CIBERDELITO, FRAUDE Y CIUDADANÍA. PERSPECTIVA DE POLICÍA NACIONAL

IV Congreso de Educación Financiera Edufinet "Educación financiera para una época de cambio de paradigmas"
Málaga, 17-19 noviembre 2021

Working Paper 22/2022

Andrés Román Izquierdo

Inspector Jefe de la Policía Nacional y Jefe de la Sección de Ciberdelincuencia de la Comisaría Provincial de Málaga

Resumen

El mundo digital no es una promesa de futuro, es una realidad presente y la pandemia ha agilizado un proceso que era natural. Se ha evitado el contacto físico y el resultado ha sido la aceleración de esos procesos digitales que impregnan tanto nuestra vida económica, comercial e incluso personal.

En este contexto, el auge de los ciberdelitos se ha hecho patente en una sociedad que cada vez está más digitalizada. Es conveniente conocer, al menos en sus aspectos básicos, los distintos tipos de ciberdelitos y fraudes que se suelen dar en la operativa online para estar protegidos.

Palabras clave: ciberdelitos; toma de decisiones financiera; educación financiera.

1. Introducción

El mundo digital no es una promesa de futuro, es una realidad presente y la pandemia ha agilizado un proceso que era natural. Se ha evitado el contacto físico y el resultado ha sido la aceleración de esos procesos digitales que impregnan tanto nuestra vida económica, comercial e incluso personal.

Las personas se relacionan por Internet desde hace mucho tiempo, también compran e incluso teletrabajan. En un mundo digital en el que todo está presente, desde el punto de vista de la ciberdelincuencia, muchas veces es difícil seguir el rastro del delito una vez que se ha producido, por lo tanto la mejor protección es la prevención.

Es decir, en la medida en que la gente conozca esta casuística que nos puede afectar a todos, haremos prevención y habrá mejor protección.

En el mundo digital hay un cóctel que está formado por tres elementos: en primer lugar, están las dos brechas digitales que tienen dos facetas, por un lado está la brecha intergeneracional y por otro lado está la brecha del delincuente respecto a la potencial víctima. Estas brechas nos hacen vulnerables dada la diferencia de conocimientos y competencias entre la población mayor y joven (brecha intergeneracional) y entre el delincuente y la víctima.

El segundo ingrediente del cóctel son las ventajas que proporcionan las TICs y sus aplicaciones al delincuente. Antiguamente cuando alguien quería obtener dinero de manera ilícita atracaba, robaba, etc. pero dirigía su acción sobre una víctima. Hoy día, sin embargo, existe la posibilidad de ataques masivos y la cantidad de afectados dependerá de la información de que disponga el ciberatacante. Otra ventaja que proporcionan las TICs es la facilidad de enmascaramiento. En Internet también es muy fácil falsificar, porque no estamos viendo una persona, estamos viendo una representación digital que es muy fácil alterar.

Otro elemento de las ventajas de las TICs para los ciberdelincuentes es la eficacia que les brindan. Por ejemplo, con el uso de medios de pago inmediatos y rápidos como las criptomonedas, Bizum, PayPal o las transferencias inmediatas es muy fácil para la víctima perder el control y eso es lo que busca el delincuente que es definitiva, disponer rápida e inmediatamente del producto del engaño.

En el caso de las criptomonedas, en el momento en el que se produce el desfalco del dinero, con un solo botón, el ciberdelincuente lo puede mover por múltiples países a través de carteras digitales. Esto no sucedía antiguamente, ya que las transferencias tardaban un día y había posibilidad de interceptación e incluso de retrocesión, cosa que no ocurre hoy día.

En definitiva, las TICs proporcionan múltiples ventajas a los ciberdelincuentes como:

- Ataques a gran número de víctimas.
- Facilidad de enmascaramiento/anonimización.
- Facilidad de engaño y falsificación.
- Menor exposición/riesgo para el delincuente.
- Mayor eficacia para obtener dinero/beneficios.

El último elemento de este cóctel es el factor humano. El eslabón más débil en ciberseguridad no son las máquinas, son los seres humanos, que son los objetivos de los delincuentes. En el momento que la víctima es engañada, no importan las medidas de seguridad que tenga. Por tanto, es importante que la gente sepa que el eslabón débil de la cadena son los seres humanos, no las máquinas.

Es muy fácil engañar por Internet y aquí juega un factor importante la psicología. Esta facilidad deriva de que el engañado no es la máquina, sino el humano que la está operando y es así porque se produce una serie de procesos psicológicos. A la hora de operar por Internet, el comportamiento de las personas cambia, la percepción de riesgo disminuye y es un mecanismo de proyección sobre el que muchas veces volcamos nuestras ansiedades, expectativas, necesidades, etc. y esto es lo que nos hace tremendamente vulnerables.

En resumen, esta vulnerabilidad que se deriva de las brechas digitales, de las ventajas que proporcionan las TICs y el factor humano, se combate con la prevención y la información de los ciudadanos, a través de la cultura digital y financiera. Se trata no tanto de saber lo que tenemos que hacer sino de saber lo que no tenemos que hacer, en definitiva de tener una cultura global de saber lo que es Internet, para qué nos sirve y cómo tenemos que comportarnos.

El ciberdelito patrimonial

A continuación, se va a hacer un recorrido por las distintas tipologías de delitos que cometen los ciberdelincuentes en dos grupos: uno primero, dirigidos a los ciudadanos individuales y otro segundo dirigidos a las empresas y organizaciones.

La ciberdelincuencia es como un virus; se va adaptando rápidamente y va mutando, ya que la tecnología va avanzando cada vez más.

La ciberdelincuencia está aumentando exponencialmente, y esto lo corrobora un estudio de la Secretaría de Estado de Ciberseguridad. Las estimaciones indican que a día de hoy la ciberdelincuencia está moviendo más dinero que el tráfico de drogas. Estas estimaciones demuestran que según pasa el tiempo la repercusión de este tipo de delitos y el nivel de amenaza es mayor.

La estrategia básica de protección es la autentificación de doble factor, que consiste en que para realizar cualquier operación bancaria se tienen que utilizar dos tipos de claves o contraseñas y una de ellas es algo que poseemos (la cara o la huella) y algo que sabemos (la contraseña o la firma digital).

A continuación pasamos a ver una serie de conductas delictivas de máxima actualidad:

- **El triplete Phishing-SMishing-Vishing**

La ingeniería social es el conjunto de técnicas y estrategias que utiliza el delincuente para conseguir las claves o contraseñas de la víctima o para conseguir que la víctima haga lo que el delincuente quiere que haga.

En el Phishing el vector de ataque es el correo electrónico. Y lo que se hace por medio del Phishing es, por ejemplo, la suplantación de identidad de las entidades bancarias por medio de un correo electrónico que recibe la víctima con un enlace.

En el SMishing el vector de ataque es el móvil y dicho ataque se lleva a cabo a través de la recepción de mensajes (SMSs) por parte de la víctima.

En tercer lugar está el Vishing, técnica en la que el delincuente utiliza la voz para llevar a cabo el engaño. Por tanto, en este caso se trata de un teleoperador que llama a la víctima y que le aporta credibilidad, confianza y que supuestamente va a ayudar a la víctima en un problema que haya podido tener y esto le da un mayor control sobre la víctima.

Por consiguiente, tanto en el Phishing como en el SMishing siempre se busca el mismo objetivo que es que la víctima pulse un enlace. Este enlace lo que hace es bien redirigir a la víctima a una página web falsa o bien instala en el equipo de la víctima un malware, que es un programa informático malicioso que, por ejemplo, puede obtener las contraseñas, o puede encender la cámara del dispositivo.

- **Spoofing**

El Spoofing es una técnica que consiste en el maquillaje, de tal manera que cuando la víctima recibe un correo electrónico, un SMS o una llamada, aparece proveniente de la entidad o institución de la que al ciberdelincuente le interesa que aparezca para cometer su engaño.

Estas técnicas se pueden combinar para dar mayor credibilidad al engaño que el delincuente quiere perpretrar. Por ejemplo, la víctima puede recibir un SMishing con maquillaje o Phishing con maquillaje.

- **"Mulas" en los ciberdelitos**

Los delincuentes redutan "mulas" para mover el dinero que generan con sus delitos. Esto lo consiguen a través de falsas ofertas de trabajo.

La dave de la prevención para ser víctima de este tipo de delitos es invertir la iniciativa, es decir, cuando tengamos conocimiento sea por la vía que sea (SMS, correo electrónico, etc.) lo recomendable es no seguir las instrucciones porque eso supone entrar en la trampa que el delincuente está preparando. Lo recomendable, por ejemplo, es que nosotros mismos llamemos a nuestro banco para comprobar si lo comunicado es cierto

- **Estafa del bizum "el pagomocho"**

Esta estafa consiste en que el delincuente se interesa por adquirir un artículo de segunda mano que la víctima tiene publicado en algún portal o app de venta de artículos de segunda mano. Ambas partes llegan a un acuerdo de utilizar bizum como medio para el pago, pero lo que ocurre es que el delincuente, a través de esta aplicación, en lugar de pagar, lo que hace es enviar a la víctima un requerimiento de pago por el importe convenido de la compra-venta. Si la víctima no se da cuenta y acepta se consuma el engaño.

- **Broker SCAM chiringuitos basados en criptomonedas**

Este caso consiste en la inversión en criptomonedas a través de "chiringuitos financieros" en los que se promete al inversor altos retornos que se van generando. Cuando el inversor o la víctima intenta retirar sus fondos es cuando comienzan a ocurrir los problemas, en forma del pago de altas tasas o comisiones para finalmente no poder reembolsar el importe invertido.

- **Código QR**

Hay que ser consciente de que escanear un código QR equivale a pinchar en un enlace y, por tanto, si el QR es malicioso puede suponer que realmente estemos descargando un malware.

- **Estafa al CEO (Man in the middle-BEC "Business email compromise")**

A esta estafa se le llama "hombre en el medio". El atacante infecta a uno de los dos extremos (empresa-proveedor) y esta infección se puede producir simplemente porque un empleado puede haber abierto un correo electrónico o pinchado en un enlace enviado por el delincuente. Una vez que se produce esto, se instala un malware que espía y monitoriza el flujo de correo a la espera de que haya un pago pendiente.

El delincuente actúa cuando hay un pago pendiente camuflándose con la táctica del maquillaje. Una vez camuflado con la identidad de una persona conocida para la víctima, el delincuente solicitará el pago pendiente a lo que la víctima accederá creyendo estar pagando a un proveedor que conoce.

Esto se puede prevenir con una doble verificación por parte de la víctima potencial. Cuando se le solicite el pago, la víctima potencial puede llamar al contacto que se le solicita para verificar que es así.

- **Randsomware**

Esto consiste en que un empleado recibe un correo que contiene un documento y, al abrirlo, se le encripta el ordenador.