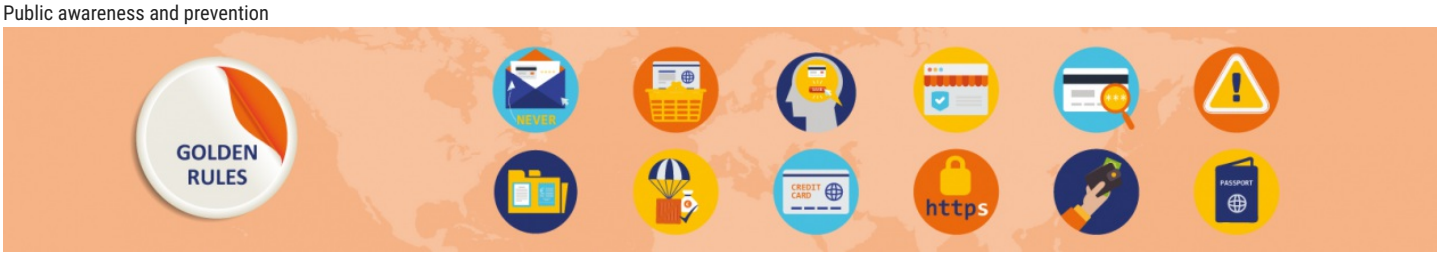
E-COMMERCE: TIPS AND ADVICE TO AVOID BECOMING A FRAUD VICTIM

Public awareness and prevention



Safe sales, safe revenue

ONLINE SHOPPING

'Online shopping' refers to purchases made either on a computer or on a smart phone/tablet. You can shop online with or without full authentication.

Using a card is a safe method of payment in online shopping as long as you exercise the same care as in other shopping.

Before Placing An Order

- Carefully read the terms and conditions, including the small print. These terms and conditions should be available on the merchant's website.
- Check that the merchant's address details are available on the webpage and save or print them in case you need to return any items. If no address details are given, you should proceed with caution. Make a note of the URL address of the shop.
- Read what the merchant has to say about delivery costs, accepted currencies and applicable taxes.

When Making A Purchase

- Save or print the description and the terms and conditions which are displayed by the merchant and which you need to accept before you can place your order.
- Accept the payment by entering the number and expiry date of your card on the online form and follow the merchant's instructions. If the online store uses full authentication, you will then be transferred for instance to your online banking service for identification.
- Save or print the acknowledgement of your payment displayed by the merchant.
- Keep the saved or printed details in case they are needed later for checking or for comparison.

Most online stores send customers a confirmation by e-mail, save those messages!

Incorrect charge?

Common errors in online shopping are delivery of a wrong product or service, faulty/damaged product, and non-receipt of goods.

1. If you have problems with a product or delivery, always first contact the store where you made the purchase. Preferably use e-mail so that you have a record of your correspondence.
2. If you cannot resolve the matter with the merchant, contact your bank's customer service. They will give you further instructions, for example if you should file a report to the police.

Remember...

1. Save all the documents related to the purchase.
2. Your first action is always to contact the merchant to resolve the issue.
3. If you contend with your bank, attach a copy of your e-mail correspondence with the merchant.
4. If you return faulty or damaged goods, always do so by registered mail. Keep the receipt with the tracking number, as you may need it later.

I am a victim of online fraud. What should I do?

- Report it to your local or national police.

› Report it to your bank, if you paid the product with a credit or debit card. You may have some rights to get your money back.

GOLDEN RULES OF ONLINE SHOPPING

Download the Golden Rules (PDF)

Golden Rules - Safe Online Shopping (EN) **Other languages:** Austria - DE | Bulgaria - BG | Belgium - NL FR | Colombia - ES | Croatia - HR | Czech Republic - CS | Denmark - DA | Finland - FI | France - FR | Germany - DE | Greece - EL | Hungary - HU | Ireland - EN GD | Italy - IT | Lithuania - LT | Malta - MT EN | Netherlands - NL | Portugal - PT | Poland - PL | Romania - RO | Spain - ES | Sweden - SV | United Kingdom - EN | North Macedonia - MK | Norway - NO | United States - EN

Better safe than sorry:

Never send your card number, PIN or any other card information to anyone by e-mail.

If you are not buying anything, don't submit your card details. There are for example games and fake lotteries online which sole purpose is to get your credit card information.

Many e-merchant sites will ask to store your payment details. **Think twice before deciding** and make sure you understand the risks this might imply - such as the site becoming compromised by cybercriminals. Most well-known brands have a strong customer security policy.

Buy from trusted sources. Use brands and shops that you are familiar with or have used before and check the ratings of individual sellers on sites such as Amazon or EBay. For Internet purchases, make sure you use the internet security protocol called 3D Secure - Verified by Visa/SecureCode/SafeKey. Ask your bank or your card issuer about it.

Whenever possible, **do your online shopping at sites that use full authentication** (Verified by Visa / MasterCard Secure Code).

If the website does not support full authentication, **make sure the data transfer is appropriately protected.** Check that there is an icon of an unbroken key or locked lock at the bottom of your browser window and that in the address bar the URL begins with https:// instead of http://.

Don't send money to anyone you don't know. If someone approaches you online and asks for money, think whether you would give the same amount of money to an unknown person on the street.

When purchasing something online from another person, **don't send money upfront** to the seller. If possible, reserve the right to receive the goods first.

Use credit cards when purchasing things online. Most credit cards have a strong customer protection policy; if you don't get what you ordered, your bank can advise you in the refund process.

Before providing your card details to pay for **a continuous service over the internet** (such as virus protection software), find out how you can stop that service and the recurring charges related to it.

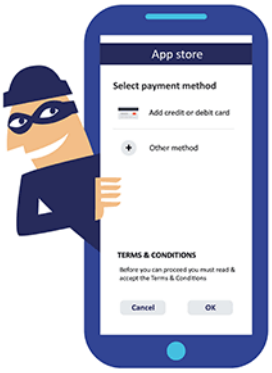
Always save all documents related to your online purchases. They may be needed to establish the terms and conditions of the sale or to prove that you have paid for the goods.

Some online shops outside of Europe may request a copy of your card and passport by fax in order to ensure that the order is being placed by the actual cardholder. Never send your card details in an unencrypted e-mail. If you do not supply these details, the shop will probably not ship your order.

A few extra tips...

1. Know your finances. When looking at your bank statement, you should be able to recognize every purchase made. Remember that it is also possible that a merchant has a different name on the outside of the shop than on the bank transaction. Report any strange activity to your bank.
2. Be very cautious of attractive offers and information you may find online or by e-mail. If it sounds too good to be true, it probably is.
3. Be wary of unsolicited e-mails. Don't open attachments or click on links they might contain, even if they appear to come from a trusted merchant, as they might be part of a phishing scam.

SAFETY TIPS FOR APPS



1. Read the Terms & Conditions of mobile apps before downloading them to your mobile device, especially if they ask you to register your credit card details.
2. Use prepaid-debit cards to register for recurring mobile app payments.
3. When giving your tablet to your kid, make sure that in-game purchases with your credit card are not possible without a PIN-code that only you know.

General online security tips:

Protect your PC, laptop, tablet and smartphone with strong passwords and with security programs such as antivirus/anti-spyware.

Only download files or software from trusted sources. If a pop-up window appears on your computer suggesting you should download something, do not click OK unless you understand what it is.

Use VPN-services when using public Wi-Fi. VPN (Virtual Private Network) will create an encrypted channel for your data. Without VPN, anyone can capture your identity information and credit card data, and read your emails.

Use HTTPS and SSL protocols when browsing over the internet. Look for the padlock symbol on the URL bar, especially when making an online payment. Reliable e-merchants usually use a secure protocol.

YOUR CREDIT CARD(S)

Only criminals will ask for your online banking credentials or card details by e-mail or phone. Neither your bank nor the law enforcement authorities will ever do so.

If you have disclosed your online banking credentials or card details to an unknown party, cancel the card and contact your bank immediately.

Your credit card is as valuable as your bank account. Take good care of it.

- Protect your cards as you would protect your cash.
- Don't store or write down your PIN code.
- Never reveal your PIN to anyone.
- Save the card blocking service contact number in your mobile phone.
- Sign you name on the reverse side of the card. A merchant is not obliged to accept payment using an unsigned card.
- Familiarize yourself with the general terms and conditions of your card. Regularly check that your card is where it should be.
- Always keep your card in your possession. Do not leave your card in a car, a restaurant table, a visible location in your office or hotel room, or anywhere else unsupervised.
- Set withdrawal and purchase limits on your card that meet your needs. These limits can be changed when necessary. Ask your bank if setting limits is possible with your card.
- Beware of pickpockets. Be especially alert when moving in a crowd. Never keep your card in a back pocket or in other easily accessible place.
- Expired cards should be cancelled by cutting them into several pieces so that the magnetic stripe and chip are destroyed.

When using a card to pay in a retail outlet:

- Always use your hand, wallet, or purse as a shield when entering your PIN.
- Check the total amount before accepting a payment with PIN or signature.
- Never lose sight (and if possible touch) of your card during payment transactions.
- Save transaction receipts of all your purchases at least until you receive your next credit card or account statement. They may help in investigating unclear transactions.

Check your online banking service regularly. Notify your bank immediately if you see payments or withdrawals that you have not made yourself.

Withdrawing money from an ATM:

- Stand close to the ATM. Always protect your PIN while inserting it.
- Assess the ATM. If you notice something suspicious at or around the terminal, do not use it. Contact the service provider; the phone number is always visible on the terminal itself.
- Be aware of others around you.
  - If somebody is watching you, choose a different ATM.
  - If you need to queue up to a terminal, do not open your purse or wallet while waiting. If you withdraw cash, put it away immediately after retrieving it from the machine.
- Important! Remember to take your card (and your cash from the ATM) before leaving.
- In case of loss: if the ATM doesn't return your card, report it to your bank.

READ MORE IN

LEARN MORE ABOUT PAYMENT CARD FRAUD PREVENTION

READ MORE ABOUT PAYMENT SECURITY

CRIME AREAS: Forgery of money and means of payment • Payment Fraud
TARGET GROUPS: General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES: European Cybercrime Center (EC3)

Source URL: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/e-commerce-tips-and-advice-to-avoid-becoming-fraud-victim