Tecnología

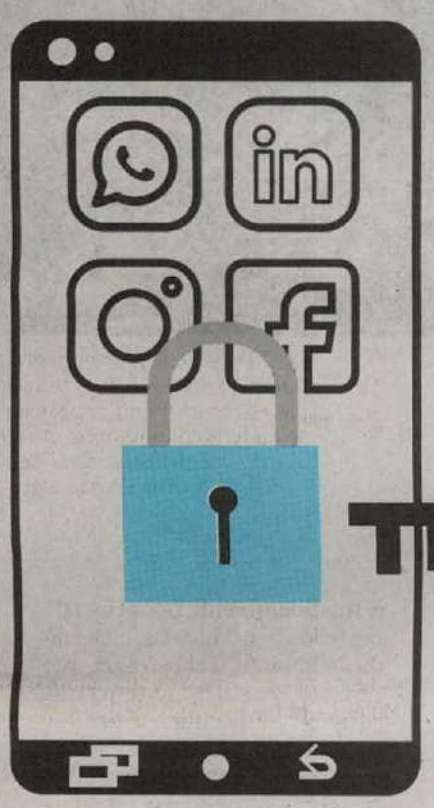
DISNEY APUESTA POR REALIDAD VIRTUAL

Disney aprobó la realización de su segundo cortometraje de realidad virtual, luego del lanzamiento de 'Cycles', un filme dirigido por Jeff Gipson que explora la vida de una familia.

Manual para evitar caer en estafas en redes sociales

Falsas ofertas laborales, cupones para robar su información y *apps* fraudulentas hacen parte del panorama de engaños a los que acuden los cibercriminales.

ANA MARÍA VELÁSQUEZ DURÁN - REDACCIÓN TECNOLOGÍA | @Anamariavd19



Un mensaje privado en LinkedIn sobre una tentadora oferta laboral es uno de los ganchos que usan los cibercriminales para engañar a sus víctimas. Los requisitos del puesto se ajustan a su perfil, y el implicado parece cumplir con todas las habilidades solicitadas en la oferta. Luce como un mensaje real, personalizado y dirigido con exclusividad. Sin embargo, no existe tal oportunidad de empleo y el texto solo hace parte de una estrategia de los atacantes para cumplir dos objetivos particulares: acceder a su información para luego venderla o robarle dinero.

"Muchas veces, la obtención de datos es para perfilar usuarios o para poder armar otro perfil y vender esa información (como los números de teléfono y los correos electrónicos), que luego será usada en ataques de *phishing* o suplantación de identidad", explica William Gómez, experto en seguridad digital de la compañía de seguridad informática Digiware.

En otros casos, se les exige a las víctimas un pago adelantado para supuestamente cumplir con temas administrativos durante el proceso de reclutación y contratación. Una vez se consigna el dinero, el supuesto reclutador desaparece.

Las estrategias de estafa dentro de las redes sociales son variadas e incluyen desde *links* de transmisiones falsas que lo pueden llevar a descargar un código malicioso, hasta un falso cupón de una promoción que llega vía WhatsApp y con la que se busca robarle su información bancaria. Es una realidad: las plataformas digitales se han convertido en una cuna del cibercrimen.

"Pueden hacer también una copia de un perfil real y empiezan a contactar a todos los contactos, diciendo que la mamá está enferma y necesita plata para hacerse un examen", señala Maximiliano Cantis, especialista en seguridad informática de Eset Latinoamérica.

Son ataques que van dirigidos contra las personas, dice Gómez. "No hay un sello de herramientas tecnológicas que nos apoyen y nos protejan de este tipo de ataques", afirma Gómez, quien reitera que la protección más importante proviene del mismo usuario. Es usted quien debe tomar medidas y estar pendiente de qué consulta, qué sitios visita y qué tipo de información comparte en internet.

Tenga en cuenta esta guía de recomendaciones que lo ayudarán a evitar ser víctima de estafas en redes sociales:

Falsas ofertas

Si recibe una oferta laboral en LinkedIn que tal vez promete muchos beneficios, lo mejor es que investigue sobre la empresa y el supuesto destinatario del mensaje. "En primer lugar, hay que buscar la compañía y 'googlearla'. La segunda recomendación es investigar más a la persona que le está pidiendo todos esos datos, verificar si tiene una historia, revisar sus contactos y sus publicaciones y tener en cuenta que jamás le van a solicitar plata para un proceso de selección", afirma Cantis.

Fíjese en la dirección de correo electrónico y verifique que el dominio sea corporativo. "No es común que alguien de recursos humanos tenga un correo con gmail", agrega Cantis. Otra manera sencilla de comprobar la veracidad del mensaje es buscar el nombre de esa persona y verificar si aparece un perfil similar dentro de LinkedIn para descartar que no sea una suplantación, por ejemplo. Por último, si es necesario llame directamente a la empresa para comprobar sobre la oferta laboral.

Ojo con las promociones

Dude de las ofertas que le lleguen por cualquier servicio de mensajería como WhatsApp. Confirme siempre en los sitios oficiales si esa promoción es efectivamente real. "Hay campañas en las que le piden llenar los datos y meter la contraseña para así poder robarle su cuenta de Instagram, por ejemplo", dice Cantis. Se recomienda activar la opción de verificación de dos pasos en servicios que dispongan de esta opción.

En algunos casos pueden pedirle instalar una aplicación para acceder a la información. "Parece una *app* normal, pero por debajo están haciendo una serie de actividades maliciosas", dice Gómez.

En agosto de 2018, fue difundida una falsa campaña en la que supuestamente la marca de ropa deportiva Adidas estaba reclutando 'embajadores' e 'influenciadores' en el país para promocionar contenido. Los usuarios debían seguir una cuenta en Instagram y tener al menos 200 seguidores en esa red social. El objetivo era promocionar una cuenta de Instagram para luego venderla.

Sea precavido

Revise la configuración de privacidad de todas sus redes sociales. No solamente verifique qué tipo de información es pública, sino que además identifique qué datos están tomando las aplicaciones que tiene conectadas a esas plataformas.

"A veces, los usuarios no se dan cuenta y dan permisos demasiado amplios, por lo que terminan robando información de los contactos. Eso puede llevar a que terceros sepan los hábitos de consumo o las páginas que generalmente visitan, etc., y a partir de ahí se pueden hacer muchas cosas. Si admiten ciertos permisos, podrían desde explotar alguna vulnerabilidad y llegar a tomar control del dispositivo hasta robar información o fotos y utilizar el celular para temas de criptominería", dice Gómez.

Publique lo necesario

Evite publicar en redes sociales información sensible, como fotos de su cédula, su pasaporte o tiquetes aéreos de sus viajes. "Deberíamos dejar de compartir absolutamente todo, ser moderados a la hora de subir información a las redes sociales y limitar el acceso a las fotos y otros datos. Uno de cada dos usuarios en redes sociales publica su número telefónico, pero tenga en cuenta que si tienen su teléfono y su nombre, ya pueden enviarle un engaño personalizado mediante WhatsApp", afirma Cantis.

Lo básico

Existen unas características básicas que lo pueden ayudar a identificar en cualquier red social cuando una cuenta es falsa. "Normalmente, la foto de perfil no es de una persona, sino de una mascota o de un artista; si tiene pocas fotos o una sola también es sospechoso", afirma Cantis. Es conveniente que revise la cantidad de contactos que tiene el usuario y sospeche cuando este número sea muy bajo. Si la persona genera poco contenido propio y comparte información repetitivamente, puede que se trate de una cuenta bot, es decir, un programa informático que publica automáticamente.

BREVES NOTICIAS DE

Telecomunicaciones

El 5G impulsa ganancias

Xilinx sorprendió a los analistas al mostrar ganancias mejores que las esperadas en el deprimido paisaje de la producción de semiconductores. La explicación del éxito de la firma china es haber logrado aprovechar las fases tempranas del 5G. Mientras la atención se dirige a los resultados en ventas proyectados para 2020, los analistas creen que muy pronto, otras compañías del sector comenzarán a mostrar los beneficios de su apuesta por las redes de quinta generación. REUTERS

Economía

Tecnológicas revelarán resultados financieros

Los principales grupos tecnológicos estadounidenses presentarán sus resultados financieros esta semana y ofrecerán una visión de conjunto de un sector que atraviesa un periodo turbulento. Apple, afectada por un estancamiento en las ventas de sus iPhone, será la primera en informar sobre sus ingresos hoy, seguida de Facebook y Microsoft.

Regulación

Facebook, a responder en el país

La Superintendencia de Industria y Comercio emitió una orden preventiva para Facebook a fin de que en cuatro meses implemente medidas de seguridad en protección de datos para los 31 millones de usuarios colombianos, so pena de incurrir en la sanción de dos mil salarios mínimos.