Universidad Viña del Mar

A un click del fraude: ¿Cómo operan los delitos financieros y qué hacer para evitar ser víctima de ellos?

Desinformación y pesimismo son factores que los expertos reconocen como claves a la hora de analizar el aumento de este tipo de hurtos.

En pandemia han aumentado los delitos informáticos y para los expertos esto se debe al estado de pesimismo y desinformación que existe en las personas, así lo detalla el académico de la carrera de Ingeniería Civil Informática de la Universidad Viña del Mar (UVM), **Pablo Ormeño**, quien señala que “al necesitar información sobre el avance del Covid, estadísticas relacionadas o por la necesidad de recibir ayuda de entidades públicas o privadas, **la gente está más propensa a abrir correos** con temas relacionados o hacer click en enlaces en redes sociales que tengan que ver con temas afines, la mayoría de los cuales se crean con

la intención de hacer phishing.

Pero, **¿Qué es el phishing?** Según relata el docente UVM, “es un tipo de delito que permite engañar a las personas para que comparta información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la ´pesca´ existen más de una forma de atrapar a la víctima y existe muchas tácticas que permiten estafar a la gente”.

Ormeño explica el funcionamiento de este tipo de fraude indicando que “por lo general, el modus operandi es el mismo en todos los casos, es decir **las víctimas reciben un mensaje de correo electrónico o un mensaje que imita o ´suplanta la identidad´** de una organización de confianza como un banco o una entidad de gobierno. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un texto cuya intención es asustarla y de esta forma debilitar su buen juicio e infundir miedo. Dicho mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá alguna consecuencia”.

Para evitar ser víctima de un fraude, el experto enfatiza que **“la primera forma de defensa es el criterio**. Es necesario aprender a reconocer los signos del phishing, por lo que se recomienda practicar informática segura cada vez que se vea

un correo electrónico, se lea un post de Facebook o juega su juego favorito".

Además, agrega **"evite abrir correos de remitentes que no parezcan familiares,** no haga click en enlaces que estén dentro de un correo electrónico, salvo que sepa exactamente donde lo lleva. Haga una búsqueda manual de la fuente hacia donde lo dirige el correo para comprobar veracidad y asegúrese que la página que le solicita información confidencial sea del tipo HTTPS".

En caso de ser víctima de algún tipo de delito, el ingeniero civil informático recomienda que "es importante asesorarse inmediatamente con un abogado especializado. También se recomienda no borrar ni hacer modificación alguna de cualquier información que posea el dispositivo que ha sido comprometido, ya que la integridad es de vital importancia en un proceso judicial".

Finalmente, añade que **"no informar por redes sociales, ni reenviar la información por correo, chat o mensaje de texto.** Puede realizar capturas de pantalla para mostrar a los peritos informáticos sin que haya alteración de pruebas. De esta forma el experto puede informarle los pasos a seguir. En caso de hacer una denuncia se debe acudir a la Policía de Investigaciones o a la Fiscalía", acotó.

LINK