

¡Ojo con el coronavirus virtual!: advierten por el uso del home office y las estafas en la web

19 marzo, 2020

El titular de la Unidad Fiscal Especializada en Ciberdelincuencia dio consejos para estar alerta ante el uso de la pandemia para robar datos personales: “Muy atentos a lo que parece tentador y urgente”.

El coronavirus tiene su versión virtual en forma de estafa. Todavía no se conocen casos en Argentina, por lo menos denunciados, pero sí en otros lugares del mundo. Hackers que usan herramientas digitales para cometer delitos –como robo de datos personales y bancarios– aprovechando el miedo o la búsqueda de información por la pandemia del virus.

“Siempre que hay situaciones excepcionales –y hoy estamos ante una de ellas y en todo el mundo– que suelen aprovechar los estafadores y las organizaciones criminales para lucrar con la necesidad de la gente”, le dijo a Infobae el fiscal Horacio Azzolin, titular de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) de la Procuración General de la Nación. Y dio una fórmula para estar prevenidos: “Muy atentos a lo que parece tentador y urgente, porque lo que buscan es que no pienses y hagas click”.

Correos electrónicos falsos de bancos o páginas web con ofertas especiales, aplicaciones en celulares, cadenas de Whatsapp con información de origen dudoso. Todo es propicio para una estafa y ahora llega por el coronavirus, un tema que genera atención y preocupación en todo el mundo.

“Hasta el momento no recibimos denuncias en la Fiscalía. Pero estamos alertas porque el coronavirus va a ser la excusa para cambiar los fraudes habituales. Todavía no tenemos denuncias porque primero suelen ocurrir en Europa y después llegan acá”, explicó Azzolin.

La referencia es que se descubrió una aplicación falsa en los Playstore de los celulares con el sistema Android que se llamaba “Coronavirusapp”. Con la excusa de aportar información y consejos sobre el virus, la aplicación tenía un ransomware, que es un sistema por el que se bloquean datos. En este caso el bloqueo era sobre todo el teléfono y los estafadores le pedían al dueño dinero a cambio de liberarlo.

El phishing es la estafa por internet más conocida. Es el robo de datos –personales, bancarios y de claves– que se hace mediante correos electrónicos, páginas web o redes sociales. “Hay que ignorar todo mensaje que no llegue por los carriles habituales. Nada de cadenas de Whatsapp o mensajes de texto. Sobre todo cuando las ofertas son tentadoras y urgentes, porque lo que buscan es que no pienses y hagas click”, explica

Azzolin. Así, dice que hay que tener cuidado con las ofertas o promociones de productos como alcohol en gel o lavandina, muy buscados estos días. “No descartamos fraudes en compras por Internet de artículos de primera necesidad”, sostuvo.

Las organizaciones criminales usan como pantalla a las grandes empresas. “Hoy hay que tener especial atención con los mails que llegan de los bancos”, advierte el fiscal. Con las medidas de restricción que impuso el gobierno nacional, las entidades bancarias alentaron el uso del home banking para hacer operaciones y en los últimos días utilizaron el correo electrónico para enviar información. “Una estafa común es que te dicen que tu cuenta se bloqueó y te piden que vuelvas a poner tus datos. No lo hagas, porque los bancos no piden eso por mail, y si tenés dudas comunicate al 0800 del banco. Y si los datos te los piden por teléfono, vos solicitale a esa persona su nombre, su legajo, un número de referencia del trámite y llamá al 0800 del banco”, recomendó el fiscal.

Azzolin advierte que en el contexto de cuarentena y las recomendaciones de quedarse en casa pueden surgir estafas en, por ejemplo, cupones de descuentos. “Pueden aparecer en páginas web ofertas para deliverys de comida y para eso te piden tus datos, como la tarjeta de crédito. Así te los roban”, señaló.

Por esas mismas restricciones de circulación muchas empresas y organismos de gobierno aplicaron el "home office", que es el trabajo desde casa. Y en este punto Azzolin hace particularmente hincapié porque se acrecentó esta semana. "Somos muchos trabajando desde casa y conectados a Internet y eso puede ser riesgoso para la seguridad", planteó. Y da algunos consejos. El primero es que el router para la conexión a Internet tenga una contraseña segura y que no sea la que da el instalador. "Suelen usar la misma contraseña para instalar y pasa que en una misma zona, que es en la que trabaja esa persona, mucha gente tenga la misma", explicó. También que las computadoras tengan un antivirus.

En el trabajo desde casa se utiliza información sensible sobre el trabajo de cada persona. "Para eso hay que cifrar el tráfico de esa información y lo recomendable es tener una VPN", dice. VPN es la sigla de "Virtual Private Network", que son redes que aseguran la información que se transmite.

Azzolin también recomienda que las personas pidan en sus trabajos que las computadoras que se van a usar en home office tengan todas esas herramientas. "Es que las PC hogareñas suelen tener menos medidas de seguridad que las de los trabajos", sostiene.

Otro aspecto del trabajo fuera de la empresa –tal vez con menos uso estos días por las restricciones y el distanciamiento social– es usar la computadora en los bares. "Allí te ofrecen un acceso a Internet por red

wifi abierta o cuya contraseña la tienen muchas personas. De esa forma alguien puede monitorear lo que estás haciendo en tu computadora. Lo mismo ocurre con el wifi de los aeropuertos. Las VPN también sirven para evitar esos ingresos”, explica.

¿Qué hacer ante una estafa virtual? “La denuncia siempre, pero hoy la recomendación es no salir de casa. Lo importante es que no hay plazo para denunciar, por lo que no es algo urgente. Y además los tribunales hoy atienden los casos prioritarios y estas denuncias no se van a tratar ahora”, explica. Pero por consultas o dudas se puede contactar a la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) por mail a denunciasufeci@mpf.gov.ar o por su página web www.mpf.gob.ar/ufeci.

“Formamos parte de grupos de trabajo con fiscales de Sudamérica y el Caribe, y ayer se hizo una consulta y por el momento no se registran casos. Pero sí hubo en Europa. Empiezan allá y a la región llegan primero a Brasil y Colombia y después a Argentina. Tenemos todos los sensores alertas y estamos atentos”, cierra Azzolin.

Fuente: Infobae