TIPO DE FRAUDE. PHISING

CAJA RURAL

¿QUÉ ES?

El phishing es un fraude por el que los ciberdelincuentes envían correos electrónicos haciéndose pasar por organismos o empresas legítimas, como por ejemplo tu entidad financiera, con el fin de obtener tus datos personales como nombre o DNI y los datos bancarios (números de tu tarjeta, usuario y contraseña de tu banca digital, claves SMS).

¿CÓMO LO HACEN?

Estos mensajes solicitan que se realice alguna acción de forma URGENTE, normalmente que se faciliten datos, para evitar alguna consecuencia negativa.

Los argumentos que suelen utilizar para engañar son:

- **Tu cuenta ha sido bloqueada** o va serlo de forma inminente.
- Necesitamos que **confirmes tu identidad.**
- **Estamos haciendo mejoras en las medidas de seguridad** de la entidad.
- **Has ganado algún premio** o te han concedido alguna ayuda pública, que no has solicitado.
- **Te ofrecemos obtener descuentos** o participaciones en promociones y sorteos.
- Te ha llegado un **paquete en Correos** que debes recoger.
- Ha entrado en vigor una nueva normativa y **necesitamos que confirmes unos datos para que puedas operar.**

¿QUÉ PODEMOS HACER PARA EVITARLO?

Fíjate muy bien en el contenido del correo electrónico y ten en cuenta que:

- **Nunca te vamos a pedir** por correo electrónico, teléfono, ni por SMS **que facilites tus claves de acceso** a Ruralvía o los datos de tus tarjetas de Caja Rural.
- **Si el correo tiene archivos adjuntos, desconfía** y nunca los abras, seguramente este archivo oculta un virus informático.
- **Comprueba la dirección del remitente,** normalmente los ciberdelincuentes consiguen ocultar la dirección real detrás de una falsa. Comprueba que la dirección de la web lleva un dibujo de un candado, símbolo de página segura.
- **Desconfía de los correos que contienen enlaces y revísalos antes de pinchar sobre ellos.** Puedes pasar el cursor del ordenador sobre el enlace para ver la dirección verdadera. Lo que quieren es dirigirte a una página falsa que parece ser nuestra web verdadera para robar tus contraseñas de acceso.

¿QUÉ HAGO SI TENGO SOSPECHAS DE QUE ESTÁN INTENTANDO COMETER FRAUDE EN MIS CUENTAS O TARJETAS?

No facilites nunca la información que se te piden.

- **No pinches en los enlaces, ni descargues los archivos** adjuntos.
- **Márcalo como «no deseado» en tu gestor de correo, así siempre irán a la bandeja de "Spam"** o bloquea al remitente para evitar recibir correos de este tipo en el futuro.
- **Modifica la contraseña** de acceso a Ruralvía.
- **No olvides interponer denuncia** ante la Policía, Guardia Civil o en el Juzgado.

TIPO DE FRAUDE. VHISING

CAJA RURAL

¿QUÉ ES?

El vishing es un fraude que tiene como objetivo obtener tus datos personales y bancarios a través de una llamada telefónica, engañándote mediante la suplantación de la identidad de una entidad o persona sobre la que tienes habitualmente confianza.

¿CÓMO LO HACEN?

Como en el caso de Phising, **la persona que te llama va a intentar convencerte con diferentes argumentos de que necesita tus datos bancarios con urgencia**. ¡Ten mucho cuidado!

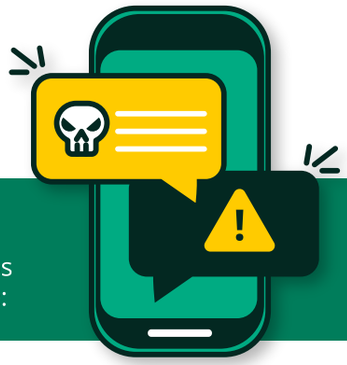
Aquí tienes algunos ejemplos de las personas por las se hacen pasar, para evitarlo:

TÉCNICO INFORMÁTICO: bajo el pretexto de limpiar tu ordenador de virus, te exigen el pago de una pequeña cantidad a través de una plataforma que registra tus datos bancarios y seguidamente solicitan hacerse con el control del dispositivo infectado para acceder a tu banca electrónica y realizar operaciones en tu nombre.

EMPLEADO DE UNA ENTIDAD BANCARIA: te avisan de que se está realizando una operación fraudulenta (y ficticia) con tu tarjeta y solicitan datos de la tarjeta. Mientras hablan contigo, realizan compras en línea reales y te piden las claves OTP recibidas por SMS en tu móvil haciéndote creer que son códigos para cancelar la operación falsa.

PERSONAS INTERESADAS en productos que has anunciado en webs de venta de productos de segunda mano, en este caso justificando una mayor rapidez en los pagos, te solicitarán los dígitos de tu tarjeta bancaria.

COMERCIAL DE UNA COMPAÑÍA TELEFÓNICA: te comunica que te han cobrado de más por error en la factura y solicita tus datos bancarios para abonar la diferencia.



¿QUÉ PODEMOS HACER PARA EVITARLO?

Utiliza el sentido común. ¿A qué nunca le darías la dirección de tu casa o de tus datos bancarios o personales a un desconocido? Estas personas son desconocidos así que:

No facilites a nadie los datos de tu cuenta o tarjeta por teléfono.

No des información sobre ti ni respondas a peticiones de información personal en situaciones que tú no hayas solicitado o iniciado.

Las compañías auténticas ya disponen de toda tu información personal; no necesitan pedírtela de nuevo y mucho menos por teléfono.

Familiarízate con los datos que sí solemos requerirte como, por ejemplo, una determinada posición o posiciones de tu contraseña. Pero recuerda que nunca te la pedimos completa, así que no la facilites.

¿QUÉ HAGO SI TENGO SOSPECHAS DE QUE ESTÁN INTENTANDO COMETER FRAUDE EN MIS CUENTAS O TARJETAS?

Si la llamada te parece sospechosa, no lo dudes, cuelga el teléfono y llámanos a nuestro teléfono gratuito de atención al cliente (900 822 670), contrastaremos lo sucedido y podrás quedarte más tranquilo.

Registra el número de teléfono que te ha llamado, apúntalo o guárdalo en tu agenda, para reconocerlo por si te vuelven a llamar de nuevo.

Bloquea en tu móvil ese número de teléfono que se ha puesto en contacto contigo y así evitarás llamadas no deseadas.

Denuncia los hechos ante la Policía, la Guardia Civil o los tribunales.