



## Tipos de ataques cibernéticos a usuarios

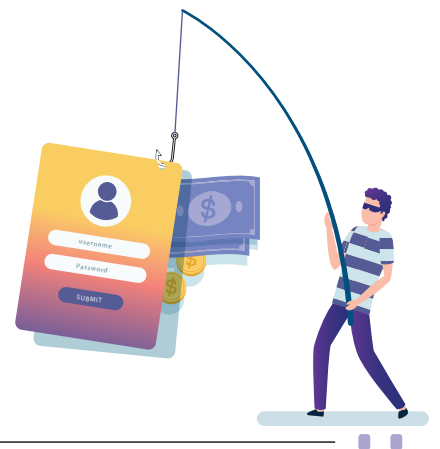
Se debe tener en cuenta que todos los ataques buscan robar información privada del usuario, como, por ejemplo, credenciales de acceso. Con estas, los atacantes pueden acceder a mas información o incluso robar dinero.



### Tipos de ataques cibernéticos

#### 01 *Phishing* por correo electrónico

Cualquier mensaje de correo electrónico malintencionado con el fin de engañar a los usuarios para que divulguen información sensible o confidencial. Principalmente, buscan robar las claves de acceso de cuentas o sistemas que contienen información delicada del usuario o de sus lugares de trabajo.



#### 02 *Smishing*

Son aquellos mensajes de texto o SMS, que los atacantes utilizan para engañar a los usuarios. Envían mensajes de carácter urgente junto con enlaces a páginas web malintencionadas, con el objetivo de que el usuario revele sus claves de acceso.

#### 03 *Whaling* (Fraude a los peces gordos de la empresa) y *Spear Phishing*

Son ataques dirigidos principalmente a empleados de alto nivel de las empresas o a aquellos con privilegios específicos. Los atacantes se hacen pasar por el director general de la empresa o la persona encargada de transferir dinero. El objetivo principal es robar dinero y credenciales de acceso.



#### 04 *Vishing*

Son los mensajes por llamada telefónica o grabaciones en los buzones de voz. Los atacantes se hacen pasar por un familiar en una dificultad o por una entidad con la que el usuario está vinculado.

#### 05 *Wifi gemelo maligno*

Los atacantes suplantan una red wifi gratuita, engañando a los usuarios para que se conecten a un punto de acceso malintencionado. El objetivo es robar credenciales o descargar programas malintencionados en sus dispositivos.



Lea con calma cada mensaje que le llegue, revise dirección de correo, logos, firmas, redacción del mensaje, entre otros detalles. Si sospecha de algo, es mejor no responder o comunicarse con sitios oficiales para validar la información recibida.