

# Estado Mayor General de la Armada

## Coordinadora General del Ciberespacio



### Dossier de Ciberseguridad: CGC-DOSS-37-2024

**Objetivo:** Crear conciencia sobre las vulnerabilidades, amenazas o ventajas existentes del ciberespacio, mediante la difusión de noticias nacionales e internacionales de ciberseguridad.

#### 1.- ¿Cómo evitar virus en tú teléfono sin ser experto en ciberseguridad?

Cada día es más sencillo descargar aplicaciones y tenemos un mayor volumen de páginas web, lo cual también es sinónimo de peligro para nuestros teléfonos, ya que se incrementan las posibilidades de que estos acaben con un software indeseado. No obstante, al igual que se crean nuevos virus, también se idean innovadoras soluciones que pueden evitarnos más de un dolor de cabeza. La primera medida que debes tomar es descargar un antivirus, lo cual será útil para evitar la entrada de virus y hackeos, Otro modo de evitar virus es mantener el móvil actualizado, ya que los sistemas operativos estudian las amenazas más recientes para proteger los dispositivos. [\[cybersecuritynews\]](#)

**CATEGORÍA: INFORMATIVO NACIONAL**

#### 2.- Cómo utilizan falsas redes Wi-Fi en vuelos para robar información.

Uno de los “problemas” más grandes cuando iniciamos un viaje en avión es la desconexión a la que podemos estar expuestos durante el vuelo. Gracias a que algunas aerolíneas cuentan con el servicio a Internet, son muchos los pasajeros que se valen de la red Wi-Fi disponible para estar conectados estando entre las nubes. Pero esta práctica que pareciera ser inofensiva, también puede representar un riesgo para conectarse a una red WiFi gratuita, no debería ser necesario introducir ningún dato personal, como iniciar sesión a través de un correo electrónico o una cuenta de redes sociales, cualquiera que intente conectarse a redes Wi-Fi gratuitas en aeropuertos o vuelos nacionales, cambiar la contraseña después de hacer uso de ellas y reportar al aeropuerto cualquier actividad sospechosa. [\[welivesecurity\]](#)

**CATEGORÍA: INFORMATIVO NACIONAL**

#### 3.- Falso SMS de AEMET: cómo funciona este engaño por phishing y cómo evitarlo.

Esta es una estafa en la que los atacantes te envían un SMS haciéndose pasar por AEMET (Agencia Estatal de Meteorología en España). En él, te dicen que hay una tormenta que se acerca, y te invitan a descargarte una aplicación. En el mensaje también adjuntan una dirección en la que supuestamente podrás descargar la aplicación. Esta aplicación es un virus, un malware. Concretamente es un troyano, que es como se le llaman a las aplicaciones aparentemente inofensivas que tienen un virus en el interior. La app tendrás que descargarla e instalarla manualmente, y una vez lo hagas empezará a robar datos de tu móvil. [\[xataka\]](#)

**CATEGORÍA: INFORMATIVO INTERNACIONAL**

#### 4.- Alertan sobre el “trashing”, la amenaza que rebusca entre los documentos desechados para cometer ciberestafas.

“Trashing” o “dumpster diving” son los nombres en inglés que recibe la técnica por la que los cibercriminales obtienen información sensible de sus víctimas que recuperan del material que han descartado, como facturas, embalajes de paquetes o dispositivos electrónicos, como móviles u ordenadores. Estos documentos y dispositivos pueden contener información sensible, como el nombre completo de la víctima, su dirección, teléfono, documento de identidad, y número de cuenta bancaria, pero también credenciales de servicios digitales. Todo ello puede utilizarse posteriormente para hacer un ciberataque. [\[infobae\]](#)

**CATEGORÍA: INFORMATIVO INTERNACIONAL**

**Análisis:** Los ataques cibernéticos a nivel mundial continúan creciendo, y seguirán debido a la alta dependencia tecnológica de la sociedad, lo que hace que a día de hoy la probabilidad de sufrir ataques informáticos o ciberataques sea muy elevada, empleándose diversos métodos de ataque, por lo que se recomienda no tener acceso a páginas de dudosa reputación, a fin de prevenir y disminuir la superficie de ataque que pueden aprovechar los ciberdelincuentes.

