PREVENCIÓN DE ESTAFAS TELEMÁTICAS

MODUS OPERANDI

- Los autores de este tipo de estafas poseen información de la víctima, obtenida previamente mediante técnicas de ingeniería social (redes sociales, encuestas telefónicas, etc.).
- El modus operandi se lleva a cabo a través de una llamada telefónica o correo electrónico en los que los delincuentes se hacen pasar por técnicos de conocidas empresas tecnológicas.
- Comunican a la víctima que su ordenador ha podido ser hackeado o infectado por un malware.
- Indican que de forma "*online*", pueden proceder a solucionar el problema, realizando además un mantenimiento del dispositivo y una actualización del antivirus.
- Acceden al ordenador, pidiendo a la víctima la contraseña del mismo o mediante un programa de control remoto descargado por la víctima a petición del "falso técnico".
- Por el servicio prestado, el autor solicita el pago de una cantidad no muy elevada de dinero mediante tarjeta bancaria o transferencia o a través de la cumplimentación de una ficha con los datos bancarios de la víctima, con el consiguiente perjuicio económico que le pueda suponer.

¿QUÉ HACER?

- **No debe dar credibilidad a comunicaciones que ofrecen servicios que no ha solicitado.** En todo caso, no facilite datos personales, bancarios ni realice ningún pago si no ha solicitado previamente los servicios que supuestamente le ofrecen.
- **Anote el número de teléfono, email o link** utilizado por los delincuentes para facilitarlo a la Policía cuando **interponga la denuncia**.
- **En caso de haber seguido sus indicaciones y tener sospechas de haber sido víctima de una posible estafa:**
  - Desconecte el equipo de la red, para cortar el acceso remoto y que no puedan seguir manipulando el equipo.
  - Desinstale cualquier programa que hayamos instalado por indicación de estas personas.
  - Analice de forma completa con un antivirus el equipo afectado.
  - Cambie las contraseñas que estén almacenadas en el equipo o dispositivo.

En todo caso, DENUNCIE

☎ 091