## TÍTULO

**GUÍA DE CIBERATAQUES DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD**

## RESUMEN

El **Instituto Nacional de Ciberseguridad** ha publicado una **Guía** que alerta sobre las distintas técnicas que se ponen en práctica para acosar a los usuarios con **ataques informáticos**, y pretende servir como una herramienta para prevenir y evitar los perjuicios derivados de esas prácticas ilícitas.

## CONTENIDO

La **GUÍA DE CIBERATAQUES del Instituto Nacional de Ciberseguridad** describe los distintos métodos utilizados por los ciberdelincuentes para acceder ilícitamente a datos de los usuarios con fines defraudatorios. Así, se refiere a **técnicas para averiguar la contraseña** de acceso a dispositivos, o al ingente número de tipo de **ataques denominados "por ingeniería social"**, como son el *Phishing,* el *Vishing*, el *Smishing*, el *Baiting*, el *Shoulder Surfing*, el *Dumpster Diving*, el envío de *Spam*, y otro tipo de fraudes online.

La Guía hace referencia también a los **ataques a las conexiones**, que se basan en interponerse en el intercambio de información entre un usuario y un servicio web, para monitorizar y robar datos personales, bancarios, contraseñas, etc., entre los que se encuentra la creación de redes wifi falsas, el *Spoofing* en sus distintas modalidades (IP, web, email, DNS), el ataque a Cookies, la Inyección SQL, el escaneo de puertos, y ataques por malware, que engloba la propagación de virus, de troyanos, gusanos, apps maliciosas y otros.

Finalmente, la Guía propone el siguiente **Decálogo de Buenas Prácticas en ciberseguridad** para mejorar la protección de los dispositivos y la seguridad de la información de los usuarios:

## CONTENIDO

- **Utilizar un antivirus** para analizar todas las descargas y archivos sospechosos, y mantenerlo **siempre actualizado y activo**.
- **Mantener el sistema operativo, navegador y aplicaciones siempre actualizados** a su última versión para evitar vulnerabilidades.
- **Utilizar contraseñas robustas y diferentes** para proteger todas las cuentas. Si es posible, utiliza la **verificación en dos pasos u otro factor de autenticación**.
- **Desconfiar de los adjuntos sospechosos, enlaces o promociones demasiado atractivas**. La mayoría de los fraudes se basan en ataques de ingeniería social que pueden ser detectados aplicando el sentido común.
- Tener cuidado por dónde se navega. **Utilizar solo webs seguras con https y certificado digital** y utilizar el modo incógnito cuando no se quiera dejar rastro.
- **Descargar solo de sitios oficiales aplicaciones o software legítimo** para evitar acabar infectado por malware. En el caso de las aplicaciones, recordar dar solo los permisos imprescindibles para su funcionamiento.
- **Evitar conectarse a redes wifi públicas o a conexiones inalámbricas desconocidas**. Especialmente cuando se vaya a intercambiar información sensible, como los datos bancarios. Y, en caso de que haya que conectarse por una emergencia, tratar de utilizar una VPN.
- **No compartir información privada con cualquier desconocido** y no publicarla o guardarla en páginas o servicios webs no fiables.
- **Hacer copias de seguridad** para minimizar el impacto de un posible ciberataque.

En Madrid, a 30 de noviembre de 2020