Ciberseguridad: He pinchado en un link fraudulento. ¿Qué hago?

Es muy útil un aviso en las redes sociales para avisar a los contactos y urge cambiar rápidamente las contraseñas y activar la doble verificación.

Avisa a los posibles afectados

Fuente: EL HERALDO.ES

Para contactar con el Instituto Nacional de Ciberseguridad hay que llamar al número gratuito 017 de ayuda en ciberseguridad y se puede contactar también a través de Whatsapp en el 900 116 117 (antes hay que guardar este teléfono en la agenda de contactos del móvil) o en el canal de Telegram @INCIBE017. La persona que ha sido víctima de un fraude de estas características también puede denunciarlo en comisaría y aportar toda la documentación que haya podido recoger en el momento en que se percató del engaño.

Alerta a las autoridades y denuncia

Algunas veces, los delincuentes toman el control de las redes sociales de la víctima para, desde ellas, mandar mensajes de spam o enviar a los contactos nuevos enlaces que les dirijan a webs fraudulentas. Al provenir de alguien conocido es más fácil que los receptores abran los enlaces y se conviertan en nueva víctimas. En el caso de las redes sociales, es muy útil escribir mensajes públicos avisando de que la cuenta ha sido víctima de un ataque. Y a través del correo electrónico se puede avisar a todos los contactos (si ya no podemos acceder porque los delincuentes han cambiado las contraseñas, hay que avisar a la empresa que proporciona el servicio).

Si la contraseña que se facilitó a los ciberdelincuentes es la que utilizamos en varios sitios (redes sociales, bancos o cuentas de correo electrónico) hay que entrar en todos esos servicios lo antes posible, cambiar la contraseña y activar la doble verificación.

Cambia las contraseñas

Esto supone eliminar cualquier archivo que se haya descargado en el móvil y revisar con un antivirus actualizado que el teléfono no esté infectado. Hay que avisar al banco para que se pueda cancelar cualquier pago no autorizado y desactivar la tarjeta bancaria si hay sospecha de que los delincuentes pueden haber accedido a esos datos.

Analiza el alcance de los daños para solucionarlos

Thank you for watching

Hay que recordar qué datos (contraseña de un sitio determinado, número de la tarjeta de crédito...) han obtenido los delincuentes. Si es posible todavía, tenemos que hacer capturas de pantalla de la web fraudulenta y del mensaje que nos haya dirigido a ella y guardarlos en un lugar seguro, por ejemplo, enviándolas a un correo de seguridad que no hayamos proporcionado, de manera que no puedan acceder los delincuentes.

Toma pruebas desde los primeros momentos

¿Qué podemos hacer cuando nos damos cuenta o sospechamos que ese link al que hemos accedido es en realidad un fraude? Estas son algunas de las recomendaciones que ofrecen desde las distintas agencias de ciberseguridad.

Los expertos insisten en que dudemos siempre de cualquier mensaje que redirija a una web en la que haya que introducir nuestros datos, pero los delincuentes han perfeccionando tanto tus tácticas que muchas veces picamos: en el mensaje advierten de la urgencia de entrar en el enlace y proporcionar esa información si no queremos exponernos a una multa, perder un paquete que nos va a llegar por mensajería o que nos bloqueen la cuenta bancaria, por ejemplo.

Son constantes las alertas de las agencias de ciberseguridad y de los cuerpos de seguridad sobre oleadas de estos mensajes de ‘phising’ o ‘smishing’. El primero de estos engaños consiste en enviar a la víctima un email con un enlace que dirige a una página en la que se le pide que introduzca información personal (nombre de usuario, contraseñas, número de tarjeta de crédito...). La víctima generalmente accede, ya que cree que se trata de la web de una empresa con la que tiene relación, pero en realidad es una página trampa que han creado los delincuentes imitando el aspecto de la marca original para conseguir así información de ese cliente y poder suplantar su identidad. El ‘smishing’ es similar, pero en lugar de un correo electrónico los delincuentes envían un mensaje de texto con el link.

Ojo, ciberataque. Y somos todos vulnerables, ya que los ciberdelincuentes atacan cada vez más a los móviles. Lo hacen enviando correos electrónicos y SMS fraudulentos para que pinchemos en algún enlace que nos dejará expuestos.

Sara Borondo

FUENTE: EL HERALDO.ES