

08/04/26

La Guardia Civil evita una estafa de 2,2 millones de euros gracias a una denuncia telemática

Resumen

La Guardia Civil ha bloqueado seis transferencias fraudulentas destinadas al extranjero, gracias a una denuncia telemática y a la rápida actuación de la Cibercomandancia

Los estafadores emplearon el método del “smishing”, por el cual suplantarón la identidad de una entidad para acceder a datos bancarios de una empresa madrileña

Contenido

La Guardia Civil ha logrado obtener el bloqueo preventivo de seis transacciones no reconocidas desde dos cuentas bancarias de una empresa madrileña por valor de más 2.200.000 euros, que estaban destinadas a seis cuentas bancarias en el extranjero.

La investigación se inició inmediatamente después de que el responsable de la empresa perjudicada interpusiera una denuncia telemática a través de la sede electrónica de la Guardia Civil. La denuncia se produjo después de que la directora financiera de la empresa recibiera un SMS que suplantaba a su entidad bancaria, donde falsamente le informaban de un cargo en una de las cuentas de la empresa por valor de 4.900 euros proveniente de una empresa de Hong Kong. En el mensaje se le instaba a realizar actuaciones urgentes e inminentes para anular el cargo si no lo reconocía, facilitándole un enlace para ello.

Al pinchar sobre el enlace proporcionado, le redirigió a una página web que reproducía la apariencia de la banca online de su entidad financiera donde facilitó la clave de acceso y la clave de firma de operaciones. Esta actuación de introducir claves una vez clikeado el enlace enviado por SMS constituyó el eje central del engaño. Tras confiar en la autenticidad del SMS, introdujo sus claves personales en una página destinada a obtener fraudulentamente sus credenciales.

Momentos después, y sin que el perjudicado pudiese percatarse hasta el día siguiente, se ordenaron seis transferencias por importes entre los 250.000 y los 500.000 euros desde varias sucursales a cuentas bancarias situadas en terceros países de la Unión Europea.

La rápida actuación policial de la Cibercomandancia de la Guardia Civil, bajo el marco de la operación “Cibermot” desarrollada por su Equipo @, permitió identificar con detalle el modus operandi del fraude y rastrear la trazabilidad de la operativa empleada. Pretendían mover los fondos a un entramado de cuentas en diversos países del extranjero para dificultar su rastro y recuperación. Por el rápido y minucioso análisis, así como por la inmediata actuación de los guardias civiles, se lograron paralizar hasta seis transferencias por valor total de más de 2.200.000 euros, siendo bloqueadas y quedando a disposición de la empresa denunciante.

Técnica empleada

Este tipo de fraude, denominado smishing, consiste en el envío de mensajes de texto o de mensajería instantánea que simulan proceder de entidades bancarias apelando a una urgencia o amenaza que necesita una reacción inmediata para evitar un cargo sospechoso. Los mensajes suelen incluir números de teléfono o enlaces fraudulentos donde, como en este caso, imitan de forma muy elaborada la apariencia de las páginas web de los servicios oficiales de la entidad financiera del perjudicado.

Cuando la víctima accede a esos enlaces o contacta con los números facilitados, puede llegar a introducir datos bancarios, entregar contraseñas o incluso descargar malware en su dispositivo, quedando así fácilmente expuesta a la sustracción de fondos.

Claves determinantes para el éxito de la investigación

La empresa perjudicada, nada más percatarse de los movimientos no reconocidos, presentó una denuncia telemática en la sede electrónica de la Guardia Civil narrando los hechos sucedidos y adjuntando copia de los extractos bancarios.

La Cibercomandancia de la Guardia Civil, responsable de la gestión de la denuncia telemática, inmediatamente que recibió la denuncia inició la investigación, primero comprobando e identificado el hecho delictivo y sus circunstancias, para

seguidamente requerir el bloqueo preventivo de los seis movimientos fraudulentos desde dos sucursales de una misma entidad financiera.

La entidad bancaria de la empresa perjudicada, a petición de la Guardia Civil, bloqueó y paralizó toda operativa relacionada con los cargos indebidos denunciados a la vez que aportó los datos de trazabilidad disponibles, no llegando a transcurrir más de 24 horas entre que fueron ordenados hasta que fueron paralizados a instancias de la Guardia Civil, en virtud de la denuncia telemática y de la investigación realizada.

Por la Guardia Civil se continúa con la investigación para la identificación de los titulares de las cuentas extranjeras y la determinación de las posibles responsabilidades penales de los presuntos autores.

Para evitar estos fraudes, la Guardia Civil recomienda:

- Desconfiar de SMS de supuestas entidades bancarias y nunca hacer click sobre los enlaces que pudieran incluir.
- Desconfiar de cualquier solicitud por mensaje o llamada telefónica que requieran actuaciones urgentes o inmediatas.
- En caso de querer contactar con las entidades bancarias hacerlos a los de contacto teléfonos oficiales, nunca usar los que figuran en el mensaje recibido.
- Nunca facilitar por teléfono ni por mensaje de texto o de cualquier aplicación las claves de acceso a la banca online ni de tarjetas.
- Denunciar inmediatamente el hecho delictivo, bien a través de la sede electrónica o bien en una dependencia de la Guardia Civil o de otras policías.

Creación de la Cibercomandancia de la Guardia Civil:

La Cibercomandancia amplía los servicios de atención a la ciudadanía de la Guardia Civil, en este caso a través de medios telemáticos, complementando y auxiliando en el "ciberespacio" las 24 horas del día los 365 días del año, al resto de unidades de seguridad ciudadana de la Guardia Civil.

En la sede electrónica de la Guardia Civil, <https://guardiacivil.sede.gob.es> mediante el uso de un certificado electrónico, se pueden denunciar de manera telemática los siguientes hechos delictivos:

- Estafas y cargos indebidos a través de medios informáticos.
- Sustracción de vehículos y/o sustracción en su interior.
- Hurtos y Daños.

También se puede comunicar la pérdida o extravío de documentación oficial y, en su caso, su recuperación.

Para más información contactar con la oficina de comunicación de la Cibercomandancia, en el teléfono 987 914 013 ext. 6542262 o en el móvil 627 672 729.