecen a sus clientes** los cuales decidieron tercerizar este servicio de almacenamiento de datos.

Dado al contexto, podemos aprender de **tres distintas perspectivas**, desde el punto de vista de snowflake, desde la visión de sus clientes, y por último como consumidores finales. Los procesos de prevención para cada una de las partes incluyen, **políticas de uso aceptable** por parte de la empresa y énfasis en la ciberseguridad hacia sus empleados, **controles de tercerización y monitoreo** constante a las prácticas de seguridad de los servicios contratados, por ultimo **análisis de seguridad y confiabilidad del manejo de nuestros datos personales**.



MUCHAS GRACIAS POR ACOMPAÑARNOS

A S O C I A C I Ó N U R U G U A Y A D E
C O M P L I A N C E

L I N K E D I N : S E B A S T I A N S A B E L L A