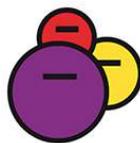


GUÍA CIBERSEGURIDAD

CONOCE E IDENTIFICA LAS PRINCIPALES ESTAFAS Y FRAUDES A TRAVÉS DE INTERNET, APRENDE A EVITARLAS Y A AFRONTARLAS EN CASO DE SUFRILAS



ADICAE CV

Asociación de Usuarios de Bancos, Cajas y Seguros



**GENERALITAT
VALENCIANA**

Conselleria d'Economia
Sostenible, Sectors Productius,
Comerc i Treball

CONOCE E IDENTIFICA LAS PRINCIPALES ESTAFAS Y FRAUDES A TRAVÉS DE INTERNET, APRENDE A EVITARLAS Y A AFRONTARLAS EN CASO DE SUFRIRLAS

¿QUÉ ES EL PHISHING?

Con este término se hace referencia a **FRAUDES** que **tienen como finalidad robar información confidencial** del receptor, (nombres de usuarios, contraseñas y datos bancarios).



Utilizan para ello, correos electrónicos, mensajes SMS, redes sociales, aplicaciones de mensajería instantánea o incluso llamadas de teléfono.

CÓMO IDENTIFICARLO:

LA DIRECCIÓN DEL CORREO ELECTRÓNICO SUELE SER FALSA:

Es importante comprobar por ejemplo que el dominio coincide con la entidad bancaria, que supuestamente remite el correo.

SUELE SER UN CORREO, SMS O LLAMADA, INFORMANDO DE SITUACIONES NEGATIVAS Y PROBLEMÁTICAS QUE PARA RESOLVERSE REQUIEREN UNA ACTUACIÓN URGENTE

por parte del receptor, generalmente aportación de datos bancarios o realización de transferencias a su favor, con la finalidad según refieren de evitar un perjuicio mayor, en caso de no realizarlas.

SUELEN CONTENER COMUNICACIONES UNIPERSONALES,

por ejemplo no se dirigen al receptor con su nombre y apellidos, contienen expresiones genéricas e indeterminadas.

SOLICITAN DATOS BANCARIOS, (números de cuenta, tarjetas, claves).

SUELEN CONTENER ERRORES ORTOGRÁFICOS, GRÁFICOS MUY SIMPLES Y LOGOS FALSOS,

similares pero distintos a los de entidades bancarias o empresas de las cuales refieren el envío.



RECOMENDACIONES PARA EVITAR EL PHISHING

LA BANCA, EMPRESAS DE ENERGÍA Y DE TELECOMUNICACIONES

NO SUELEN PEDIR DATOS PERSONALES MEDIANTE CORREO ELECTRÓNICO

ANTE UN CORREO DONDE SE SOLICITAN DATOS PERSONALES: ¡ALERTA!



1 COMPROBAR LA REDACCIÓN Y ORTOGRAFÍA DE LOS CORREOS RECIBIDOS.

► Suelen tener errores de redacción y ortográficos, al utilizar traductores automatizados.



2 COMPROBAR QUE EL CORREO PROCEDE DE UNA CUENTA ORIGINAL.

► El email debe coincidir con la empresa que lo envía, suelen utilizar un correo similar al oficial.
Ejemplo: gmail.com en vez de gmaill.com



3 REVISAR LA URL.

► Colocar el cursor del ratón sobre el texto para ver la URL a la que nos dirige.



4 NO DESCARGAR ARCHIVOS ADJUNTOS.

► No descargar los archivos adjuntos al email sin confirmar que se trata de un mensaje legítimo.



* * * *

5 SI TE HA OCURRIDO: MODIFICAR LA CONTRASEÑA DEL SERVICIO SUPLANTADO Y PONERLO EN CONOCIMIENTO DE LA ENTIDAD.

FALSOS PRÉSTAMOS

CORREOS ELECTRÓNICOS O PÁGINAS WEB QUE OFRECEN PRÉSTAMOS

UN PRESTAMISTA DE OTRO PAÍS NO SUELE PRESTAR DINERO SIN PEDIR NADA A CAMBIO O CON UN INTERÉS TAN BAJO

¿Cómo identificarlos?



1. Comprobar datos nombre, apellidos, email. Por si los datos aparecieran en otra estafa.



2. Buscar si estamos ante una entidad fiable. Hay que acudir a entidades oficiales de crédito.



3. Ojo, a la ortografía y a los errores gramaticales.



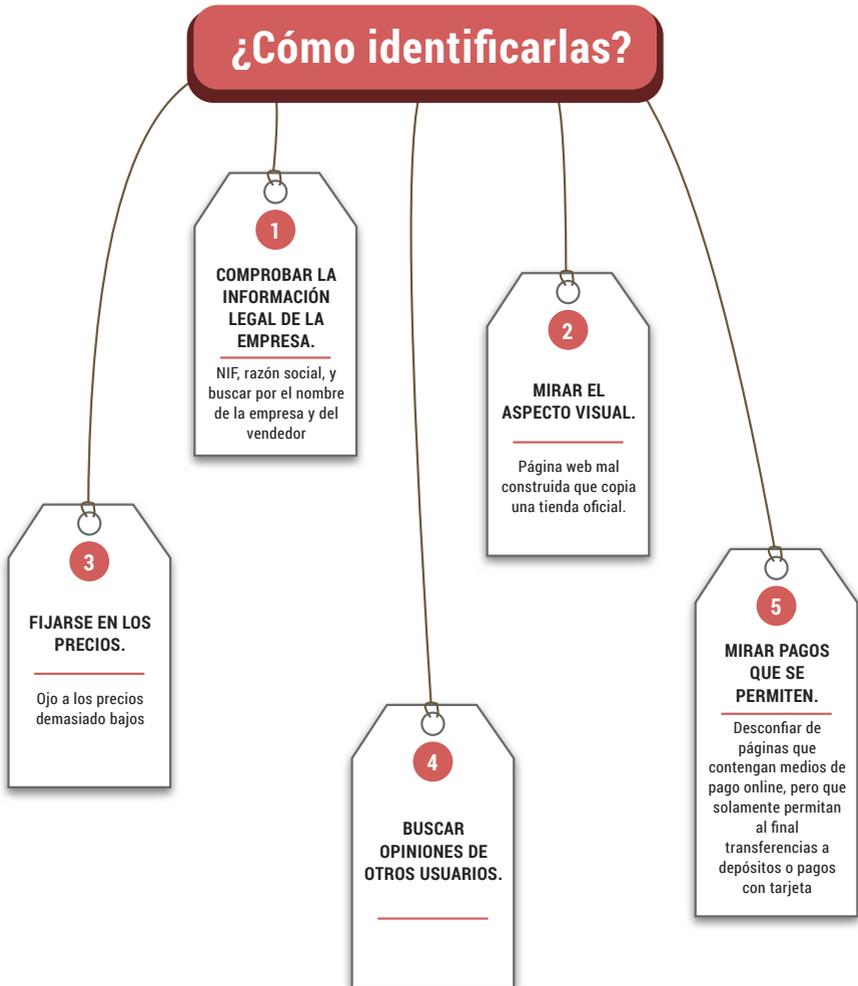
4. Denunciar ante el banco correspondiente la cuenta fraudulenta.

TIENDAS ONLINE FRAUDULENTAS

LAS TIENDAS ONLINE FIABLES TIENEN UNA CONEXIÓN SEGURA POR HTTPS Y CUENTAN CON CERTIFICADO DE SEGURIDAD.

APARECE UN "AVISO LEGAL" EN LA WEB QUE CONTIENE LA POLÍTICA DE PRIVACIDAD.

¿Cómo identificarlas?



FRAUDES EN COMPRAVENTAS OLINE

COMPRAVENTA EN PÁGINAS O A TRAVÉS DE APP EN LOS GENERALMENTE APARECE UN PRODUCTO A BAJO PRECIO.

Piden pago por adelantado mediante transferencia como condición previa al envío. Tras efectuar el ingreso, el envío nunca llega. El usuario desaparece y su perfil deja de aparecer en la aplicación.

CÓMO EVITARLOS:

REVISA EL PERFIL DEL COMPRADOR O VENDEDOR



SI ERES COMPRADOR:

Pon atención en el perfil del vendedor, suelen crearse a propósito. No llevan mucho tiempo creados en la página y siempre tienen urgencia en realizar la venta.



SI ERES VENDEDOR:

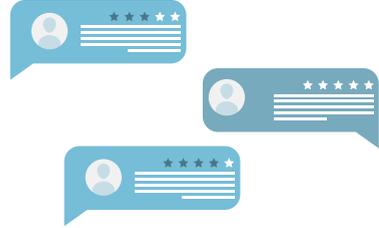
Desconfía de perfiles extraños, de países extranjeros y de las prisas para realizar la compra bajo cualquier condición.

MIRA BIEN EL ANUNCIO



Suelen utilizar imágenes falsas y productos falsificados. Pide información adicional al vendedor, más imágenes y fotografías para comprobar que es real.

REVISAR COMENTARIOS



Revisa comentarios y valoraciones de otros usuarios sobre el vendedor. **Sino tiene, son pocos o negativos: desconfía.**

MIRA SU PRECIO



Desconfía cuando ofrecen un producto muy por debajo de su valor en el mercado.

MEDIOS DE PAGO SEGUROS



Intenta pagar contra reembolso, paypal o con otros medios que aseguren que se recibe el dinero o el producto.

DENUNCIA

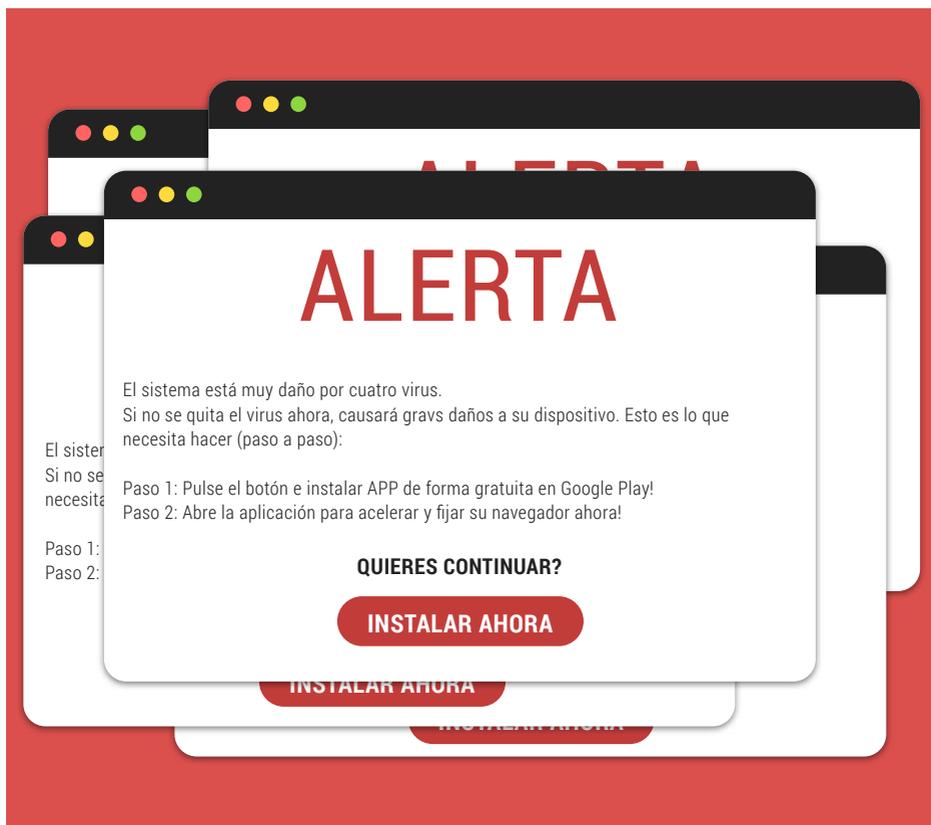


Denuncia ante la plataforma si consideras que el anuncio es falso, para que pueda ser revisado y eliminado.

¡NUNCA! ESCRIBAS EN UN CORREO EL NÚMERO DE LA TARJETA NI EL PIN PARA REALIZAR UNA COMPRA. SOLAMENTE SE PIDE EL CÓDIGO DE SEGURIDAD QUE ESTÁ EN LA PARTE TRASERA DE LA TARJETA.

FRAUDES CON INSTALACIÓN DE SOPORTE TÉCNICO

APARECEN VENTANAS EMERGENTES DICHIENDO QUE EL ORDENADOR ESTÁ INFECTADO Y QUE SE LLAME UN SOPORTE TÉCNICO.



Piden dinero para una falsa reparación.

Pueden instalar programas maliciosos para robar información o realizar operaciones en nuestro nombre.

CÓMO EVITARLOS:



1.-
Instalar solo aplicaciones originales desde páginas webs oficiales.



2.-
Desinstalar aplicaciones que hayan podido instalarse.



3.-
Cambiar claves de acceso, y utilizar claves complejas que contengan números y mayúsculas.



4.-
Reportar el incidente, poniéndolo en conocimiento del proveedor original.



5.-
Llamar al banco para cancelar los pagos al soporte técnico falso, lo antes posible.

Y SOBRE TODO:

INFÓRMATE, FÓRMATE Y PROTÉGETE



Infórmate y participa para ser un consumidor crítico,
responsable y solidario con Adicae CV. Únete a la fuerza
colectiva de los consumidores y consumidoras.

NUESTRAS REDES SOCIALES



@ADICAE



AdicaeConsumidores



user/ADICAE1

NUESTRA PÁGINA WEB

comunidadvalenciana.adicae.net

VEN A NUESTRAS SEDES EN:

VALENCIA

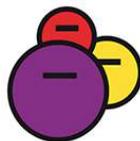
C/ Navarra 9, bajo
46008 . Valencia (Zona
Abastos, metro Ángel
Guimerá)
963 540 101

ALICANTE

C/ Arquitecto Guardiola,
15, Entresuelo A.
03007 - Alicante (Barrio
Benalúa)
965 286 538

CONTACTA CON ADICAE COMUNIDAD VALENCIANA:

coordinacionvalencia@adicae.net
963540101



ADICAE CV

Asociación de Usuarios de Bancos, Cajas y Seguros



**GENERALITAT
VALENCIANA**

Conselleria d'Economia
Sostenible, Sectors Productius,
Comerc i Treball