Boletín Informativo

Edición #91

Contenido: Evitemos cualquier intento de estafa / ¿Cómo identificar en redes sociales si un perfil es falso? Pag 5 / Su teléfono celular puede infectarse con virus. Conozca los más comunes Pag 8

Evitemos cualquier intento de estafa

Nuestro país se ha visto afectado en los últimos días por un impacto negativo provocado por eventos relacionados ataques cibernéticos en algunas instituciones.

Eso nos demuestra el avance y la especialización que este tipo de actividades ilícitas están teniendo en el mundo entero.

Vida Plena siempre está al cuidado y resguardo de su información. Pero también es muy importante que cada uno aprenda a prevenir cualquier intención de este tipo.

Si como consecuencia de estos ciberataques llegan a publicarse datos, personas mal intencionadas tendrían más información que les facilitará la credibilidad en su esfuerzo por engañar.

Por su seguridad le invitamos a seguir estas recomendaciones:

1. Identificar mensajes sospechosos

- Existen algunos aspectos que ayudan a identificar este tipo de mensajes:
- Utilizan nombres y adoptan la imagen de empresas reales
- Incluyen sitios web que visualmente son iguales a los de empresas reales
- Solicitan datos personales, contraseñas, números de cuenta, etc.
- Incorporan archivos adjuntos que pueden contener programa maligno (virus, ransomware, etc.)

2. Verificar la fuente de los correos o llamadas entrantes

Vida Plena ni ninguna entidad financiera le solicitará nunca que se le envíen claves, números de cuenta o datos personales por correo electrónico o en una llamada telefónica.

Nunca se debe responder a este tipo de preguntas y si se tiene duda se debe terminar la llamada y contactarse directamente con la organización para aclarar la situación.

3. Nunca hacer clic en links incluidos en mensajes de dudosa procedencia

No hacer clic en los hipervínculos o enlaces que se adjuntan en el mensaje ya que de forma oculta podrían dirigir a una web fraudulenta, descargar o ejecutar software malicioso.

4. Nunca abrir un archivo adjunto sospechoso o que no se ha solicitado

Los correos con archivos adjuntos son una de las formas en que el ransomware puede ingresar en los dispositivos. En caso de dudas de un archivo, es mejor no abrirlo.

Nunca se deber abrir un archivo adjunto si, para verlo, se necesita habilitar las macros. Para asegurarse de que un mensaje sea confiable, se deber verificar quién lo envió y que la dirección de correo sea correcta.

5. Nunca usar un dispositivo USB sospechoso o desconocido

Evitar conectar dispositivos USB u otros dispositivos de almacenamiento si no se sabe de dónde provienen o parecen sospechosos.
Los ciberdelincuentes pueden regalar o dejar unidades infectadas en sitios públicos con la intención de que alguien los utilice en su lugar de trabajo o el hogar.

6. Utilizar sitios web seguros

Los sitios web seguros contienen 'https://' en su dirección y de acuerdo con el navegador utilizado puede aparecer el icono de un pequeño candado cerrado.

7. Poner atención al idioma

El phishing y la ingeniería social puede presentarse mediante ataques en cualquier idioma. Es usual notar que los mensajes están mal traducidos, presentan errores ortográficos, carecen de tildes y de una correcta redacción.
Se debe poner especial atención a estos indicadores para juzgar si estamos ante un mensaje malicioso, ya que cada vez es más difícil notar inconsistencias.

8. No arriesgarse

La mejor forma de prevenir es rechazar de forma sistemática cualquier correo electrónico o comunicado que solicite datos confidenciales y comunicarse con el departamento de Tecnologías de Información o con la entidad financiera respectiva.

9. Ser más precavidos

Aun cuando el mensaje provenga de una persona conocida o de confianza debemos ser muy precavidos al hacer clic en links y descargar archivos o enviar información pues la cuenta de correo de esta persona podría estar comprometida.

10. Mantenerse informado

Siempre es conveniente informarse, buscar recomendaciones o consejos para evitar cualquier peligro al utilizar el correo electrónico, aplicaciones para dispositivos móviles, redes sociales e Internet en general.

Las amenazas están en constante evolución por lo que informarse y hacer uso del buen juicio es absolutamente necesario.

¿Cómo identificar en redes sociales si un perfil es falso?

Los ciberdelincuentes pueden hacer mucho daño por medio de perfiles falsos. Pueden perjudicar la imagen de una persona, cometer un delito bajo otro nombre y buscar estafar personas.

Las redes sociales parecen ser en ocasiones un universo paralelo al de la vida real, y a pesar de que muchos lo emplean como medio de desconexión temporal, otros hacen uso de ellas para fines delictivos o maliciosos, como la suplantación de identidad o la creación de un perfil falso.

No es complicado crear perfiles falsos, cuando solo se trata de registrarse bajo unos términos ficticios, a pesar de las políticas de uso que lo prohíbe como en el caso de Twitter, Facebook o Instagram.

Los objetivos principales de los cibercriminales son: perjudicar la imagen de una persona, cometer un delito con otro nombre ya sea el envío de un virus o poner en marcha una estafa o campaña, o acosar a un usuario y extorsionarle.

¿Cómo identificarlos?

Para detectar estos falsos perfiles los usuarios se pueden fijar en ciertas características que les delatan, como el hecho de que su cuenta se centre en una temática única sin tener interacción con otros usuarios. Además, utilizan fotos de perfil de personas atractivas a quienes suplantan o de figuras famosas, como si fueran sus fans. En algunas ocasiones el nombre también es muy extraño, como si fuera extranjero, e incluso la fotografía no coincide con el nombre.

Asimismo, los ciberdelincuentes que se hacen pasar por otras personas que no solo utilizan fotografías de sus víctimas, sino también datos pocos fiables que son incompletos o descripciones copiadas de otros perfiles. Este tipo de acciones ya se están tratando de corregir por mecanismos de verificación.

Las cuentas de reciente creación suelen ser sospechosas cuando se usan para un fin concreto, como apoyar una campaña política, una causa o a una empresa. Pero también existe un mercado en el que se reutilizan antiguos perfiles, lo que significa que hay muchas de segunda mano. Para ver este dato debemos ver la fecha de creación de la actividad en la red social.

También podemos detectar inconsistencias cuando vemos la cantidad de seguidores y seguidos, por ejemplo en Instagram o Twitter. Podemos encontrar disparidad de que un

perfil sigue a muchos pero a él no le sigue nadie, lo que incita a pensar que es un bot. Pero por otra parte, existen cuentas que poseen una cantidad muy elevada de seguidores a pesar de no tener prácticamente ninguna actividad - o es muy reciente-.

El cambio de nombre del perfil, puede ser también una señal. Si lo han cambiado una vez puede ser normal, quizá el nombre no le gustara. Pero si lo han cambiado cuatro o cinco ya es más raro. Si además ha borrado todas las publicaciones anteriores, o ni siquiera las han borrado y antes hablaba de fútbol y ahora de política, entonces hay que sospechar todavía más.

¿Qué debemos hacer si detectamos un perfil falso?

Cuando un usuario se topa con un perfil falso debe proceder a ponerlo en conocimiento de las empresas proveedoras del servicio y de otros usuarios para que **no caigan en sus trampas**. Algunas redes sociales como Twitter o Instagram tienen herramientas integradas para denunciar a estos perfiles. También Facebook permite informe sobre un perfil desde la propia red social.

Su teléfono celular puede infectarse con virus. Conozca los más comunes

Los teléfonos móviles no son ajenos a los virus que circulan por internet, ya sea en la descarga de alguna aplicación o a través de algún mensaje circulando por un sistema de mensajería instantánea.

Los tipos de virus más habituales

'Adware'

Es uno de los más habituales y está relacionado con la **publicidad invasiva**. Es muy molesto para el usuario porque normalmente se manifiesta en el dispositivo a través de continuas ventanas emergentes, complicadas de cerrar en muchos casos. Lo más habitual es que busquen proporcionar ingresos a sus creadores a través de los **clics en las ventanas** pero en ocasiones pueden añadirse al navegador y a partir de ahí hacerse con los datos personales del usuario, tales como contraseñas, cuentas bancarias o números de teléfono de la agenda.

Troyano

Quizá sea el más conocido de todos y toma su nombre prestado del famoso episodio de la Antigua Grecia en el que los griegos entraron en la fortaleza de Troya escondidos en el interior de un enorme caballo de madera. Los troyanos se cuelan en el móvil sin levantar sospechas y abren un acceso desde dentro para **enviar información del usuario** a quien lo ha introducido.

'Spyware'

Puede ser el más peligroso de todos dado que, como su propio nombre indica, esta diseñado para espiar y así sustraer los datos más sensibles del propietario del dispositivo. Su detección también es muy complicada.

Scareware'

Se trata de uno de los virus más conocidos, tanto en los móviles como en los ordenadores, porque se manifiesta a través de pantallas que anuncian que el terminal está infectado y ofrece una solución para limpiarlo. Se trata de un '**sofware' para descargar** o de una redirección a otra página desde donde se cuela el virus. No suele conllevar peligro habitualmente pero es tremendamente molesto.

'Ransomware'

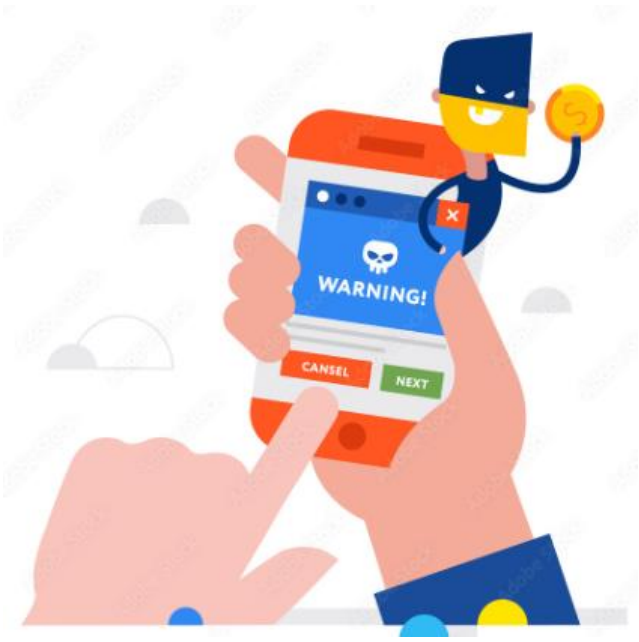
La clase de virus de la que más se ha escuchado hablar en los últimos tiempos por su gran peligrosidad, que llega a **bloquear el dispositivo** sin que su usuario pueda defenderse ante ello. Una vez bloqueado el terminal, los ciberdelincuentes se ponen en contacto con el usuario damnificado pidiéndole el pago de un rescate si desea volver a recuperar los datos o el dispositivo.. En Costa Rica estamos viviendo esta situación en los sistemas del Ministerio de Hacienda.

Gusano

Los gusanos suelen colarse en el terminal a través de ciertos **correos electrónicos** en cadena y tienen una enorme facilidad para reproducirse. Sus dos características más reconocibles son la de que son capaces de consumir la memoria del móvil y que disminuyen en gran medida el ancho de banda de la conexión a internet.

¿Cómo evitar la infección?

Si descarga siempre las 'apps' desde la tienda de aplicaciones de Google (Play Store), lo normal es que su exposición a la amenaza de los virus no sea significativa. El problema es que existe una cierta cultura de instalarse aplicaciones desde fuera del sistema a través de los conocidos archivos .apk, que muchas veces ofrecen atractivos reclamos como el de versiones más novedosas o funcionalidades que no se pueden encontrar en el repositorio oficial y que son la puerta ideal para los ciberdelincuentes.



Otras acciones que conviene llevar a cabo son las de no conectarse a redes públicas wi.fi, como ya mencionamos, descargar solamente aplicaciones de la Play Store, usar métodos seguros de desbloqueo para el móvil como las contraseñas, el sensor de huellas o el reconocimiento facial, no almacenar claves críticas en el teléfono y revisar los permisos que solicitan las aplicaciones antes de descargarse, como las más destacadas.

Cabe también destacar que los móviles de gama baja y, fundamentalmente, los de marcas menos conocidas suelen estar menos preparados para combatir la ciberdelicuencia, ya que invierten menos en seguridad para ser más competitivos en precio y ofrecen menos actualizaciones que las compañías más reconocidas del mercado.