Uso seguro de su Tarjeta ING Corporate

Introducción

Con su Tarjeta Corporate de ING podrá pagar, entre otras cosas, el alojamiento en hoteles, la asistencia a congresos, billetes de avión, restaurantes y taxis. Pero la Tarjeta Corporate le ofrece aún más.

Piense, por ejemplo, en las agencias de viajes que, por la gran comodidad que ofrece, han optado por la Tarjeta Corporate para hacer las reservas. Esta tarjeta la usa cada vez más gente por la sencillez y facilidad de su sistema de pago (de profesionales).

Naturalmente, usted querrá asegurarse de que sus pagos se realizan de forma correcta. En este documento le ofrecemos información al respecto. ING hace todo lo que está en su mano para hacer que los pagos sean seguros y para que así se mantengan. Pero ese objetivo no lo podemos lograr nosotros solos. Con solo atenerse a las reglas básicas ya estará quitando oportunidades a los delincuentes.

En este folleto le explicamos dichas reglas básicas y le damos consejos sobre cómo hacer los pagos de forma segura y cómo reconocer el fraude; además le explicamos lo que hacemos en ING para que su Tarjeta Corporate sea lo más segura posible. Al final de este folleto incluimos un glosario en el que se explica el significado de los diferentes términos (de Internet) que se han utilizado en él.

Útil y gratuita

Use la aplicación ING Commercial Card y use el portal ING Commercial Card. De esa manera tendrá una visión clara de sus transacciones, de sus gastos, de su saldo y del importe que queda hasta llegar al saldo máximo disponible. La aplicación ING Commercial Card se puede descargar de Apple App Store y de Google Play (Android).
Para buscar la aplicación escriba: ING Commercial Card
El portal ING Commercial Card la encontrará en: www.ingcommercialcard.com

En caso de fraude, notifíquelo de inmediato

¿Ha sido usted víctima de fraude con su Tarjeta Corporate? Si es así, comuníquenoslo de inmediato. Así podremos ayudarle a usted y a otros clientes, ahora y en el futuro. Estamos disponibles las 24 horas del día, los 7 días de la semana, incluso si se pone en contacto con nosotros desde el extranjero o mediante nuestros números de acceso locales. Dichos números constan al final de este folleto.

Índice

1. Las cinco reglas básicas para un pago seguro

Hemos sintetizado las reglas de seguridad uniformes de los bancos holandeses en cinco reglas básicas de uso de su Tarjeta Corporate. Así las podrá recordar fácilmente.

Regla básica 1: Proteja sus códigos

Si usted no daría nunca la llave de su casa a un desconocido, no lo haga tampoco con sus códigos de seguridad. Protéjalos bien.

- **Apréndase de memoria sus códigos**
  A la hora de crear un código de seguridad o una contraseña no elija fechas de nacimiento o el nombre de un miembro de su familia ni ningún otro dato que sea fácil de adivinar. ¿Teme olvidar los códigos de seguridad? En ese caso, anótelos de tal forma que sea imposible que los descifren otras personas o invéntese una regla mnemotécnica. Por ejemplo, una frase con mayúsculas y números es segura y fácil de recordar. Por ejemplo: «¡Prefiero oír a U2 que la 6ª de Beethoven!». Si la frase entera no cabe, utilice solo las iniciales de cada palabra: «¡PoaU2ql6ªdB!»

- Una buena manera de recordar la clave de su Tarjeta Corporate es asignar a cada cifra de la clave una palabra que conste del mismo número de letras que la cifra a la que representa. Con 4 palabras se puede crear una frase. Pongamos que su clave es: 9246. Con esa combinación de cifras puede crear la siguiente frase: En (2) Lhardy (6) despachan (9) consomé (7).

- **Impida que nadie miren**
  Asegúrese de que nadie pueda mirar cuando introduce el código. Puede hacerlo tapando el teclado con el cuerpo o con una mano.

- **No revele nunca sus códigos**
  Si alguien le pide sus códigos de seguridad o contraseñas, por ejemplo para el portal ING Commercial Card, no se los dé bajo ningún concepto. Sus códigos son estrictamente personales. Así que no se los debe dar a nadie; recuerde también que los empleados de ING nunca le pedirán sus códigos de seguridad: ni en el mostrador, ni por teléfono, ni por e-mail, ni en ninguna página web o aplicación de ING de ningún tipo, ni de ninguna otra manera.

Regla básica 2: Proteja su Tarjeta Corporate

Si no permite que le roben la cartera, no lo haga tampoco con su Tarjeta Corporate. Protéjala bien.

- **Maneje su Tarjeta Corporate con precaución**
  Su Tarjeta Corporate es estrictamente personal. Por ello no la debe prestar. No deje la Tarjeta Corporate en cualquier sitio; guárdela siempre en un lugar fijo y seguro inmediatamente después de usarla. Asegúrese de que nadie pueda llevarse la Tarjeta Corporate de forma desapercibida.

  No entregue la Tarjeta Corporate a un camarero, por ejemplo: es preferible que le acompañe hasta la terminal de pago. Si, a pesar de todo no le queda más remedio que entregar la Tarjeta Corporate, asegúrese de que la tarjeta que le devuelven es la misma que usted ha entregado..

  Compruebe al menos una vez al día que sigue teniendo la Tarjeta Corporate. Ésta es una obligación que también se incluye en nuestras condiciones.

- **No se deje distraer**
  No permita que nadie le distraiga cuando esté usando la Tarjeta Corporate. Si no está usted atento, en un descuido le podrían cambiar fácilmente su Tarjeta Corporate por otra tarjeta de crédito del mismo color, por ejemplo. A eso se le llama el truco del trueque. Si en un momento determinado sospecha que no es seguro utilizar la Tarjeta Corporate, es mejor que siga su instinto y que mantenga la tarjeta a buen recaudo.

- **Compruebe regularmente que tiene la Tarjeta Corporate**
  ¿Le ha abordado algún desconocido en la calle? ¿Ha tropezado con alguien? En ese caso compruebe siempre de inmediato si aún tiene su Tarjeta Corporate. ¿No se la devuelven después de haber pagado con ella? En ese caso póngase en contacto con nosotros (24 horas al día, 7 días a la semana) llamando al +31 (0)10 428 95 81 o a uno de nuestros números de acceso locales (se indican al final de este folleto).

Regla básica 3: Proteja su equipo

Si usted cierra con llave la puerta de casa, hágalo también con los dispositivos que utilice para las transacciones por Internet con su Tarjeta Corporate, tales como el móvil, la tableta, el ordenador de mesa o el ordenador portátil. Dótelos de buenos sistemas de protección. De esa manera los delincuentes tendrán pocas posibilidades de instalar software malicioso, tal como, por ejemplo, un «troyano», que les permita averiguar los datos personales de su Tarjeta Corporate.

- **Instale solamente software legal y conocido ale en bekende software**
  Asegúrese de configurar su móvil de tal manera que no permita el acceso a aplicaciones provenientes de fuentes desconocidas. Por tanto, no haga «root» o «jailbreak» a su móvil ni descargue aplicaciones que no procedan de tiendas de aplicaciones oficiales. Instale solamente software legal de procedencia comprobada. Lo puede hacer yendo a la página web oficial del proveedor. Si le ofrecen un programa de software desconocido, no descargue el programa inmediatamente: compruébelo antes con un detector de virus.

- **Utilice la versión más moderna de la aplicación y de su sistema operativo**
  Tanto la aplicación ING Commercial Card como el sistema operativo de su móvil, tableta y ordenador se van complementando regularmente con más y mejores técnicas de seguridad. Por eso le recomendamos que actualice regularmente su dispositivo. Active preferentemente la opción de actualización automática.

- **Introduzca un código de acceso en su dispositivo**
  Con un código de acceso evita usted que otras personas tengan acceso demasiado fácilmente a sus datos personales. Piense no solo en los datos de su Tarjeta Corporate, sino también en sus contactos, mensajes y fotografías.

- **Utilice un detector de virus, un firewall y un anti-spyware**
  Asegúrese de que en su ordenador de mesa o portátil esté instalado un detector de virus, un cortafuegos y un anti-spyware antes de hacer pagos por Internet con su Tarjeta Corporate. De esa manera tendrán menos oportunidades los virus y los programas no deseados. Actualmente también hay detectores de virus para móviles y tabletas.

- **Proteja su conexión de Internet inalámbrica (wifi)**
  Probablemente, usted no hará transacciones por Internet con su Tarjeta Corporate si la Red no está protegida. Proteja por ello su propia wifi con una contraseña. Pida consejo al respecto a su servidor de Internet. ¿Utiliza redes wifi públicas fuera de casa? Si es así, es preferible que no haga transacciones por Internet con su Tarjeta Corporate.

Regla básica 4: Compruebe sus pagos y disposiciones de dinero de su cuenta

Siempre es interesante comprobar previamente qué es lo que uno paga exactamente. Y confirmar regularmente los importes que después se deducen de la cuenta. Eso se puede hacer con el portal ING Commercial Card o con la aplicación ING Commercial Card. Con la aplicación ING Commercial Card puede usted ver sus transacciones a tiempo real, entre otras cosas.

- **Sepa qué paga**
  Compruebe que el importe que tiene que pagar se muestra correctamente en la pantalla o – si está en el extranjero y tiene que firmar un recibo – que en éste figura el importe correcto. Guarde la copia del recibo para su administración. De esa manera siempre tendrá un documento probatorio para el caso de que el importe que figure en el extracto de su Tarjeta Corporate no sea correcto.

  Asegúrese de evitar sorpresas a la hora de convertirse la divisa extranjera en la que ha pagado en la divisa de su país, y que no le sorprenda el importe que se cargue a su Tarjeta Corporate.

- **Siga un orden adecuado**
  Si va a realizar una compra por Internet, introduzca el número de la tarjeta de crédito, la fecha de caducidad y los códigos de seguridad solamente cuando esté seguro de hacer la compra.

- **Compruebe en línea sus extractos bancarios**
  Compruebe sus extractos bancarios al menos una vez cada dos semanas. Así podrá ver si las transacciones que figuran en ellos son legítimas y podrá informarnos a tiempo de cualquier anomalía.

- **Comunique cualquier perjuicio a tiempo**
  Si ha sufrido algún perjuicio por no haber podido comprobar durante cierto tiempo los extractos de su Tarjeta Corporate, podremos pedirle que lo demuestre. En principio, los perjuicios de los que se informe después del plazo de treinta días desde la fecha del extracto correspondiente no se abonan.

Regla básica 5: Ante la duda, llame a ING

Si está seguro de que ha sido víctima de un fraude, o si lo sospecha, comuníquenoslo de inmediato. Haciéndolo así podremos intervenir directamente y evitar más perjuicios. Podemos eliminar páginas web falsas, por ejemplo, evitándose así que otros clientes sean víctimas de ellas.

- **Llame de inmediato**
  Si sospecha la existencia de fraude, nos puede llamar de inmediato. También si se ha bloqueado su Tarjeta Corporate, su aplicación ING Commercial Card o su user ID del portal ING Commercial. O si ha recibido un e-mail sospechoso o si alguien le ha intentado sonsacar los datos de su Tarjeta Corporate.

- **Asegúrese de que también nosotros le podamos localizar**
  Si constatamos operaciones sospechosas, intentaremos ponernos en contacto con usted, bien por teléfono o bien con un mensaje de SMS. Por ello le rogamos que indique un número de teléfono móvil a nuestro servicio de atención al cliente. Lo puede hacer en el teléfono +31 (0)10 428 9581 o mediante nuestros números de acceso locales (se indican al final de este folleto).

2. Cómo reconocer un fraude

A pesar de las medidas de seguridad que aplique y de un uso seguro por su parte de la Tarjeta Corporate, siempre cabe la posibilidad de que usted sufra algún tipo de fraude con su Tarjeta Corporate. A continuación le informamos de los diferentes tipos de fraude que se pueden dar.

Fraude con su Tarjeta Corporate

- **Skimming**
  Una modalidad muy conocida de fraude es el skimming: la copia de los datos de la tarjeta de crédito que figuran en la banda magnética. En los últimos años se han tomado diversas medidas para evitar el skimming. Por esa razón cada vez se ve menos esta forma de fraude.

- **Robo, trucos de trueque y maniobras de distracción**
  Aún se siguen viendo casos de cambio fraudulento de Tarjetas Corporate o de robo de códigos de seguridad a base de mirar subrepticiamente mientras se usa la tarjeta de crédito. También se ven casos en los que se distrae al cliente en el cajero automático para llevarse el dinero que se ha sacado. Un ejemplo de ello es el truco del billete de diez euros. Se le distrae a usted con un billete de 10 euros tirado en el suelo mientras le quitan el dinero de cajero.

  Estas modalidades de fraude se dan principalmente en tiendas y en cajeros automáticos. Los mirones se colocan detrás de usted para mirar por encima de su hombro mientras está introduciendo la clave, mientras que otro delincuente intenta distraerle de lo que está haciendo.

Fraude mediante el ordenador

- **Phishing**
  Con el phishing, los delincuentes “pescan” sus códigos de seguridad mediante mensajes de SMS o con páginas web falsas. Usted recibe un SMS o un e-mail en el que le invitan a entrar en un enlace. Sin darse usted cuenta le dirigen a una página web falsa, del portal ING Commercial Card, por ejemplo, en la que se le solicita que introduzca sus códigos de seguridad para acceder a ella. Por tanto, no pulse en enlaces sospechosos y elimine de inmediato el e-mail en cuestión de su buzón de entrada.

  Los mensajes de phishing se reconocen por las siguientes características:
  - En el mensaje se suele aducir alguna razón de urgencia.
  - En él se le solicita que pulse en un enlace. Sin darse usted cuenta le dirigen a una página web falsa en la que se le solicita que introduzca sus códigos de seguridad para acceder a ella.
  - El mensaje se parece a menudo a un mensaje de su banco.

- **Malware**
  El malware es software malicioso con el que el delincuente, por ejemplo, puede manejar su ordenador a distancia. Así pueden averiguar sus datos de acceso. El malware se puede instalar con total facilidad en cualquier ordenador que no esté protegido con un antivirus y un buen cortafuegos. Y eso ocurre a menudo sin que usted se dé cuenta. Un ejemplo clásico de malware son los troyanos.

El malware se reconoce por las siguientes características:
- A veces una determinada página web tiene un aspecto diferente al que usted está acostumbrado. Aparece en ella, por ejemplo, un campo adicional para que introduzca su número de teléfono.
- Un ordenador infectado con malware suele ser más lento de lo habitual y se bloquea con frecuencia.

Fraude mediante el teléfono

- **Phishing**

  Los delincuentes también "pescan" con el phishing llamándole por teléfono y pidiéndole sus códigos de seguridad, tales como la clave de su Tarjeta Corporate, sus datos de acceso del portal ING Commercial Card u otros datos personales. El phishing también se da mediante SMS, con mensajes de e-mail y en páginas web falsas.

  Una técnica habitual es que el delincuente le llame por teléfono y se haga pasar por otra persona, por ejemplo por un empleado de ING o de una empresa de ordenadores o de software. Le suelen contar una historia creíble ante la que usted tiene que responder de inmediato, a continuación de lo cual le solicitan sus códigos de seguridad. Recuerde que los empleados de ING (y de otras empresas) nunca le van a pedir sus códigos de seguridad.

  ¿Duda de que tenga al teléfono un empleado de ING? Si es así, pregúntele su nombre y llámenos al teléfono que figura al final de este folleto. El empleado de ING entenderá perfectamente su preocupación. Y nosotros le pondremos en contacto con él.

  Ejemplos de llamadas de teléfono falsas:
  - Unos días después de haber cumplimentado los datos de su tarjeta de crédito en un e-mail falso recibe una llamada de phishing de su banco, diciéndole que hay una incidencia con su Tarjeta Corporate y pidiéndole datos adicionales para "solucionar el problema". Más tarde se da usted cuenta de que se ha cometido un fraude en la cuenta de su Tarjeta Corporate.
  - Usted recibe una llamada de una persona que se hace pasar por empleado de una empresa de ordenadores o de software. Dicho empleado le dice que vaya a una página web para instalar determinado software.
  - A menudo se le dice que es necesario para la seguridad de su ordenador. El software que se le pide que instale es malware. Una vez instalado dicho malware, cuando introduzca los datos de su Tarjeta Corporate para hacer cualquier transacción de Internet, esos datos quedarán expuestos.
  - Usted recibe una llamada de una persona que se hace pasar por empleado de ING y que le dice que tiene que comprobar sus datos, por ejemplo, el nombre de usuario y contraseña de su portal ING Commercial Card.
  - Los empleados de ING nunca le pedirán esos datos. Por tanto, no comunique sus códigos a nadie.

3. ¿Qué medidas preventivas toma ING?

En los puntos anteriores le hemos dado una serie de consejos de seguridad para sus pagos. Naturalmente, ING aplica una serie de técnicas, visibles e invisibles, para garantizar la seguridad de su Tarjeta Corporate.

Seguridad en la Tarjeta Corporate

- El chip de su Tarjeta Corporate y la ranura protegida de los cajeros automáticos son medidas de seguridad para evitar el skimming.
- Cuando paga con su Tarjeta Corporate se le suele pedir su clave en lugar de su firma, porque es más seguro.
- Además del número de tarjeta, su Tarjeta Corporate tiene en el reverso un CVC (Código de verificación de la tarjeta). Ese código de tres cifras es un elemento de seguridad adicional.

Seguridad en los pagos

- **Alerta de Seguridad SMS**
  Cuando vaya a realizar alguna transacción de riesgo para la que se requiera una verificación adicional, recibirá en su móvil una Alerta de Seguridad mediante un mensaje de SMS. En ese SMS le pedimos que confirme la transacción que esté realizando. Si nota cualquier anomalía, comuníquenoslo de inmediato para bloquear al momento su tarjeta y evitar así que se cometa cualquier otro fraude con ella. El SMS se envía desde el número: +44 78 60 04 74 44.
  - Si se trata de una compra conocida, proceda tal como se le indique en el SMS. Después no será necesaria ninguna acción más por su parte.
  - Si se trata de una compra desconocida para usted, proceda tal como se le indique en el SMS. ING bloqueará su Tarjeta Corporate de inmediato y le enviará un segundo SMS con información detallada sobre cómo tiene que proceder a continuación.

  Este servicio es gratuito para todos los titulares de una Tarjeta Corporate. Lo único que necesitamos de usted es un número de teléfono móvil correcto. Llame a nuestro servicio de atención al cliente para confirmar que disponemos de su número de teléfono.

  Conviene saber, por otro lado, que no responder al SMS de Seguridad no conlleva ninguna responsabilidad en caso de fraude. Pero su compra sí se realizará. Dependiendo de la situación, más tarde se puede bloquear (temporalmente) su tarjeta en la siguiente compra.

- **Mastercard ID check**
  Las compras por Internet en empresas participantes en el sistema de Mastercard ID check están protegidas contra el fraude. Usted verá una pantalla con el texto «Procesar». En la mayoría de los casos ING realizará de forma inadvertida todos los controles de seguridad, aunque en determinadas transacciones le pediremos que introduzca un determinado código. Ese código se le enviará por SMS. Le rogamos que nos facilite las cosas comunicándonos su número de móvil.

- **Bloqueo de la Tarjeta**
  Si ING detecta alguna situación (muy) sospechosa, podrá bloquear su Tarjeta Corporate de forma preventiva. Tal circunstancia se le comunicará con la mayor rapidez posible por teléfono, mediante un SMS o por carta. Por eso, si no puede realizar una determinada operación, póngase en contacto con nosotros de inmediato.v

4. Fraude, ¿y ahora qué?

ING hace todo lo que está en su mano para evitar que usted sufra cualquier tipo de fraude. Y si usted aplica los consejos que le damos en este folleto, los delincuentes tendrán pocas posibilidades de cometer fraude con su Tarjeta Corporate.
Si, a pesar de todo, es usted víctima de un fraude, nosotros arreglaremos rápidamente la situación por usted. Proceda, por tanto, del modo siguiente:

Comunique el fraude

- **Con la mayor rapidez posible**
  Si constata o sospecha la existencia de cualquier fraude, comuníquenoslo por teléfono con la mayor rapidez posible. Puede hacerlo durante las 24 horas del día, 7 días a la semana. En todo caso, debe hacerlo dentro del plazo máximo de 30 días desde la fecha de su extracto bancario (en soporte digital o en papel). Si usted procede diligentemente, podremos evitar que el importe en cuestión se cargue en su cuenta o en la cuenta de la empresa. Y así evitaremos consecuencias financieras imprevistas para usted o para la empresa. En caso necesario también le podemos enviar inmediatamente una Tarjeta Corporate nueva.

- **Formulario de fraude**
  Tras la llamada telefónica le enviaremos un formulario de fraude por correo o, si lo prefiere, por e-mail. Nuestra condición: el formulario nos lo tiene usted que reenviar dentro del plazo máximo de 14 días. Cuanto más rápidamente nos reenvíe el formulario, más rápidamente se podrá tramitar el caso de fraude. En determinados casos, si el dueño de la tienda donde se ha cometido el fraude lo solicita, es posible que le pidamos información adicional a usted.

- **Denuncia**
  Si el fraude con su Tarjeta Corporate se ha cometido después de haberla perdido o de que se la hayan robado, o si usted aún no la ha recibido o si no la ha solicitado, junto al formulario de fraude deberá usted presentar la correspondiente denuncia ante la policía.

Indemnización

- **Nuestra política**
  Nosotros indemnizamos por cualquier fraude que se cometa con su Tarjeta Corporate, siempre que no se le pueda achacar a usted. Durante la conversación telefónica que usted mantenga con nuestro empleado intentaremos causarle las mínimas molestias. Sin embargo, en determinados casos (por ejemplo si ya hemos enviado la orden de cobro) no lo podremos evitar. En todo momento procederemos de acuerdo con usted, de forma que el pago se pueda realizar lo más rápidamente posible.

  Basándonos en su declaración por escrito y tras la investigación que realicemos sobre el fraude cometido con su Tarjeta Corporate, se dará carácter definitivo a la indemnización, cosa de la cual le informaremos siempre por escrito.

5. Glosario

A

Anti-spyware
El anti-spyware es uno de los elementos con los que puede usted proteger su ordenador. Se trata de software que evita que se instalen en su ordenador programas que usted no ha solicitado y que podrían divulgar sus datos personales.

Aplicación ING Commercial Card
La aplicación ING Commercial Card es la aplicación oficial para su Tarjeta Corporate. Con ella podrá consultar sus transacciones con un máximo de 12 meses de antigüedad. La puede encontrar en las tiendas Apple App Store o en Google Play (Android). Busque en ellas «Aplicación ING Commercial Card».

Ataque DDoS
El ataque DDoS consiste en sobrecargar una página web con un flujo masivo de datos. Ese flujo de datos no deseado se detiene con el cortafuegos, pero llega un momento en que es tan intenso que el cortafuegos, en su labor de detenerlo, tampoco deja acceder a los visitantes de buena fe. ING dispone de un alto nivel de medidas de seguridad diseñadas para diferenciar el flujo de datos no deseado del flujo de datos de buena fe.

B

Bloqueo preventivo
ING toma inmediatamente medidas de protección del flujo de pagos cuando detecta alguna situación sospechosa. En ese marco podemos bloquear su Tarjeta Corporate de forma preventiva para protegerla, por ejemplo, si sospechamos que se ha robado información de su Tarjeta Corporate mediante skimming. En ese caso bloqueamos su tarjeta de crédito y nos ponemos en contacto con usted de inmediato.

Botnet
Una botnet es una red de numerosos ordenadores infectados con un troyano o con un virus. De esa manera el ordenador se convierte en una especie de robot que realiza tareas de forma autónoma y automática. Los ordenadores infectados se pueden encontrar en cualquier lugar. También el suyo puede formar parte de esa red. Con este sistema los delincuentes pueden dar una misma orden a todos esos ordenadores a la vez. Los ordenadores se utilizan, por ejemplo, para enviar e-mails de phishing. O para interceptar los datos de su Tarjeta Corporate.

C

Chip EMV
El chip EMV es desde hace unos años el chip instalado en su Tarjeta Corporate. Con él puede usted, por ejemplo, pagar con su Tarjeta Corporate en tiendas introduciendo una clave personal. El chip EMV es un estándar internacional que se aplica en todo el mundo. Este chip reduce el fraude crediticio en las tiendas. Con este sistema ya no hace falta pasar la tarjeta por un lector de bandas magnéticas sino que se introduce en la ranura de la terminal de pago, la cual lee el chip.

Código de acceso
En el ordenador, en el teléfono y en la tableta puede usted programar un código para que no pueda acceder a ellos ninguna otra persona que no sea usted.

Contraseña
La banca por Internet debe estar bien protegida con una contraseña fuerte. La contraseña será fuerte si es imposible adivinarla y es difícil de krakear. Por ello es recomendable que cree una contraseña fuerte para todos sus entornos online.

Cookie
Una cookie es un pequeño archivo que una determinada página web instala en su ordenador. De esa manera dicha página web guarda sus preferencias de navegación. Muchas tiendas online utilizan cookies con las que guardan sus datos, los cuales no necesitará usted introducir de nuevo en sucesivas visitas.

CVC
CVC significa Código de Verificación de la Tarjeta. Se trata de un código de seguridad de 3 cifras que figura en el reverso de su Tarjeta Corporate, a la derecha del espacio reservado para la firma. Ese código se le puede solicitar cuando vaya a realizar un pago por Internet con su Tarjeta Corporate.

D

Delincuencia cibernética
La delincuencia cibernética es aquella que se comete por Internet. Consiste, entre otras cosas, en el envío por parte de los delincuentes de e-mails en los que le piden sus datos de acceso a páginas web y/o los datos de sus tarjetas de crédito (phishing) y en la creación de páginas web que se asemejan asombrosamente a las de ING. Esos delincuentes también intentan sacar sus datos personales de su ordenador mediante virus enviados junto a otro programa (los llamados troyanos).

Detección
La detección es la localización de actuaciones sospechosas. ING tiene un equipo de expertos que se ocupan diariamente de la seguridad de los pagos. Analizamos los pagos continuamente para detectar las transacciones y las actuaciones sospechosas y entramos en acción cuando es necesario. ING colabora estrechamente con la policía, con el Gobierno y con otros terceros, tanto a nivel nacional como internacional. De esa manera podemos informarle a usted de la forma más rápida y adecuada posible.

Delincuente cibernético
Los delincuentes cibernéticos son aquellos que delinquen en Internet. Su modus operandi consiste en enviar e-mails en los que solicitan al destinatario sus datos de acceso a páginas web y/o los datos de sus tarjetas de crédito (phishing). También crean páginas web que se asemejan extraordinariamente a las páginas de ING. Esos delincuentes también intentan sacar sus datos personales de su ordenador mediante un virus que le envían junto a otro programa (los llamados troyanos).

E

El portal ING Commercial Card
Con el portal ING Commercial Card puede consultar en soporte digital las operaciones de su Tarjeta Corporate con una antigüedad de 12 meses como máximo. Con ella puede descargar los extractos que desee y guardarlos en su equipo. De esa manera no necesitará archivar extractos en papel.

Escáner de virus
Un escáner de virus es uno de los elementos con los que puede proteger su ordenador. Este software comprueba si su ordenador contiene virus y los elimina.

Experto en seguridad
En ING tenemos un equipo de expertos en seguridad, que analizan continuamente las transacciones y las operaciones sospechosas. Y entramos en acción cuando es necesario. ING colabora estrechamente con la policía, el Gobierno y otras entidades como la Asociación Neerlandesa de la Banca.

Extensión
Una extensión es una aplicación adicional para su navegador que puede descargar usted mismo. Con ella puede añadir nuevas funciones a su navegador. Ejemplos de extensión son Adobe Reader, para leer archivos PDF, y Flash, para ver vídeos de YouTube.

F

Firewall (Cortafuegos)
Un cortafuegos es uno de los elementos con los que puede proteger su ordenador. Se trata de software con el que se impide el acceso a su ordenador a personas no autorizadas cuando está conectado a Internet o a cualquier otra red de ordenadores. El cortafuegos controla el tráfico de entrada y de salida de Internet y le avisa cuando detecta un intercambio de datos sospechosos.

Fraude
Usted puede ser víctima de diferentes modalidades de fraude. Este folleto es para informarle al respecto.

Fraude de identidad
El fraude de identidad consiste en la recopilación de sus datos personales y financieros para cometer actos delictivos con ellos. Determinadas conductas ya muy comunes, tales como tirar descuidadamente información financiera, extractos de la Tarjeta Corporate, la firma o una copia del documento de identidad pueden ayudar a la comisión de fraudes. Pero los delincuentes también adquieren datos personales, mediante el phishing y la ingeniería social, con los cuales pueden solicitar tarjetas de crédito en su nombre.

G

Gusano
Los gusanos se caracterizan porque se distribuyen autónomamente por las redes. Los gusanos se mueven automáticamente, como en una reacción en cadena. Por lo general se desplazan aprovechando las direcciones de e-mail que encuentran en los ordenadores que van infectando.

H

Hombre de paja
Véase «Mula»

I

Ingeniería social
Con la ingeniería social, los delincuentes intentan sonsacarle información confidencial, recurriendo malintencionadamente a determinadas características de las personas, tales como la curiosidad, la confianza, la codicia, el miedo y la ignorancia o el desconocimiento. La ingeniería social adopta numerosas formas. Desde páginas web falsas hasta phishing mediante e-mails y desde conversaciones telefónicas hasta visitas casa por casa. Los delincuentes le inducen a realizar determinadas acciones tales como proporcionar datos personales, códigos de seguridad o datos de sus tarjetas de crédito, pulsar una determinada tecla o instalar malware.

J

Jailbreak
El jailbreak es la eliminación de las medidas de seguridad del sistema operativo de dispositivos tales como el iPhone, el iPod touch o el iPad. Haciendo jailbreak en su dispositivo, el usuario puede, por ejemplo, instalar aplicaciones que no han recibido el visto bueno de Apple. De esa manera el dispositivo en cuestión puede quedar expuesto a los ataques de virus y de malware.

M

Malware
El malware es el término colectivo para designar el software malicioso y/o dañino. Es una abreviatura del inglés «malicious software» (software malicioso). El malware está diseñado para infiltrarse en un ordenador sin que su propietario lo sepa. El malware se puede introducir en su ordenador en un e-mail o junto a imágenes descargadas de páginas web, por ejemplo.

MasterCard ID check
Véase el capítulo «¿Qué medidas preventivas toma ING?»

Money mule
Véase «Mula»

Mula
Una mula pone su cuenta bancaria a disposición de los delincuentes para realizar actividades delictivas. Los delincuentes ingresan dinero en la cuenta en cuestión y, a continuación, lo transfieren a otras cuentas bancarias o lo sacan en efectivo. De esa manera ocultan dinero robado a los ojos la policía y de la justicia.

N

Navegador
Un navegador es un programa informático con el que puede visitar páginas web. Los navegadores más conocidos son Internet Explorer, Chrome, Firefox y Safari

NCSC
Nationaal Cyber Security Centrum. Órgano de cooperación entre gobiernos y empresas. Misión: El NCSC contribuye a incrementar conjuntamente la capacidad de defensa de la sociedad holandesa en el dominio digital y, de esa manera, a crear una sociedad de la información segura, abierta y estable, proporcionando una mejor comprensión del sistema y ofreciendo perspectiva de actuación.

P

Phishing
Phishing es la actividad de «pesca» de sus datos personales por parte de los delincuentes, y tiene un solo objetivo: Obtener información sobre su Tarjeta Corporate para realizar transacciones ilícitas con ella. Se suele hacer por e-mail, por teléfono o en páginas web. Una de las maneras de hacerlo es pidiéndole que pulse en un enlace de un e-mail falso, que se parece extraordinariamente a los de ING. Sin darse usted cuenta entra en una página web falsa y proporciona los datos de su Tarjeta Corporate. Sin que usted se entere, los delincuentes realizan transacciones con su Tarjeta Corporate.

R

Ransomware
El ransomware es un método de chantaje mediante malware. El ransomware es un programa con el que le bloquean el ordenador y, a continuación, le piden dinero para «liberarlo». Sin embargo, los pagos (con su Tarjeta Corporate, por ejemplo) no sirven para «liberar» su ordenador, porque a los delincuentes solo les interesa su dinero.

Ranura protegida
Una ranura protegida es una pieza que se coloca en la ranura de inserción de tarjetas del cajero automático. Así los delincuentes no pueden colocar un lector de tarjetas para copiar los datos de las tarjetas de crédito. La copia de datos de las tarjetas de crédito se denomina skimming. La ranura protegida puede ser de diferentes formas, según el cajero automático del que se trate. En la pantalla del cajero automático se muestra el modelo correcto.

Root
El root es la eliminación de las medidas de seguridad del sistema operativo de los teléfonos y tabletas Android. Haciendo root en su dispositivo, el usuario puede, por ejemplo, instalar aplicaciones que no han recibido el visto bueno del Mercado Android. De esa manera el dispositivo en cuestión puede quedar expuesto a los ataques de virus y de malware.

S

Servicio de Alerta de Seguridad
Véase el capítulo «¿Qué medidas preventivas toma ING?»

Sistema operativo
Los ordenadores, las tabletas y los teléfonos inteligentes solo pueden funcionar adecuadamente si tienen instalado determinado software. El software programado para que esos dispositivos funcionen adecuadamente se denomina sistema operativo.

Skimming
El skimming consiste en copiar los datos de su Tarjeta Corporate mediante un lector de tarjetas que se coloca en la ranura de los cajeros automáticos o de las terminales de pago en establecimientos. Con este método los delincuentes acceden a su clave personal y a sus datos, con los cuales sacan dinero de su cuenta. ING intenta evitar que los delincuentes puedan leer las tarjetas mediante la colocación de ranuras para las tarjetas con protección especial en sus cajeros automáticos. Además, animan a los propietarios de las tiendas a que comprueben regularmente que no se hayan manipulado sus terminales de pago.

Smishing
Smishing es phishing por SMS. Véase «Phishing»

Software antivirus
Véase «Escáner antivirus»

Spyware
El spyware es software que se instala en su ordenador (de forma inadvertida). Con él se pueden recopilar datos sobre el usuario y enviarlos a terceras personas.

T

El truco del billete de 10 euros
Con este truco el delincuente intenta distraer al usuario cuando está sacando dinero del cajero, tirando un billete al suelo. Te avisan de que se te ha caído y, mientras tanto, te roban el dinero del cajero.

Troyano (o caballo de Troya)
El término «troyano» viene del famoso caballo de Troya. Un troyano es un programa que se instala sin que usted se dé cuenta en su ordenador «disfrazado» de archivo inofensivo. Con él, el delincuente puede acceder a su ordenador a distancia. Sin que usted se entere. Con un troyano se puede averiguar el nombre de usuario y la contraseña de su portal ING Commercial Card, por ejemplo.

V

Virus
Un virus es una variedad de software dañino. Los virus pueden producir graves daños en su ordenador, borrando información (confidencial). Con ellos los delincuentes también pueden entrar en su ordenador y averiguar su nombre de usuario y su contraseña.

Virus informático
Véase «Virus»

W

WiFi
WiFi es la abreviatura inglesa para indicar una red inalámbrica. Mediante la red inalámbrica puede usted conectarse a Internet.

6. Teléfonos importantes

Si constata o sospecha la existencia de cualquier fraude, puede ponerse en contacto con nosotros 24 horas al día, 7 días a la semana, llamando al teléfono

+31 (0)10 428 95 81

o mediante nuestros números de acceso locales. Esos números los puede consultar en:

www.ingwb.com/cardcontact

¡No lo dude, estamos a su pronto servicio!

ING