



**ATTACK
SIMULATOR**



**ATTACK
SIMULATOR**

Páginas de Educación



**ATTACK
SIMULATOR**

Conciencia educativa

1. Malware

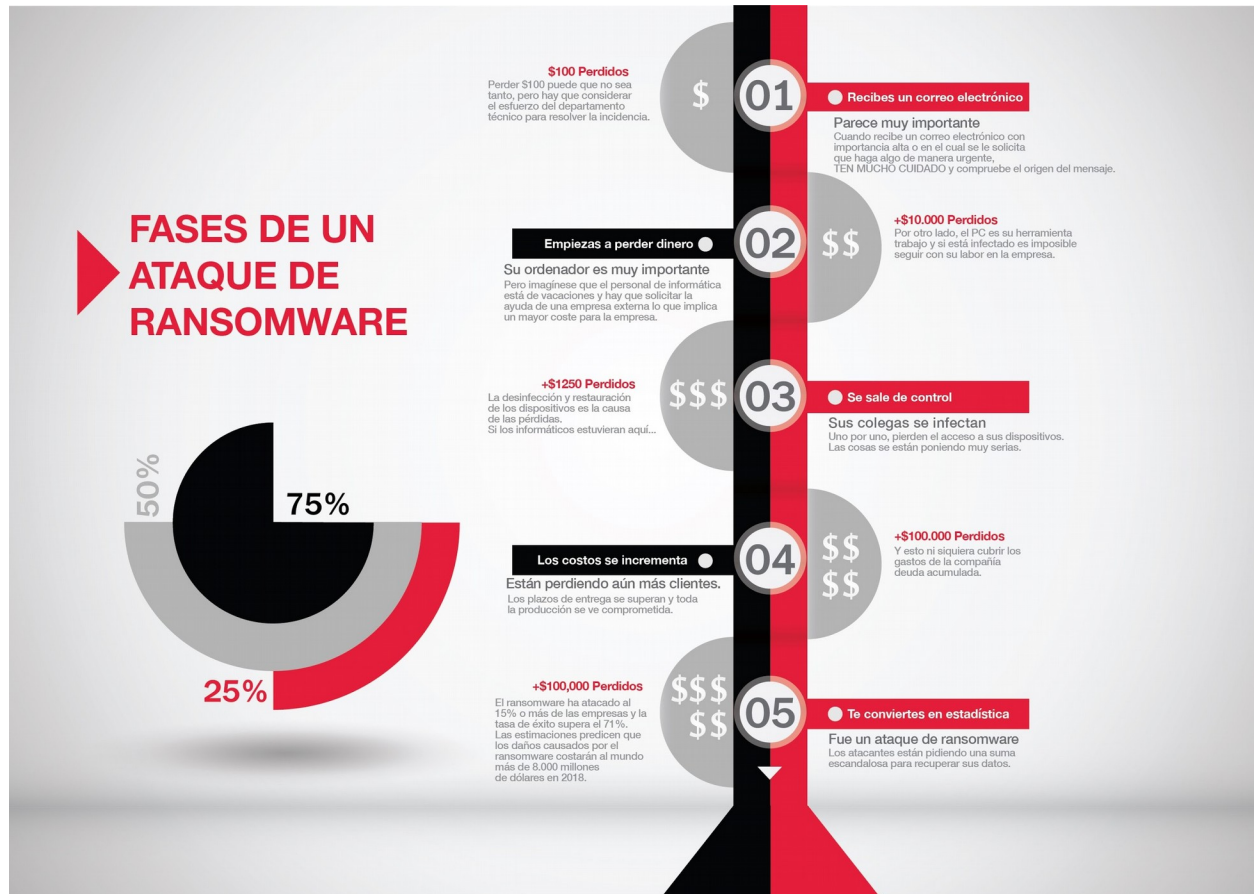
1.1 Impacto de malware





ATTACK SIMULATOR

1. 2 Fases de un ataque de ransomware





**ATTACK
SIMULATOR**

1.3 Malware - video

<https://www.youtube.com/watch?v=rvTrFuXUoN4>

Ataques de Malware

Watch later Share

0:00 / 1:27

YouTube

- ✓ El malware es un tipo de ciberataque.
- ✓ Las descargas son la forma principal a través de la cual el malware llega a usted.
- ✓ Los atacantes pueden engañarle para descargar diferentes archivos.
- ✓ La mayoría de los ataques de malware dan la impresión de urgencia.
- ✓ Los correos electrónicos son la principal fuente de malware.
- ✓ Preste atención a todos los correos electrónicos que reciba y edúquese sobre los ataques de malware



ATTACK SIMULATOR

1.4 Vectores de Ataque de Correo



ATAQUES VÍA CORREO ELECTRÓNICO

Un correo electrónico es, la mayoría de las veces, su primer encuentro con un potencial ataque cibernético. También es el mejor momento para detectarlo y evitar ser víctima de un ciberataque. A continuación, le presentamos los principales elementos que debería analizar cuando recibe un correo electrónico.

Pago rechazado - ¡Se requiere actualización inmediatamente!

From: **AppleCustomers Support** <support_for_customers@apple.com>

To: **me** <maria@email.com>, **John** <john@email.com>, **Jennifer** <jennifer@email.com>

11:30 PM (2 horas atrás)

Estimado usuario de Apple,

Nos hemos enterado de que su cuenta ha sido suspendida debido a un fallo en su cuenta. pago declinado

Una actualización de su información personal es requerida inmediatamente.

Haga clic aquí para revisar su información:

<https://www.applesupports.com/account-update>



<http://www.45apple.com/index>

Después de las próximas 24 horas, su cuenta será desactivada, a menos que usted actualice su información personal.

Saludos cordiales,
Apple Customer Support

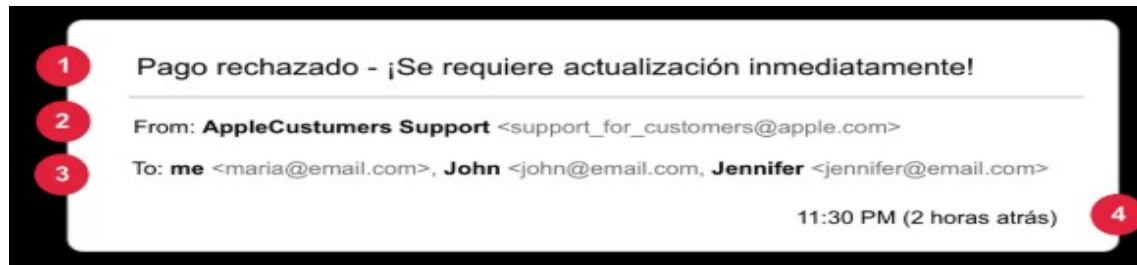


apple-customers-invoice.zip

[Download](#)



ATTACK SIMULATOR



1 EL CAMPO 'ASUNTO'

- ¿La información del asunto está relacionada con el contenido del mensaje?
¿Es relevante?
- ¿Parece una respuesta a otro correo electrónico que nunca ha enviado?
- ¿El asunto **hace referencia a una tarea URGENTE poco habitual** para este tipo de mensajes?

2 EL CAMPO 'DE'

- ¿**Conoce al remitente del correo?** ¿Alguien de su entorno familiar, amigos o compañeros del trabajo?
- Debe preguntarse si el remitente del mensaje, aunque le suene familiar, le contactaría para las tareas o los asuntos indicados en el correo. Si generalmente no suele recibir este tipo de mensajes, es recomendable prestar atención a todos los elementos para descartar que se trate de una estafa.
- **La dirección del remitente podría indicar nombres o marcas reales, pero están escritas de forma atípica** (por ejemplo, @netflix-customers.com).
- También debe prestar más atención a los correos electrónico donde **desconoce al remitente**, o si no tiene ninguna relación con la empresa que envía el mensaie.

3 EL CAMPO 'PARA'

- **El correo electrónico se envía a una lista muy larga de personas desconocidas** y lo normal sería no estar copiado como destinatario.
- Enviaron el correo electrónico a varias personas de la empresa pero que habitualmente no están relacionadas con el tipo de asunto indicado en el mensaje.

4 FECHA

- ¿Ha recibido el correo en **horas inusuales** o fuera de su horario de trabajo?
¿Tal vez en un momento muy atípico, incluso para una emergencia?



ATTACK SIMULATOR


Estimado usuario de Apple,

5 Nos hemos enterado de que su cuenta ha sido suspendida debido a un fallo en su cuenta. pago declinado Una actualización de su información personal es requerida inmediatamente.

6 Haga clic aquí para revisar su información:
<https://www.applesupports.com/account-update>
<http://www.45apple.com/index>

Después de las próximas 24 horas, su cuenta será desactivada, a menos que usted actualice su información personal.

Saludos cordiales,
Apple Customer Support

7  apple-customers-invoice.zip
[Download](#)

5 CONTENIDO

- Prestar mucha más atención a los mensajes de correo electrónico en los cuales se les **solicita realizar ciertas tareas con urgencia**.
- El correo electrónico tiene muchos **errores de ortografía y gramática**.
- El remitente le insta a abrir un **archivo adjunto** para validar algunos datos importantes o revisar un documento supuestamente interno.

6 ENLACES

- **Preste mucha atención a la información que se muestre en pantalla cuando pasa el ratón por encima de los enlaces incluidos en los mensajes electrónicos.** Si son diferentes a las direcciones esperadas es mejor descartar los mensajes o consultarse con su departamento de TI.
- Recomendamos también **descartar los correos electrónicos sin contenido** pero que incluyen simplemente un enlace largo, sin más explicaciones.

7 ADJUNTOS

- **Prestar siempre atención a los archivos adjuntos** y en especial a los que no está relacionados en absoluto con el asunto o el contenido del correo electrónico.
- **Revisar siempre los nombres de los archivos, así como el tipo de extensión que tienen.** Los archivos con doble extensión o ejecutables (por ejemplo exe) es mejor analizarlas antes con una solución antivirus antes de abrirlas o simplemente descartarlas si no tienen mayor importancia para Ud.



ATTACK SIMULATOR

1.5 Comparación de Correos Electrónicos

i VULNERABILIDADES DE UN CORREO ELECTRÓNICO

La mayoría de las cosas en la vida son fáciles de diferenciar. ¿Pero qué tal un correo electrónico de ataque cibernético y un uno real? ¿Qué tan fácil es distinguirlos para usted? ¿No está seguro de qué es lo que hace que un correo electrónico sea real? No se preocupe, ¡estamos aquí para ayudarte! Aquí están las principales diferencias entre un correo electrónico real y uno enviado por un atacante cibernético.

Después de estudiar la siguiente información, debe estar preparado para tomar la decisión correcta cada vez que reciba un correo electrónico.

Por favor, actualice sus datos de pago

From: **Apple Support** <noreply@email.apple.com>

To: **me** <maria@email.com>

11:30 AM (2 hours ago)



Estimada Maria,

Hemos notado que los detalles de pago de tu cuenta de Apple no han sido actualizados después de que se haya actualizado la opción última notificación.

Si todavía está interesado en utilizar los servicios personalizados de su cuenta, por favor visite el enlace y revise su información personal.

<https://www.apple.com/account-update>

<http://www.apple.com/account-update>

Usted todavía tiene 7 días hasta que su cuenta sea suspendida debido a la inactividad.

Saludos cordiales,
Apple Customer Support



ATTACK SIMULATOR

Pago rechazado - ¡Se requiere actualización inmediatamente!

From: **AppleCustomers Support** <support_for_customers@apple.com>

To: **me** <maria@email.com>, **John** <john@email.com>, **Jennifer** <jennifer@email.com>

11:30 PM (2 horas atrás)

Estimado usuario de Apple,

Nos hemos enterado de que su cuenta ha sido suspendida debido a un fallo en su cuenta.
pago declinado

Una actualización de su información personal es requerida inmediatamente.

Haga clic aquí para revisar su información:

<https://www.applesupports.com/account-update>



<http://www.45apple.com/index>

Después de las próximas 24 horas, su cuenta será desactivada, a menos que usted actualice su información personal.

Saludos cordiales,
Apple Customer Support



apple-customers-invoice.zip

[Download](#)



ATTACK SIMULATOR



1 EL CAMPO 'ASUNTO'

- Por lo general, un correo electrónico falso tiene un tema que parece ser muy urgente y ruidoso. Se podría anunciar que ganó algo inesperadamente o que alguien recientemente hackeó su cuenta. No se apresure por la escasez del tiempo. Solo después de analizar el correo electrónico, tome la decisión de hacer clic en los enlaces o descargar el archivo adjunto.

2 EL CAMPO 'FROM'

- Espere que se envíe un correo electrónico falso desde una dirección de aspecto extraño y difícil de leer, como ddx22kab@custom-service.com o de un imitador, sospechoso, similar a gmail-support@support.com

3 EL CAMPO 'TO'

- Como puede ver, un correo electrónico enviado por un pirata informático generalmente puede tener varios correos electrónicos con CC junto con el suyo. La mayoría de las veces no conoce a la gente que también recibió el mismo correo electrónico y el hacker solo espera que al menos algunos de ustedes caigan en la trampa.

4 FECHA

- En general, los atacantes cibernéticos viven en una zona horaria diferente a la suya, por lo que probablemente le envíen correos electrónicos a horas extrañas de lo que está acostumbrado.
- Las compañías respetuosas solo envían correos electrónicos entre las horas de trabajo y evitan molestarlo en horas inesperadas, incluso para ofertas especiales.



ATTACK SIMULATOR

Estimada Maria,

5 Hemos notado que los detalles de pago de tu cuenta de Apple no han sido actualizados después de que se haya actualizado la opción última notificación.

Si todavía está interesado en utilizar los servicios personalizados de su cuenta, por favor visite el enlace y revise su información personal.

6 <https://www.apple.com/account-update>

<http://www.apple.com/account-update>

Usted todavía tiene 7 días hasta que su cuenta sea suspendida debido a la inactividad.

Saludos cordiales,
Apple Customer Support

7

Estimado usuario de Apple,


5 Nos hemos enterado de que su cuenta ha sido suspendida debido a un fallo en su cuenta. pago declinado
Una actualización de su información personal es requerida inmediatamente.

6 Haga clic aquí para revisar su información:
<https://www.applesupports.com/account-update>

<http://www.45apple.com/index>

Después de las próximas 24 horas, su cuenta será desactivada, a menos que usted actualice su información personal.

Saludos cordiales,
Apple Customer Support

7  apple-customers-invoice.zip
[Download](#)



ATTACK SIMULATOR

5 CONTENIDO

- ¿Sabía que muchos hackers viven en países que no hablan inglés y que a menudo cometen errores de ortografía? Tenga cuidado con tales errores y tómelos como una señal de advertencia para la credibilidad de un correo electrónico.
- No podemos enfatizar lo suficiente la apariencia profesional de un correo electrónico enviado por una empresa respetuosa y el gran signo de advertencia que trae la falta de tal apariencia.

6 HIPERENLACES

- Comprobación de un hiperenlace es bastante fácil. Pase el cursor sobre el enlace en el correo electrónico y verifique si el enlace a es diferente al que se muestra. Esto sería una gran bandera roja y una señal obvia para que no haga clic en ella.

7 ADJUNTO

- La bandera roja más grande de un correo electrónico falso, en lo que respecta a los archivos adjuntos, es la falta de relación con el resto del correo electrónico. Podría darse el caso de que algunos de ellos no estén allí o que no sean lo que usted esperaba que fueran (es decir, espera recibir una imagen pero recibió un archivo .exe).
- Los accesorios de baja calidad son otro problema común. A menudo, los archivos adjuntos son solo imágenes de lo que deberían ser, por lo que están mal hechos.



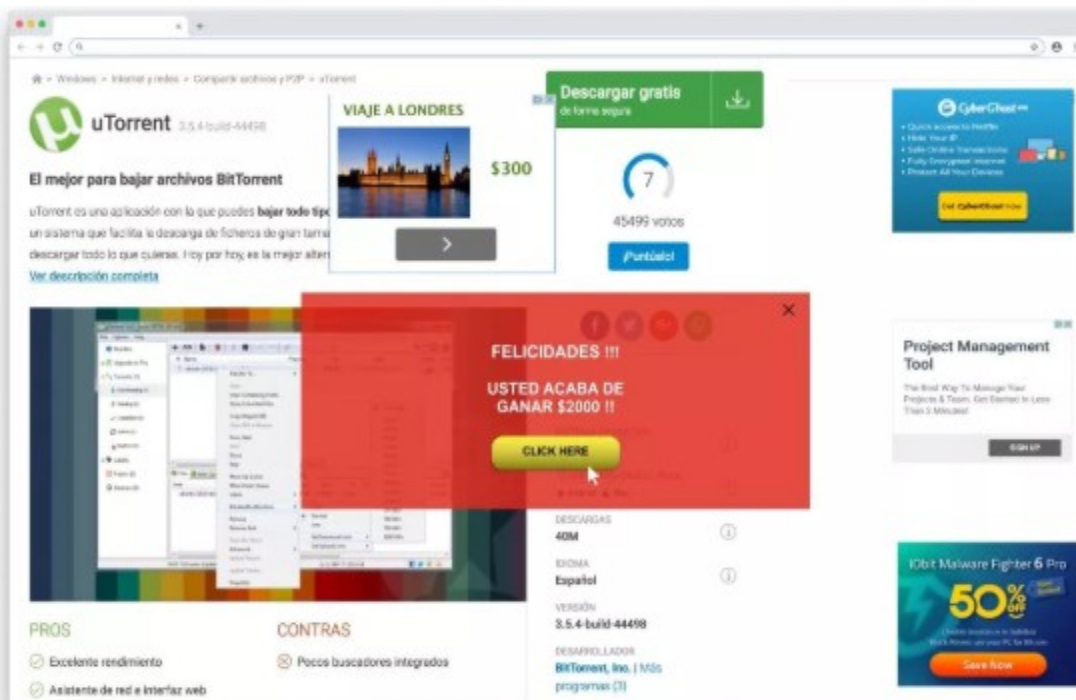
ATTACK SIMULATOR

1.6 Vectores de Adware

i VULNERABILIDADES DEL ADWARE

Adware es **un tipo de MALWARE** diseñado para mostrar publicidad en su computadora, para recopilar información sobre su comportamiento en línea y para redirigir sus solicitudes a otros sitios web relacionados con la publicidad.

A continuación tiene un ejemplo de cómo podría verse una página web de adware:





ATTACK SIMULATOR

- ✔ **Los anuncios emergentes** son un tipo de adware a través del cual el malware puede infectar su computadora. A veces, los anuncios emergentes pueden tener **botones de cerrar falsos**. Cuando hace clic en estos “botones de cierre” simulados, en realidad **se le redirige a otra página web**.

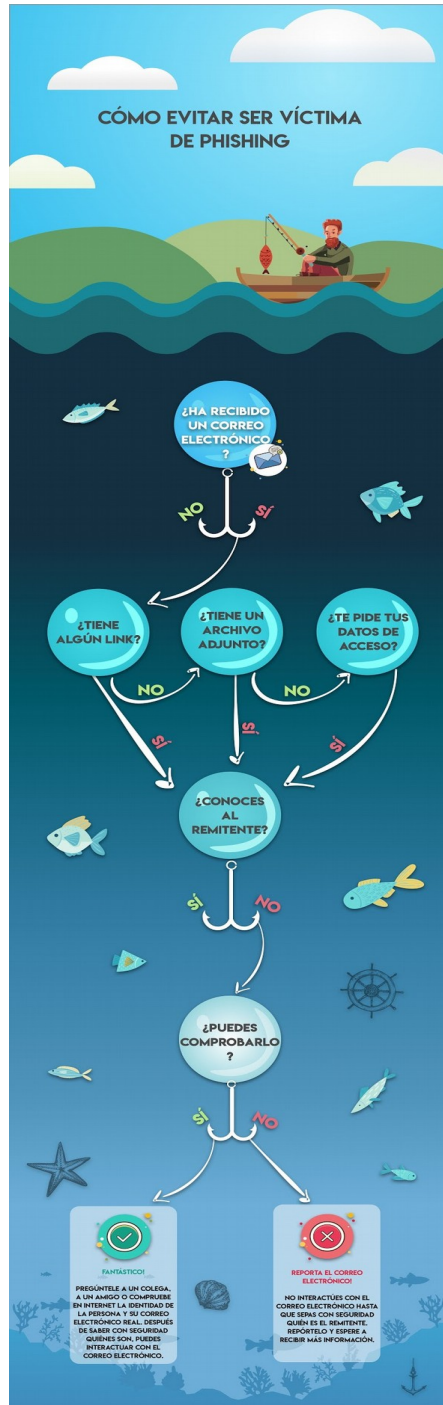
- ✔ Las tecnologías de hackers se utilizan a menudo. Por ejemplo, **su navegador puede ser vulnerable** y, como efecto, los troyanos pueden infectar su computadora.

- ✔ La mayoría de las veces puede encontrar sitios web de programas publicitarios inflados cuando intenta descargar software ilegal o escuchar música o ver películas de manera ilegal. Los piratas informáticos aprovechan su interés en dicho software y lo dirigen a través de otras páginas web que pueden aportarles dinero.

- ✔ **Le recomendamos que tenga de los anuncios en los en los que haga clic y evite descargar software sin licencia.**



ATTACK SIMULATOR





ATTACK SIMULATOR