Sabadell
Consumer

Nos tomamos muy en serio la seguridad de tus productos.

Nuestro compromiso es que puedas operar y hacer tus gestiones con toda la tranquilidad del mundo.

Sabadell Consumer

Para poder garantizar tu seguridad, tomamos una serie de medidas efectivas.
¡Sigue leyendo!

Medidas para la prevención del fraude

Sabadell Consumer aplica distintos límites de importes por operación como mecanismo de prevención del fraude. Por ejemplo, siempre solicitaremos el PIN de tu tarjeta Contactless para tus pagos superiores a 20 €. O si quieres retirar efectivo mediante alguna de nuestras tarjetas debes saber que el límite diario permitido es de 300 €. **En caso de que detectemos determinados patrones u operaciones fuera de lo común, nos pondremos en contacto contigo.**

Compras online y e-commerce

Los e-commerce son uno de los sitios en los que los usuarios confían sus datos bancarios, por lo que no es casual que los ciberdelincuentes hayan puesto sus ojos en este canal.

Las estafas mediante los e-commerce pueden tener dos objetivos: o bien robar los datos bancarios del usuario o bien robar el dinero que el cliente está dispuesto a pagar por un producto que, finalmente, no recibirá.

Sabadell Consumer

Los pilares para una seguridad de primera

¡Sigue estos consejos!

Está bien tener nociones de ciberseguridad, pero muchas veces **garantizar la máxima seguridad de los datos bancarios** depende de uno mismo.

Te explicamos algunas de las buenas prácticas que puedes aplicar desde hoy para **proteger mejor tus y tarjetas**.

Consejos para la gestión de contraseñas

- **Cambia periódicamente tus contraseñas**, tanto el PIN de tus tarjetas. Y mejor aún: diversifícalas, de tal modo que utilices una contraseña para cada una de tus cuentas.
- **Guarda en un lugar seguro tus contraseñas**, donde nadie más que tú pueda verlas o acceder a ellas. Por ejemplo, no apuntes nunca tus credenciales en un post-it y lo dejes en el monitor a la vista de todo el mundo. Lo mejor que puedes hacer es, simplemente, no apuntarlas en ningún lugar físico, así no estarán expuestas a nadie. Existen programas de gestión de contraseñas para no tener que memorizarlas. Es muy importante que la contraseña que uses para proteger este gestor sea difícil de adivinar, lo suficientemente robusta y la cambies si sospechas que puede haber sido comprometida.
- **No confíes datos de acceso a nadie**, ni por teléfono, ni por correo electrónico. Sabadell Consumer jamás te pedirá esta información. Asegúrate siempre que estás en la página que quieres estar. Fíjate en la dirección que empezará por https y mostrará un candado. Cuando hagas clic sobre el candado, comprueba que la dirección está bien escrita. Tampoco compartas tus contraseñas con nadie, por mucha confianza que tengas, para no favorecer la filtración de las mismas.
- **No uses contraseñas predecibles o relacionadas con los datos personales.**
- El tamaño importa, así que **genera contraseñas con un mínimo de 8 dígitos de longitud.**

Consejos para vigilar de cerca tu seguridad

- **Utiliza siempre el correo de modo seguro**. Desconfía de aquellos correos que provengan de sitios desconocidos o que contengan información incoherente. Desconfía de cualquier email o mensaje que te pida introducir datos, más aún si proviene de direcciones desconocidas o nos lleva a links o archivos adjuntos. Otra pista para sospechar de emails o mensajes de origen desconocido es que normalmente están

plagados de faltas de ortografía o incoherencias gramaticales. No cedas tus credenciales ni datos personales a través del correo.

- En la medida de lo posible, **no introduzcas contraseñas ni inicies sesión de tu banca online en ordenadores públicos.**
- **Evita proporcionar datos** relativos a cuentas o acceso a terceros.
- Cada vez que inicies sesión en la web de Sabadell Consumer, **recuerda desconectar la sesión**. Así no se lo pondrás fácil al siguiente que utilice el ordenador. Sobre todo, no le pidas a tu navegador habitual que almacene tu contraseña.

Consejos de seguridad en dispositivos

- Ten **actualizado el sistema operativo** y las apps de tu móvil.
- **No instales apps de orígenes desconocidos**. Te recomendamos descargar las apps de sitios oficiales y certificados, como Google Play Store o App Store.
- **Instala antivirus**, tanto en tu ordenador como en tu móvil.
- **Activa el firewall o cortafuegos** para controlar las comunicaciones de red.
- **Realiza copias de seguridad** periódicamente. Así protegerás mejor tus bases de datos de contraseñas y los tendrás almacenados previamente en caso de riesgos.
- **Protege tu móvil**. Como sabes, los móviles cada vez tienen más diversidad de opciones de bloqueo, como la huella digital, los patrones de contraseña, el reconocimiento facial o Face ID en caso de iPhone...

Consejos para tus compras online

- **Desconfía de aquellos e-commerce en los que se vendan productos muy por debajo de su precio de mercado**. El principal cebo que usan los ciberdelincuentes para llamar la atención es la publicación de ofertas ridículas, imposibles para un e-commerce convencional. Por ejemplo, si encuentras esa cámara de 2.000 € que tanto tiempo llevas buscando con un precio de venta de 400 € no caigas.
- Comprueba que el e-commerce en el que quieras comprar algo disponga de un teléfono y una dirección postal al que puedas recurrir en caso de problemas.
- **No te fíes de los e-commerce con el 100% de opiniones positivas** ni de aquellos en los que no encontremos información en el resto de la red.

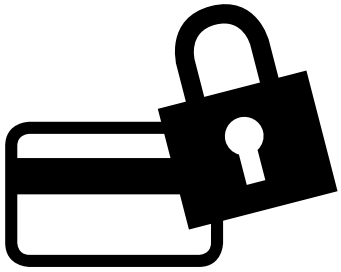
- Tener tu **antivirus actualizado** es muy importante también para tus compras online, tanto para tu ordenador como para tu móvil.
- También en los portales e-commerce es muy importante que aparezca el **icono del candado de seguridad en la barra de navegación**. Haz clic sobre el candado y asegúrate de que la dirección esté bien escrita. Y, si puedes buscar información en Internet sobre el e-commerce en el que quieres comprar algo, mejor, porque estarás prestando atención a la opinión de otros usuarios.
- **Desactiva tu tarjeta para los pagos por Internet**. Es una forma de maximizar tu seguridad, porque de esta manera tú decides cuándo se hacen las compras por Internet y nadie podrá usar tu tarjeta para los pagos online suplantando tu identidad.

Sabadell
Consumer

Glosario de seguridad

Descubre los términos básicos de ciberseguridad que pueden ser de tu interés

Consulta en este glosario los conceptos de ciberseguridad que deberías conocer para proteger mejor tus cuentas ante posibles ataques.



Phishing

Es la forma de ciberataque más usada por su simplicidad técnica y funcional. Consiste en robar datos confidenciales del usuario creando un pretexto para que se los proporcione.

Malware

Es un tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil, con la finalidad genérica de perjudicar al usuario y si se trata de un malware bancario sustraer información confidencial como contraseñas, robar dinero o comprometer la seguridad de las cuentas bancarias.

Ingeniería social

Es uno de los métodos más utilizados por los ciberdelincuentes para obtener datos confidenciales sobre los usuarios. Se basa en la manipulación psicológica: los ciberdelincuentes usan métodos de ingeniería social para conseguir información, realizar fraudes u obtener acceso ilegítimo a los espacios confidenciales de los usuarios.Firewall o cortafuegos

Es un elemento de seguridad en la red que decide si debe permitir o bloquear un tráfico específico. Los firewalls establecen una barrera entre las redes internas, que son fiables y seguras, y las redes externas poco fiables como Internet.

Antivirus

Son programas informáticos encargados de detectar a los malwares o a los softwares potencialmente dañinos.

Autenticación de doble factor

Al entrar en un móvil, programa o web, la autenticación de doble factor hace que se necesite un código para acceder al servicio requerido, aparte de la contraseña. Suele ser un código que se recibe en el móvil. Es especialmente útil en la lucha contra la ciberdelincuencia, ya que la autenticación de doble factor deja sin utilidad que un ciberdelincuente conozca las contraseñas de los usuarios, ya que nunca podrán acceder a ese segundo código necesario para completar la operativa que quieran hacer. Además, con la llegada del mensaje de doble autenticación al móvil, el usuario se percata de que alguien está intentando acceder a alguna operativa por él. Otra característica es que es un "código" que es efímero, de un solo uso, y que se recibe en un dispositivo que solo el cliente debe tener.

Gestor de contraseñas

Es una app dedicada a almacenar contraseñas en una base de datos cifrada, la cual está protegida por una contraseña maestra. Los gestores suelen generar contraseñas fuertes, con una longitud suficiente y combinando letras, números y caracteres extraños para crear palabras sin sentido y así aumentar su fortaleza. Esto permite esquivar los ataques y el uso de patrones predecibles.

Sabadell Consumer

AYUDA URGENTE SABADELL CONSUMER

Podemos ayudarte si crees que la seguridad de tus tarjetas se ha visto comprometida o para otras gestiones:

- **Me han robado una tarjeta**
  Bloquea tus tarjetas para inutilizar las que te han robado o has perdido
- **Me han robado datos de mi tarjeta**
  Si los ciberdelicuentes te han robado o han intentado robarte información de tus tarjetas.
- **Quiero aumentar el límite de mi tarjeta**, bloquear las compras online o bloquear compras en el extranjero.

Puedes contactarnos de lunes a viernes

de 9 a 14:30 y de 15:30 a 19h a través del teléfono 93 400 43 02.

Sabadell Consumer

Certificado de seguridad

(Información en inglés)

1 > ABOUT THIS DOCUMENT

1.1 Date of Last Update

This is version 1.0, published 2020/09/09.

1.2 Distribution List for Notifications

Notifications of updates to this document are submitted to internal staff members of Grupo Banco Sabadell.

1.3 Locations where this Document May Be Found

The most updated and current version of this document is available on the Grupo Banco Sabadell web site:

URL Banc Sabadell.

Please ensure you are using the latest version of the document.

1.4 Authenticating this Document

This document has been signed using the Grupo Banco Sabadell PGP key. The signatures are also on our Web site PGP Signature: URL Sabadell Consumer.

2 > CONTACT INFORMATION

2.1 Name of the Team

Grupo Banco Sabadell CERT: Grupo Banco Sabadell Computer Emergency Response Team.

2.2 Address

Grupo Banco Sabadell, Avenida Óscar Esplá, 37, 03007 Alicante, Spain

2.3 Time Zone

Central European Time - CET (GMT+0100, and GMT+0200 from April to October).

2.4 Telephone Number

None available.

2.5 Facsimile Number

None available.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

cert@bancsabadell.com.

2.8 Public Keys and Other Encryption Information

Please encrypt any sensitive e-mails with the Grupo Banco Sabadell CERT PGP key and send it to: cert@bancsabadell.com.

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: Encryption Desktop 10.3.1 (Build 13100)

mQENBFv1ZPsBCAC7ZPFKqDgw+PToDx4y5CfcX8WGDoRHSutZFPhk4tCGfDvchtIo
l5LYkph7UK/ywtF7NbL1zR1t1N+9pRlAf1cEhEtLXeiO8XPoSrCuB+IjqWMCkq7e

/J/otrOOWH4qtOov8qkIIW5DUsY78HCwHt+wWQ6Yn27ju87kiah3pS4+rb5SGcam
zLdlZtfcdcHtyXXnMczk8HwG6zQRn7m7VmsEy2Pt48FWC46lDVN6mcPCQ85k13py
PBSVybimiV4djhYBgxraIWU4CmmUuy25MAVtCHMjXNGv4ZCGlKkB3NHux0qVuAhn
khj2eAQdWKriZqDfRjmnsK0TPj4yyJm2xU5jABEBAAG0MUNFUlQgR3J1cG8gQmFu
Y28gU2FiYWRlbGwgPGNlcnRAYmFuY3NhYmFkZWxsLmNvbT6JAW4EEAECAFgFAlv1
ZPswFIAAAAAAIAAHcHJlZmVycmVkLWVtYWlsLWVuY29kaW5nQHBncC5jb21wZ3Bt
aW1lBgsJCAcCAQIZAQUbAwAAAAUWAAMCAQUeAQAAAAQVCggJAAoJEBHm6XX0H0Sv
E5oIAJkLxYpuTLF3rCd9xTQdWg/KfK8t1bvhvMTjTC2KqTQDTfc0wMzB6pkweUHd
DI3p8a8gApMvFFnlXdz7huGzi3z9hXMDfFgow9Od0Y1xm7a9fOy3Rx3Yg70BRDcx
uSe+D2OoIsZkAD3MBPk9GmRL3PrWb+kOeddDuQI16u+l02rKcQnp2Kxtu+eZy0zm
E7nZJAwQR19LuuxkorXRrwbckUCafAIZlclK2XgHfqp2bo3+5MbWdDSfSnwu4wfw
l7SY0dLN3rzS5eVErJ+YiJphNAg/38yi4CZNN3yWxjykIFIch0qu0kosDVbIjQg/
jjF2N03fhei4LONVTSxGZFhhMTa5AQ0EW/Vk+wEIANw5Ap083/F8WtcfyCes2dgK
x3MN4EgoR4a2U/XzQ/mKKl8pJpoDoCr96iVcifoswpE5qyzP43pDFDdOl3rwh5MH
TcDvy49/AEaNbaRjAbAeVvw+BvY0+xwhDBQDbt0KzO+TqYHB+fzUi0H+CZ2nZdx6
TTbDBqpe1xwHPJILlUUrC525R/fyvrdZG/xzTzXB+BTNf99fUnTEVea5bYGf6JTJ
p6U11cOfSKLupJbRkhLOoFLLPaEMdPcj7ho5FwDokKPBtibQ8bVL3RI23CeZvA4S
tXeFxIwSsA9cABOWDlt1QHe4nsZ+QvDOh/yzT/ERiy51yQ+5TpsmoVEhTD22MrMA
EQEAAYkCQQQYAQIBKwUCW/Vk/AUbDAAAAMBdIAQZAQgABgUCW/Vk+wAKCRDc7+D7
snxEW5A4B/4n9o67E9Y+h1XrhEjtFl92E4nSIwKXqZrloJqMaBslMlq+H4rynml7
qWDT/UBjcsgG3uaUDckyU6u+oiCr8lZj17AloK9oThp+hHL/J9crLmCjGRChNyWS
uVcGy1LHb1+ApKlMgjdtV3xSPkXMPY0pDO4IMnHxA+nJSDPdG7t3qeVuGVVbJvIN
PDDhhDuDU/Xo9BGvOsMRhbrV9OZLaa3lJxxhNiPL62P1palZHYulPFhACV1G9ngz
Lng/2XirKFdqn/q3NGh7GSJ1P5OvhBM5BiSWRXMVwimuSnnvTZ6eiZR84pPcBdb3
Yhm/Q1CiioWHD8JCCJ27abbpJU/aZ9aRAAoJEBHm6XX0H0SvKLQIALkIskHIlAKk
75mWHPZk6oSdRTvmwmtb/33m0ir0ZSG5GbqYiL8QUGoiXg91tiN9dwcRcSGvxm25
Ey3YIpkVGtBLTvTpa06+i3VfXdjm/lap5VSyLgMdb4zsU7+23m6RoxsArktHy2Ph
EPNgCmf9lgs4XZN5g5jnt//0Ksb3P6S7J5u5ImMM+ZFgwzxuro4IdPNFKY6uOUDS
jifyVLbEsk5ukLIq7ma9NTyexbKnGVGQzBDU/3tXziimYn3t4U1BeiZzbVV2USMo
ThgjzWvFSET2L9T1uTN/8QUl4YUhQXwBr5soxmWpNhcfegLn4vyTeT/9cI1xrrHG nAiFzOXjl68= =rTLm

-----END PGP PUBLIC KEY BLOCK-----

2.9 Team Members

No public information is provided about the Sabadell Banc CERT team members.

2.10 Other Information

None available.

2.11 Points of Customer Contact

The preferred method for contacting the Grupo Banco Sabadell CERT is via e-mail.

For general inquiries, please send an e-mail to cert@bancsabadell.com

3 > CHARTER

3.1 Mission Statement

The purpose of the Grupo Banco Sabadell CERT is to provide a Response capability, formed by an Incident Handling team. CSIRT core services are responsible for monitoring, receiving, reviewing, validating, notifying and responding (takedown services) to security alerts.

3.2 Constituency

Grupo Banco Sabadell CERT supports incident response and security services for Banc Sabadell Group, their customers and related organizations.

3.3 Sponsorship and/or Affiliation

Grupo Banco Sabadell CERT is sponsored by Banco de Sabadell, S.A.

3.4 Authority

Grupo Banco Sabadell CERT operates under the auspices of, and with authority delegated by the IT Control Department of Banco de Sabadell, S.A.

4 > POLICIES

4.1 Types of Incidents and Level of Support

Grupo Banco Sabadell CERT is authorized to address all types of computer security incidents that occur at its constituency.

All incident reports received by Grupo Banco Sabadell CERT are analyzed, classified and prioritized according to an internal incident classification policy so that an efficient and appropriate level of service is provided.

Resources will be assigned according to the following priorities:

- Threats to the physical safety of human beings.
- Root or system-level attacks on any Management Information System or any part of the backbone network infrastructure.
- Root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose.
- Compromise of restricted confidential service accounts or software installations, in particular those used for MIS applications containing confidential data, or those used for system administration.
- Denial of service attacks on any of the above three items.
  Any of the above at other sites, originating from the constituency of Grupo Banco Sabadell CERT.
- Large-scale attacks of any kind.
- Threats, harassment, and other criminal offenses involving individual user accounts.
- Compromise of individual user accounts on multi-user systems.
- Compromise of desktop systems.
- Forgery and misrepresentation, and other security-related violations of local rules and regulations.
- Denial of service on individual user accounts.

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. In most cases, Grupo Banco Sabadell CERT will provide pointers to the information needed to implement appropriate measures.

Grupo Banco Sabadell CERT is committed to keeping the constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

Grupo Banco Sabadell CERT will cooperate with other organizations in the field of computer security. This cooperation also includes and often requires the exchange of information regarding security incidents and vulnerabilities. Nevertheless Grupo Banco Sabadell CERT will protect the privacy of its constituency and therefore (under normal circumstances) pass on information in an anonymized way only.

Grupo Banco Sabadell CERT will only provide information to other parties with the sole purpose of facilitating the tasks of containment, eradication and recovery of incidents under the general principle of providing the minimum information possible.

Grupo Banco Sabadell CERT operates under the restrictions imposed by the law of Spanish Data

Protection Authority. Therefore it is also possible that Grupo Banco Sabadell CERT may be forced to disclose information due to a Court's order.

4.3 Communication and Authentication

In view of the types of information that the Grupo Banco Sabadell CERT will likely be dealing with, telephones will be considered sufficiently secure to be used even if unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to the Grupo Banco Sabadell CERT, or before disclosing confidential information, the identity of the other party will be ascertained to a reasonable degree of trust. Within Community, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc., along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

5 > SERVICES

5.1 Incident Response

Grupo Banco Sabadell CERT will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

Incident triage activities include:

- > Report assessment - Interpretation of incoming incident reports, their prioritization and relation to ongoing incidents and trends.
- > Verification - Support in determining whether an incident has really occurred and its scope.

5.1.2 Incident Coordination

Incident Coordination activities include:

- > Information categorization - Categorization of incident related information (logfiles, contact information, etc.) with respect to the information disclosure policy.
- > Coordination - Notification of involved parties on a need-to-know basis, as per the information disclosure policy.

5.1.3 Incident Resolution

Incident resolution activities include:

> Technical Assistance - This may include analysis of compromised systems.
> Eradication - Elimination of the cause of a security incident and its effects.
> Recovery - Support in restoring affected systems and services to their status before the security incident.

In addition, Grupo Banco Sabadell CERT will collect statistics concerning incidents that occur within or involve the community, and will notify the community as necessary to assist it in protecting against known attacks.

5.2 Proactive Activities

Grupo Banco Sabadell CERT will take part in proactive services with the objective to reduce the number of actual incidents by providing proper and suitable information concerning potential incidents to the constituency. Grupo Banco Sabadell CERT will perform proactive activities to improve performance and capabilities, such as:

- Information services.
- Training and simulation activities.
- Forensics and malware analysis.
- Cyber Intelligence coordination and contextualization.
- Threat hunting.

6 > INCIDENT REPORTING FORMS

All incidents will be reported via email using cert@bancsabadell.com.

7 > DISCLAIMER

While every precaution will be taken in the preparation of information, notifications and alerts, Grupo Banco Sabadell CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.