Es habitual que las organizaciones criminales traten de suplantar la identidad de la víctima con el robo de las cuentas bancarias. *Foto: José Mari Martínez*

La ciberdelincuencia aumentará el año que viene más de un 30% en Euskadi

El 90% de los ataques por medios digitales son intentos de estafa, de los que este año hay registradas 17.061 denuncias

✎ ***Ane Araluzea***

DONOSTIA – Es probable que el término *phishing* no le suene de nada, pero casi seguro que habrá recibido correos electrónicos que esconden enlaces maliciosos con el objeto de robar datos de su cuenta bancaria. La delincuencia que se comete a través de los medios digitales está creciendo. De eso no hay duda. Del año pasado a éste, la ciberdelincuencia ha aumentado un 34,8% en Euskadi. "Y hemos hecho una proyección de 2023 a 2024 y se mantiene la misma tendencia", asegura Javier Diéguez, director general de Cyberzaintza, Agencia Vasca de Ciberseguridad, un servicio que se ha creado hace unos meses dentro del Departamento de Seguridad para combatir la ciberdelincuencia de una manera integral y transversal.

El incremento de la actividad digital ha conllevado una exposición mayor a caer en fraudes. "Y es más probable que alguien pueda ser agredido por medios electrónicos por su edad, género o ideología", apunta Diéguez. Sin embargo, el 90% de los ataques que se perpetran por medios digitales son intentos de estafa. "La motivación es económica y puede ser hacia empresas o instituciones públicas, para algún pago de facturas o algo similar, pero también hacia personas, para cualquier tipo de compra fraudulenta que se haya llevado a cabo", expone el responsable de Cyberzaintza, quien revela que a menudo reciben llamadas de personas que no son capaces de determinar qué tipo de ataques están recibiendo.

ESTAFAS MÁS HABITUALES Se trata de usuarios que pueden llegar a una página buscando un producto o un servicio que finalmente no existe, "principalmente a través de webs que pueden ser de electrónica, viajes, juguetes...". Pero también son comunes las estafas en las que solicitan dinero. Javier Diéguez menciona una reciente campaña de timos en Booking, donde una organización estaba suplantado a los hoteles adheridos a la plataforma. "Escribían en nombre de Booking, con lo cual parecía una petición legítima. Son ataques con un cierto nivel de sofisticación, juegan mucho con la emoción de la persona que recibe la comunicación", afirma el ingeniero informático sobre estas ofensivas que se deben contrastar, rápidamente, con el servicio de atención al cliente de la plataforma en cuestión.

> **"El robo de una credencial bancaria pasa por que tú hayas introducido información en algún lugar"**
>
> **"Muchas veces las estafas no se denuncian porque a lo mejor son cuantías pequeñas"**
>
> **JAVIER DIÉGUEZ**
> Director general de Cyberzaintza

Otra estafa habitual es la suplantación de la identidad para la usurpación de las cuentas bancarias. "El robo de una credencial bancaria pasa por que tú hayas introducido información en algún lugar", advierte Diéguez al respecto. Por ello, explica que es indispensable que cuando se esté actuando en un servicio "sensible" para la actividad personal se active el llamado "factor de autenticación múltiple". Se trata de que la compra en cuestión no solo se valide a través de una contraseña, sino que los sistemas de banca *online* envíen una comprobación "a un dispositivo de tu propiedad, ya sea un teléfono móvil o una cuenta de correo electrónico" para poder verificar que quien realiza la adquisición es el titular de la cuenta.

En ese sentido, Javier Diéguez admite que la suplantación de la identidad es más fácil si el usuario comparte información de aspectos de su vida personal a través de las redes sociales. Y pone como ejemplo lo siguiente: si publicas el nombre de tu mascota en alguna red, no utilices como pregunta de recuperación de contraseña en ningún sitio cuál es el nombre de tu mascota. También menciona el caso de personas que, por una necesidad puntual, comparten a través de medios electrónicos copias escanea-