AUMENTA EL NÚMERO DE CASOS DE INTENTO DE SEXTORSIÓN DURANTE EL CONFINAMIENTO

- **Los ciberdelincuentes amenazan a la víctima con difundir supuestos vídeos de índole sexual.**
- **En caso de chantaje, nunca se debe pagar la cantidad solicitada y hay que notificar inmediatamente a las autoridades.**

Debido al confinamiento obligatorio por la pandemia del COVID-19, el uso de Internet y de las redes sociales se ha disparado notablemente. Los usuarios están utilizando estos medios para comunicarse con amigos, familiares... Este uso elevado de la tecnología se traduce en el aumento de la probabilidad de sufrir algún intento de estafa, entre ellas las de índole sexual.

Entre estas estafas **destaca el repunte de campañas relacionadas con la sextorsión**, es decir, recepción de correos electrónicos fraudulentos que buscan chantajear a sus destinatarios amenazándoles con difundir un supuesto vídeo de contenido sexual, un vídeo que en la mayoría de las ocasiones no existe. El chantaje consiste en amenazar al destinatario con enviar el archivo a todos sus contactos si no se paga una cantidad de dinero, generalmente en moneda bitcoin, en un plazo de 48 horas.

Para realizar estas campañas, los ciberdelincuentes trabajan habitualmente en grupos organizados cuya actividad se centra en el envío masivo de correos a listados de emails que obtienen a partir de fugas de información públicas en Internet. En la mayoría de los e-mails, intentan asustar a la víctima indicándole que **han estado monitorizando la actividad de su ordenador**, y en algunos casos aluden al acceso a páginas web con contenidos sexuales. Estos e-mails, consiguen llegar a preocupar a los receptores a pesar de no haber realizado ninguna práctica sexual delante de sus ordenadores. Esto es debido a que incluyen alguna contraseña utilizada por los destinatarios de los correos, obtenida anteriormente por los cibercriminales a partir de los listados ya mencionados.

Este tipo de extorsión no conoce edad o género, se trata de un tipo de chantaje en el que se busca obtener dinero y en el que se explota el miedo del destinatario de correo. Por supuesto, pagar el rescate para que el supuesto archivo no se haga público abre la puerta a nuevos chantajes de todo tipo.

info@bcsc.eus | 945 010 059

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz

Así mismo, existen otro tipo de prácticas, que finalmente pueden terminar en un caso de sextorsión, como es el caso del **sexting**. Esta práctica consiste en **enviar mensajes, fotos o vídeos de contenido erótico o sexual personal a través del móvil, email u otro tipo de herramienta**. Generalmente, se suele realizar de manera íntima entre dos personas. El riesgo viene una vez enviadas las fotografías, ya que **se pierde el control** sobre ellas y los demás pueden hacer un uso ilícito del material, chantajeando a la otra persona o incluso amenazándola con hacer llegar el contenido sexual a sus conocidos y familiares.

Consejos para evitar caer en esta estafa

Ante el aumento de casos, desde el Basque Cybersecurity Centre, hemos creado una infografía sobre las estafas de tipo sexting, con toda la información necesaria para actuar si estás siendo víctima de una estafa de este tipo, así como las pautas necesarias para evitar serlo:

- **No abrir nunca un correo electrónico no solicitado o de una persona desconocida**. Generalmente, este tipo de correos se envían de forma masiva sin un destinatario concreto, por lo que responder implica y avisa al ciberdelincuente que la cuenta está activa. El mejor consejo es borrar directamente el email y, por supuesto, no descargar ningún archivo adjunto.
- Igualmente, y del mismo modo, **no se debe contestar a este tipo de correos, mucho menos enviar información personal** a aquellas personas que se puedan conocer en un chat o en una interacción sea del tipo que sea.
- En caso de sufrir algún tipo de extorsión, **no pagar nunca el "rescate", y pedir ayuda a los Cuerpos y Fuerzas de Seguridad**, que disponen de departamentos especializados en este tipo de temas.
- Procura **tener contraseñas seguras y robustas y no reutilices la misma para diferentes cuestiones**. En caso de que los ciberdelincuentes se hagan con una, tendrían vía libre a otros muchos servicios o cuentas que se suelan utilizar.
- **Actualiza siempre que lo solicite el sistema operativo y el antivirus**. En estas actualizaciones se cierran brechas de seguridad que han sido denunciadas y te ayudarán a navegar más seguro.

Además, es importante tener en cuenta, que **en caso de recibir una fotografía o vídeo de otra persona con contenido sexual o erótico, nunca se debe reenviar**, pues de lo contrario se estaría incurriendo en un delito.

Para finalizar, hay que concienciarse de que las formas de actuar que tenemos en la vida real también valen cuando estamos conectados, en especial en

temas tan sensibles como la privacidad personal, de nuestros datos, o simplemente de la preservación de nuestro capital. El sentido común es nuestra mejor arma, y no debería ser el menos común de nuestros sentidos.

info@bcsc.eus | 945 010 059

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz