GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

PROTEJA SU INFORMACIÓN PERSONAL

CONSEJOS DE CIBERSEGURIDAD

RECUERDE

Si es ***víctima*** de una estafa,
llame

017 (INCIBE)
(INSTITUTO NACIONAL DE CIBERSEGURIDAD)

062 (GUARDIA CIVIL)

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

¿CUÁLES SON LAS POSIBLES AMENAZAS?

PHISING O CORREOS FRAUDULENTOS

· Si recibe un correo que parece ser de su banco, una empresa con la que tenga un contrato, paquetería, etc. ALERTA, si le pide información personal, dinero o hacer clic en algún enlace.

LLAMADAS TELEFÓNICAS FRAUDULENTAS

· Si le llaman haciéndose pasar por su entidad bancaria, servicio contratado de la luz, agua o gas o algún comercio pidiéndole datos ¡DESCONFÍE! No suministre datos por teléfono ¡devuelva la llamada!

FALSO FAMILIAR

· Si un supuesto famliar, principalmente hija, hijo, nieta o nieto aparece a través de las redes sociales o recibe un mensaje de texto o un WhatsApp diciendo que le escriba o envíe dinero ¡ALERTA! puede ser una estafa ¡no se fie!

FRAUDE DE INVERSIÓN O AYUDA

· Ofrecen inversiones muy rentables, con promesas de altos rendimientos o se crean sitios web que simulan programas de ayuda... ¡CUIDADO! no envíe dinero. Contraste antes la información.

FRAUDES ROMÁNTICOS

· Tenga precaución al utilizar las páginas de citas románticas; no todo es lo que parece. Desconfíe de la persona que le de cariño a través de la pantalla sin conocerle.

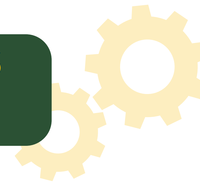
GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

CONSEJOS DE CIBERSEGURIDAD

UTILICE CONTRASEÑAS SEGURAS

- Utilice **patrones biométricos** como: **huella dactilar** o **reconocimiento facial**, además de **contraseñas fáciles de recordar**.
- Intente **no utilizar la misma contraseña** en diferentes servicios y NO las apunte en su dispositivo... **MEMORÍCELAS**.

MANTENGA SUS DISPOSITIVOS ACTUALIZADOS



- Las **actualuzaciones** deben descargarse desde **fuentes fiables**, cuidado con las páginas de apariencia legítima.
- Actualice desde ajustes o configuración en su dispositivo móvil: busque **"actualizaciones", descargue y actualice.**

EVITE CONECTARSE A REDES WIFI PÚBLICAS

- Es recomendable utilizar una **red privada**, **SU propia red**, en vez de conectarse a la red WiFi pública disponible.
- Si conecta **Bluetooth** o **NFC** en su dispositivo, **DESCONÉCTELO** una vez utilizado.

Si es ***víctima*** de una estafa, ***llame***

017 (INCIBE)
(INSTITUTO NACIONAL DE CIBERSEGURIDAD)

062 (GUARDIA CIVIL)

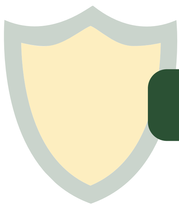
GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

NO REVELE INFORMACIÓN PERSONAL

- Si le llaman desde su **entidad bancaria** o cualquier servicio que tenga contratado, solicitando datos, **devuelva la llamada** al número que tenga **REGISTRADO** y no al que le han llamado.
- **¡CUIDADO!** no contrate servicios por teléfono sin asesoramiento.

ES MUY IMPORTANTE QUE HAGA COPIAS DE SEGURIDAD

- Si tiene información importante para usted como fotos, documentos, etc. en el teléfono, intente que **NO** sea el **único medio de ALMACENAJE**.
- **Haga copias de seguridad.**



USE ANTIVIRUS

- El **antivirus** actúa como su **defensa** frente a amenazas digitales y riesgos cibernéticos.
- Asegúrese de **mantenerlo siempre actualizado** con la última versión.

REVISE LAS PÁGINAS DONDE NAVEGA

- **Revise los enlaces**, verifique que la página web donde va a entrar es la correcta.
- **NO SE DEJE ENGAÑAR.**

Si es ***víctima*** de una estafa, ***llame***

017 (INCIBE)
(INSTITUTO NACIONAL DE CIBERSEGURIDAD)

062 (GUARDIA CIVIL)

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

IDENTIFIQUE LOS CORREOS FRAUDULENTOS

- **Evite** la apertura de **enlaces sospechosos**, por muy fiables que le parezcan. Aunque reciba un correo con apariencia de su banco o un mensaje de texto.
- **NUNCA clique** en ningún enlace ni descargue archivos.

EXTREME LAS PRECAUCIONES EN LAS COMPRAS ONLINE

- En **compras por internet** contrate una **tarjeta prepago** exclusivamente para ello y **compruebe** que los **cargos efectuados** sean correctos.
- **NO comparta códigos** recibidos por SMS ni compre desde enlaces propuestos por redes sociales.

ACTIVE VARIOS FACTORES DE AUTENTICACIÓN

- Al momento de efectuar pagos en línea o manejar datos personales, **habilite múltiples métodos** para verificar contraseñas.
- **NO SE LO PONGA FÁCIL A LOS MALOS.**

#ROMPA LA CADENA, SEA PARTE DEL CAMBIO, PIDA ¡AYUDA!

Si es *víctima* de una estafa, *llame*

017 (INCIBE)
(INSTITUTO NACIONAL DE CIBERSEGURIDAD)

062 (GUARDIA CIVIL)