

## Correos Mentirosos "pirateé tu cuenta"

Desde la SeTIC se les informa que hace varias semanas estan llegando mails "Mentirosos", que indican que han Pirateado o Hackeado su cuenta y otros temas de correo que hablan de videos pornográficos, de una difusión de este material si no se hace un pago por medio de bitcoins y demás.

Confirmamos que estos e-mails mutantes usan el denominado "Ataque por Ingeniería Social" que no es otra cosa que una "Manipulación Psicológica" mostrando cosas que aparentemente conocen de la "Posible Víctima".

De hecho, se muestran como correos que vienen de la propia persona o de personas conocidas.

Hemos detectado varios orígenes desde Argentina y otros lugares y hemos accionado según las normas de Internet.

Además, el detector de SPAM va descartando a medida que "Aprende" de los correos con este formato, pero como el ataque hace una "mutación" de los mensajes en sus diferentes partes, el proceso de eliminación ocurre pero es lento.

Simplemente, no hagan caso a estos correos y bórrenlos sin más. Manténganse atentos y no acepten cualquier información como valedera. Repasen la información sobre el tema en las "Recomendaciones" del Menú "SETIC" en la parte Superior Derecha de la página Web de la Facultad ... Gracias !!!

### Información

Desde la SeTIC se les informa que las PCs que cuentan con Sistema Operativo Windows 10 están recibiendo una actualización importante desde Microsoft, por lo que puede ocasionar la ralentización del equipo y la red, y reinicio del equipo, y/o algunas fallas en las configuraciones una vez actualizado. Así mismo les informamos que estamos atentos a esto, y que ante cualquier inconveniente puede comunicarse a la Mesa de Ayuda marcando el interno "6". Gracias.

## **Recomendaciones**

### **Protegerse de correos de suplantación de identidad (phishing)**

Un correo de suplantación de identidad (phishing) es un mensaje que parece legítimo, pero es un intento de obtener información personal o robarle dinero.

- No responda nunca a un correo que le pida que envíe información personal o de sus cuentas.
- Si recibe un mensaje que parece sospechoso o en el que le piden este tipo de información, no haga clic nunca en vínculos que se supone le llevarán a un sitio web de empresa.
- No abra nunca ningún archivo adjunto a un correo electrónico de aspecto sospechoso.
- Si el mensaje parece proceder de una compañía, póngase en contacto con el servicio al cliente de la compañía por teléfono o mediante un explorador web ver si el correo electrónico es legítimo.
- Busque la línea de asunto del correo electrónico seguida del término "información falsa" en la web para ver si alguna otra persona ha informado de esta estafa.

Si cree que ha sido objeto de suplantación de identidad (phishing), notifique el correo electrónico seleccionando la flecha situada junto a Correo no deseado y eligiendo una de las siguientes opciones.

- Correo no deseado Use esta opción para correo rutinario no deseado.
- Suplantación de identidad (phishing) Use esta opción en caso de un mensaje que intenta inducirle a que dé información personal, como, por ejemplo, su contraseña, datos de cuentas bancarias o el número de la seguridad social.
- Pirataron la cuenta de mi amigo Use esta opción si empieza a recibir correo electrónico no deseado o correos de suplantación de identidad (phishing) de un remitente en el que normalmente confía.

## Seis tipos de estafas comunes

A continuación mostramos seis de los tipos más comunes de estafas, junto con sugerencias adicionales sobre cómo reconocerlas.

### "¡Compruebe su cuenta ahora o se le cerrará!"

**El fraude:** Recibe un correo electrónico que parece ser de su banco, un servicio de comercio electrónico como PayPal o eBay o su proveedor de correo electrónico que le advierte de que su cuenta se suspenderá o cerrará a menos que la "verifique" respondiendo con su información de cuenta.

**Lo qué busca el timador:** En el caso de delitos de banco o comercio electrónico, quieren su información personal para robarle la identidad, vaciar sus cuentas bancarias y realizar cargos en su tarjeta de crédito. Si supuestamente se trata de su proveedor de correo electrónico, el timador quiere el nombre de usuario de su cuenta de correo electrónico y la contraseña para hacerse con su cuenta y enviar correo electrónico no deseado.

**Pistas adicionales de que se trata de un fraude:** Requiere una respuesta urgente (por ejemplo, "Debe comprobarlo en menos de 24 horas"). Esto le da poco tiempo para investigar si

es legítimo.

**Acciones que puede realizar:** En primer lugar y más importante, no responder con información personal o de la cuenta, independientemente de lo graves que suenen las advertencias.

- Si se trata de un banco o un sitio de comercio electrónico, póngase en contacto con el departamento de servicio del cliente de la compañía por teléfono o en línea para ver si el correo electrónico es legítimo.
- Si dice ser de Outlook.com, reenvíe el correo electrónico a [report\\_spam@outlook.com](mailto:report_spam@outlook.com).

**"Una gran cantidad de dinero puede ser suyo, solo tiene que enviar su información personal o algo de efectivo".**

**El fraude:** Hay dinero en una cuenta bancaria que una persona con aire oficial desea compartir con usted. Todo lo que debe hacer es enviarle su información personal o dinero.

**Lo que busca el timador:** A veces, simplemente quieren que les envíe dinero. Otras veces, quieren su información personal para robarle la identidad, vaciar sus cuentas bancarias y realizar cargos en su tarjeta de crédito.

**Pistas adicionales de que se trata de un fraude:**

- Cualquier trato que implique un banco internacional o en el que deba enviar su información personal o dinero a otro país es sospechoso.
- A menudo se trata de un robo. Tal vez el dinero no sea suyo, sino que su auténtico propietario haya fallecido, o sea de un oficial corrupto, o de alguna empresa anónima que no lo echará de menos. O quizá sí sea suyo, pero alguien intenta robárselo.
- Si hay algo sospechoso en el trato o no entiende por qué alguien a quien no conoce le hace esta oferta a usted (de entre todas las personas del mundo), puede estar seguro de que se trata de una estafa.

**Acciones que puede realizar:** En primer lugar y más importante, no responder con información personal o financiera, independientemente de lo tentadora que suene la oferta.

- Vaya a un sitio web dedicado a desacreditar estafas como snopes.com y busque el asunto del correo.
- Informe sobre el correo como una estafa de phishing (ver arriba).

**"¡Es usted el ganador!"**

**El fraude:** ¡Enhorabuena! ¡Le acaba de tocar la lotería! ¡O Microsoft ha realizado un sorteo y ha ganado el premio gordo!

**Lo qué busca el timador:** Información personal para poder robar su identidad y vaciar sus cuentas bancarias.

**Pistas adicionales de que se trata de un fraude:**

- No ha dado su consentimiento para participar en la lotería o en un sorteo.
- Le piden información de su banco para poder realizar un ingreso directo.
- El propósito del sorteo es que la empresa pueda recopilar su información personal cuando entre. A continuación, venderán esa información o la utilizarán para venderle productos y servicios. Ningún sorteo real le pedirá que introduzca su información, pues ya lo hizo en su momento.

**Acciones que puede realizar:** En primer lugar y más importante, no responder con información personal o financiera, independientemente de lo tentadora que suene la oferta.

- Vaya a un sitio web dedicado a desacreditar estafas como snopes.com y busque el

asunto del correo.

- Informe sobre el correo como una estafa de phishing (ver arriba).

**"¡Socorro! ¡Estoy atrapado!"**

**El fraude:** Un amigo suyo está de vacaciones y se quedó atrapado. Necesita que le envíe dinero, ¡rápido!

**Lo que busca el timador:** Que le envíe dinero.

**Pistas adicionales de que se trata de un fraude:** Esto puede ser más complicado de identificar. Normalmente, el timador habrá pirateado la cuenta de correo electrónico de su amigo y enviado este correo de emergencia a toda la lista de contactos. La dirección de correo electrónico del remitente estará legítima. Puede que incluso el saludo sea personal ("Querido Alberto"), pero ¿es este mensaje de correo electrónico realmente de su amigo?

**Acciones que puede realizar:** Antes de hacer nada más, haga una comprobación en la vida real.

- Llame a su amigo por teléfono. Si no consigue contactar con él, intente ponerse en contacto con amigos comunes.

- Pregúntese lo siguiente:

- o Es probable que el correo mencione que está desesperado y no sabe a quién más acudir, pero ¿tienen ustedes suficiente confianza el uno en el otro para hacer esta solicitud?

- o ¿Mencionó con anterioridad que se iba de viaje?

o ¿Cuáles son las posibilidades reales de que su amigo se encuentre en la situación que señala el correo electrónico o haciendo lo que menciona?

o ¿Suena como su amigo?

- A menos que pueda ponerse en contacto con su amigo o un amigo común de confianza por algún otro método distinto al correo electrónico, debe asumir que probablemente sea un fraude. Informe del robo de la cuenta de mi amigo (ver arriba).

**"¡Si (no) reenvía este correo electrónico, algo bueno (malo) ocurrirá!"**

**El fraude:** ¡Reenvíe este correo y Microsoft le entregará 500 dólares! ¡Reenvíe esta petición para que Outlook.com siga siendo gratuito! ¡Avisé a todos sus amigos acerca de este terrible virus informático!

**Lo que quiere el spammer:** Hacer viral su correo no deseado y presumir ante sus amigos.

**Acciones que puede realizar:**

- Si el correo es acerca de un virus u otra advertencia de seguridad, vaya al sitio web de su software antivirus y consulte la última información sobre amenazas.
- Vaya a un sitio web dedicado a desacreditar estafas como snopes.com y busque el asunto del correo.
- Informe del mensaje como correo electrónico no deseado (ver arriba).

**Suplantación de identidad o recepción de un mensaje de correo de usted mismo.**

Si recibe un mensaje de correo electrónico de usted mismo y sabe que no lo ha enviado,

informe de él y, a continuación, elimínelo. Los spammers usan una técnica denominada "spoofing" para hacerle creer que es seguro abrir el mensaje.

***Fuente de esta Información: Microsoft Inc.***

## **Novedades de la Secretaría de Tics**

-

### **Nuevo sistema de Administración De Aulas para nuestra Facultad**

Se encuentra Operativo el Nuevo Sistema WEB que permite visualizar la Utilización de las Aulas, la Administración de las Mismas y la Gestión de Solicitudes para usos fuera de Agenda.

El sistema ha sido implementado utilizando herramientas de uso libre en la Nube de Internet vinculadas a aplicación WEB que facilita su uso.

Se cuenta con esquemas de ubicación de las Aulas para una mejor información de Docentes y Alumnos. Para conocer su Uso hacer Click [AQUÍ](#).

-

### **Biblioteca Electrónicas**





