21/06/26

Esclarecida una estafa que introducía SMS falsos entre los mensajes de texto legítimos de un banco

Resumen

La víctima fue inducida a autorizar una transferencia de 5.000 euros bajo la falsa premisa de reforzar la seguridad de su cuenta

El equipo @ de la Cibercomandancia identificó a las dos presuntas autoras, residentes en la provincia de Madrid

La Guardia Civil recuerda la posibilidad de recurrir a la denuncia telemática para denunciar cargos fraudulentos y la necesidad de tomar medidas de precaución para evitar estafas

Contenido

La Guardia Civil ha esclarecido una sofisticada estafa cometida mediante la técnica del “smishing”, es decir, a través de SMS, a raíz de la denuncia presentada por una víctima a través de la Sede Electrónica. La investigación ha permitido identificar e investigar a dos mujeres residentes en Madrid como presuntas autoras de un delito de estafa.

La investigación se inició tras la denuncia presentada por una víctima en la Sede Electrónica de la Guardia Civil después de sufrir la sustracción de 5.000 euros de su cuenta bancaria. La víctima recibió varios mensajes SMS fraudulentos que se integraban en el mismo hilo de conversación que las notificaciones legítimas de su entidad financiera, lo que la llevó a confiar plenamente en la veracidad de los avisos.

El primero de estos mensajes alertaba sobre una supuesta transferencia inmediata no reconocida y facilitaba un número de teléfono al que la víctima debía llamar para solventar la supuesta incidencia de seguridad.

Técnicas de ingeniería social y suplantación de identidad

Para materializar el engaño, las presuntas autoras emplearon técnicas avanzadas de ingeniería social y suplantación de identidad con el fin de generar un clima de urgencia. Al contactar con el número facilitado, la víctima fue atendida por una persona que se identificaba como agente del departamento de seguridad de la entidad, quien reforzó la apariencia de veracidad mediante el envío de mensajes adicionales dentro del mismo hilo oficial.

Bajo el pretexto de activar un protocolo de protección para anular la transferencia fraudulenta, el falso agente convenció a la víctima para que introdujera códigos en su banca online. Lejos de constituir un mecanismo de cancelación, la operación ejecutada por la víctima permitió el traspaso de los fondos hacia cuentas controladas por las presuntas autoras, que cerraron el engaño remitiendo un último mensaje de confirmación de una cancelación supuestamente exitosa, ocultando así la sustracción real del dinero.

Tras tener conocimiento de los hechos, el Equipo @ de la CiberComandancia de la Guardia Civil inició de forma inmediata las diligencias de investigación, centradas en el análisis técnico de las comunicaciones mantenidas entre la víctima y las presuntas autoras.

Las labores se orientaron al rastreo pormenorizado de la trazabilidad del dinero defraudado, lo que permitió seguir el flujo de los fondos hasta su destino final. Gracias a estas actuaciones, el Equipo de Policía Judicial de Madrid investigó procesalmente a dos mujeres residentes en la provincia como presuntas responsables de los hechos. Una vez finalizadas las diligencias, el atestado instruido ha sido remitido a la Autoridad Judicial competente para la continuidad del procedimiento.

Consejos para prevenir fraudes

Para prevenir los posibles fraudes en la red, desde la Guardia Civil se recomienda:

- Desconfiar de los SMS que se reciban, evitando hacer click sobre los enlaces que pudieran incluir.
- Comprar artículos en webs seguras, desconfiando de tentadoras ofertas que se anuncien en páginas web desconocidas.
- No aceptar ofertas de trabajo inesperadas llegadas a través de redes sociales (Telegram, Whatsapp, Tik-tok, etc.).
- Desconfiar de solicitudes de cuantías económica efectuadas con cualquier pretexto a través de redes sociales.
- Solicitar a las entidades bancarias la activación de la autenticación reforzada en todos los pagos.

- Bloquear las tarjetas bancarias o medios de pago que se utilicen ante la mera sospecha de una posible utilización de los mismos por parte de terceras personas.
- Denunciar inmediatamente el hecho delictivo, bien a través de la sede electrónica o bien en una Unidad de la Guardia Civil.
- Reclamar la devolución de los cargos indebido a su entidad bancaria.
- Recopilar toda la información posible del cargo efectuado, como es cuenta de destino, comercio o entidad que lo realiza, número de teléfono en los envíos a través de Bizum, etc.

Creación de la Cibercomandancia de la Guardia Civil:

La Cibercomandancia es una unidad de reciente creación a través de la cual la Guardia Civil amplía los servicios de atención al ciudadano, 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, 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.
- Pérdida o localización de documentación

Para más información contactar con la O.P.C. de la CiberComandancia, en el teléfono 674907869.

Enlace descarga imágenes