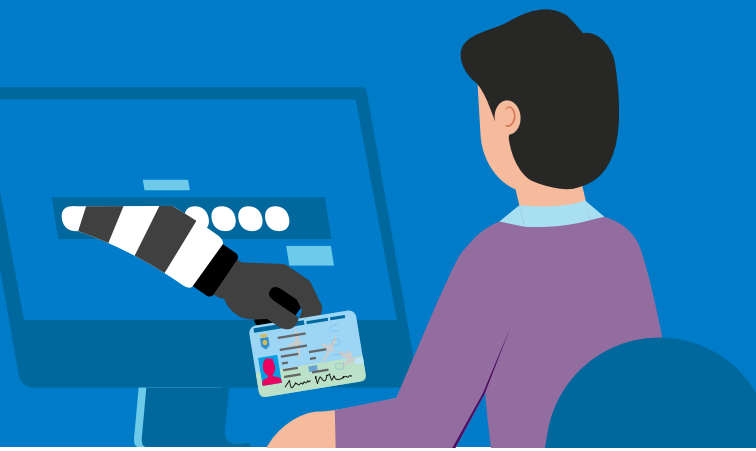
Servicio Estatal de Datos Personales
Ministerio del Interior y de Relaciones del Reino



Fraude de identidad

No le des una oportunidad a los estafadores

Un ID seguro

Pedir un préstamo de dinero y desaparecer de la faz de la tierra. Contratar un servicio de teléfono y conseguir un teléfono inteligente de última generación.

Imagínate que un estafador hace esto en tu nombre. El estafador desaparece sin dejar rastro y tú recibes la factura. Esto se llama «fraude de identidad» y puede tener graves consecuencias para las víctimas de este delito.

¿Cómo es posible? Un estafador consigue tus datos de identidad. Por ejemplo, a través de una copia de tu documento de identidad, de un anuncio en línea o de un correo de phishing. Con estos datos, el estafador puede pedir un préstamo en tu nombre.

Este folleto te informa de lo que puedes hacer para evitar el fraude de identidad.

Puede encontrar información sobre el uso seguro de su computadora, tableta o teléfono en línea en www.veiliginternetten.nl

No permitas que te roben tus datos de identidad

- Guarda tu documento de identidad (DNI o similar) en un lugar seguro. ¿Lo has perdido o te lo han robado? Si te ocurre esto, presenta una denuncia en asuntos civiles [Burgerzaken] para que bloqueen el documento y solicitar un nuevo documento de identidad.

- Complícales las cosas a los hackers y asegura tus cuentas (en línea) con la verificación en dos pasos. De esta manera, no te limitarás a acceder con tu nombre de usuario y contraseña, sino que utilizarás un código de acceso adicional que recibirás, por ejemplo, por mensaje de texto.

- Instala siempre las últimas actualizaciones en tu ordenador y teléfono, y utiliza contraseñas diferentes para tus cuentas en línea. ¿Te cuesta recordarlas? En ese caso, utiliza un gestor de contraseñas.

No compartas tus datos y documentos de identidad con otras personas

- ¿Compras o vendes en línea? Nunca envíes una copia de tu documento de identidad o tarjeta bancaria.

- ¡Reconoce la suplantación de identidad! La suplantación de identidad o phishing no solo se hace por correo electrónico, sino también por teléfono, SMS o WhatsApp. Si te piden tu DNI u otro documento de identidad, datos bancarios o de acceso, ten mucho cuidado.

- No facilites tus datos de identidad, datos de acceso o códigos PIN por teléfono. En el caso del spoofing, los estafadores utilizan un número de teléfono existente de tu banco, así que no te dejes engañar por el número de teléfono que ves en tu pantalla.

- ¿La situación te genera desconfianza? Si tienes dudas, llama a la persona u organización que te pide los datos y comprueba que la historia es cierta.

No regales tus datos de identidad

- Elimina los archivos y las cuentas de los ordenadores y teléfonos antes de venderlos o de deshacerte de ellos.
- Sé consciente de lo que compartes en las redes sociales. No muestres fotos de tu pasaporte, sédula o permiso de conducir.
- ¿Tienes que entregar una copia de tu documento de identidad? En ese caso, haz que sea inutilizable para los estafadores: escribe la fecha y la finalidad en esa copia, y tacha la información que el destinatario no necesita. Para hacer esto puedes utilizar la aplicación KopieID.

Descarga la aplicación KopieID desde Play Store o App Store.

No se lo pongas demasiado fácil a los delincuentes y mantente alerta

La Oficina central de información sobre el fraude de identidad [Centraal Meldpunt Identiteitsfraude] (CMI), ofrece consejos y asesoramiento para prevenir el fraude de identidad y apoya a las víctimas para que detengan el abuso y reparen las consecuencias.

Más información
www.rvig.nl/cmi

¿Eres víctima de un fraude de identidad?

- Denuncia en la policía
- Informa a la Oficina central de denuncias de usurpación [Centraal Meldpunt Identiteitsfraude] (CMI) a través de www.rvig.nl/cmi