DIGFINLIT

Digital financial literacy for socioeconomic inclusion and equity (DigFinLit)
No. 2023-1-LT01-KA220-ADU-000151748

Co-funded by the European Union

"SAFE ONLINE SHOPPING: TIPS TO AVOID SCAMS"?

Case study based on story from media resources

Developed by the Socialinių inovacijų fondas (Lithuania)

Introduction

Online shopping has become an integral part of modern life, offering convenience, variety, and often better prices than traditional stores. However, the rise of online shopping has also led to an increase in fraudulent activities. Scammers are continually developing new ways to deceive consumers. In this case study, we will provide practical tips and best practices helping to shop online safely and avoid fraud. According to the Lithuanian State Consumer Rights Protection Authority (SCCPA), fraudulent e-shopping is an annual occurrence, but it is not always possible to get your money back - often such shops are registered outside Lithuania, so it is not easy to find the culprit.

Case analysis

A few years ago, Rimantas from Kaunas (the case described on www.lrt.lt) and other people looking for their phones were scammed by fraudsters. When Rimantas decided to buy a new phone, he found a price comparison platform on the internet, typed in the phone model he wanted and chose the Telemaxi option he found most attractive. In terms of price, there was not a big difference that would raise much suspicion.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and National Agency (NA). Neither the European Union nor the NA can be held responsible for them.

After finding the phone, the man called the e-shop and asked if the price included delivery. Everything seemed reliable to the Kaunas man - even the payment for the phone was made through Paysera, a Lithuanian financial technology company that provides electronic payment services worldwide. He received a reply that the payment had been made. According to the terms and conditions, the phone he bought should be delivered within 2-4 days.

The days passed, but he has never received a phone which he bought. He tried to call the e-shop, using the same number he had already used, but no one answered. The man contacted the company through which the payment was made. Again, there was an answer. Those sellers, Telemaxi, are no longer in contact with Paysera, the phones are switched off. They told him that it was no longer possible to make payments to Telemaxi through them, and suggested that he contact the police and describe the whole situation.

Shortly afterwards, he filed a police report. A few days later, articles appeared in the media about the Telemaxi shop, which was suspected of having defrauded a large number of customers of large sums. More than 240 individuals and companies were recognised as victims and the total damage caused was estimated at more than €70 000.

According to experts, scams are getting better. Recently, there have been complaints about a company that swindles people out of their money but remains unidentified - neither the bank nor the other payment operators can tell who the payment was made to. In such cases, it is very difficult to recover the money lost, so shoppers are urged to use only trusted and verified e-shops.

Proposed solutions and recommendations

To shop safely online, you should remain vigilant and follow these tips:

- Never click on links in unsolicited (SPAM/spam) emails or advertisements. If you wish to view an offer, please visit the online shop directly by typing the website address into your browser rather than clicking on links.
- Shop on the *platform's website,* not the app.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and National Agency (NA). Neither the European Union nor the NA can be held responsible for them.

- Pay attention to *the price of the item and its real market value.* Huge discounts can be a scam. Check the internet to see if anyone has posted about it. Offers to buy well-known brands at particularly good prices are tempting but have little credibility. At best, you will get a fake that bears little resemblance to the original product seen in the pictures in the offer. At worst, you will lose your money and not get any product. Of course, scammers can also hide behind adverts offering to buy the desired product at market price, so it is important to assess not only the offer, but also the seller who is trying to sell you the product.
- Pay attention to the product descriptions - make sure they are written in the correct language and that they are not a dummy website. To assess the *credibility of a website,* it is important to pay attention to the ending of the domain, as the real one may be shop.com, while a fake website uses variants such as shop.net, shop.xyz or shop.biz. The trustworthiness of the website is also indicated by the address https:// and the padlock icon next to the domain, which means that the information on the page is encrypted with a Secure Sockets Layer (SSL) certificate.
- If you decide to shop at an unfamiliar online *shop*, check what information the seller makes public about itself. Does the online shop disclose details about its company - name, registration number, address, other contact information. Check reviews about the company, try to contact the company using the contact details it provides. And do this before the transaction. Sometimes it is also worth checking how many employees the company has. Also look for customer reviews on websites that are not affiliated with the seller.
- Before you buy, make sure the seller has a return policy and how many different payment options they offer their customers. Usually, reputable e-shops try to offer at least several payment options. A seller who only provides his account number should raise suspicions.
- It is worth noting which *payment methods are offered* on the website. E-shops should use security systems marked with MasterCard SecureCode or Verified by VISA. For international payment methods, PayPal is one of the most secure, offering consumer protection and the possibility of a refund in the event of non-delivery. Fraudsters prefer payment methods such as

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and National Agency (NA). Neither the European Union nor the NA can be held responsible for them.

Western Union, Moneygram, Skrill and Bitcoin, as they are often untraceable and it is almost impossible to recover the money spent through these methods.

- If you intend to make a *payment* transaction or connect to the internet bank, it is recommended that you do not use a public WiFi network that is accessible to everyone (whether password protected or not). Choose a reliable, secured internet connection and use the mobile data you have.
- Avoid connecting to the online shop using *social networking accounts* or connecting the shop to other online accounts.
- Do not enter your payment details in your account. Also set up two-factor authentication to protect your account with more than just a password.
- Don't be tempted by offers that ask you to enter a reference code, especially on social networks supposedly offered by famous people.
- Use virtual, disposable credit cards for payments to avoid damage if your details are leaked. If you frequently shop online, it's best to have a separate card specifically for such payments. You can top it up with the right amount of money before you make a payment, and you can quickly and conveniently change other settings on the mobile banking app, such as deactivating and reactivating the card's ability to pay online. If you have a credit card, you can choose one - many of them offer purchase insurance.
- If you use the mobile app, turn on automatic notifications - you'll get real-time information about transactions made from your card account. This means that if a potentially unauthorised payment has been made, you'll know right away and can contact your bank immediately.
- Many sellers offer the possibility to create a buyer profile and save your personal data, including your card information. If possible, avoid leaving this data in each seller's information systems, and if you choose to do so, remember to whom you have given your information and what you have given it to, and protect your account only with a password you know, which is difficult to guess.
- Choose delivery to a post office rather than to your home.
- Exercise your rights as a consumer and report fraudulent sellers to the relevant authorities, including your bank.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and National Agency (NA). Neither the European Union nor the NA can be held responsible for them.

Self-reflection questions

These questions can serve as prompts for introspection and self-assessment, helping individuals gain insight into their financial habits, values, and aspirations.

1. What do I need to pay attention to in order to shop safely online?
2. Have you had a similar situation and how did you deal with it?
3. What else could have been done in the case described to avoid the deception?
4. What do you think are the advantages and disadvantages of online shopping?

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and National Agency (NA). Neither the European Union nor the NA can be held responsible for them.

Self-assessment questions

*Read each question carefully and select the best answer from the options provided.**

1. **For a safe shopping experience, it is recommended:**

   a) Clicking on links in SPAM/spam emails or advertisements.
   b) In-app shopping.
   c) Visit the online shop directly by entering the website address in your browser.
   d) Connect to the online shop using your social media accounts.

2. **What do you need to consider to assess the reliability of an e-commerce website:**

   a) What information the seller makes public about itself: does the online shop disclose details about its company - name, registration number, address, other contact information Investment fraud
   b) Does the seller have a return policy?
   c) Are there at least a few different payment methods on offer?
   d) Whether the e-shop uses an SSL certificate (the lock badge in the address bar).
   e) Whether the goods are described in the correct language, or whether it is a translation.
   f) All answers are correct.

3. **Is it important to pay attention to the price of the product and its real market value.**

   a) Yes
   b) No

4. **Which online payment methods are safe?**

   a) “MasterCard SecureCode“
   b) “Verified by VISA“
   c) ,,PayPal"
   d) All of the above.

5. **To keep your payments secure, it is recommended:**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and National Agency (NA). Neither the European Union nor the NA can be held responsible for them.

a) Do not use a public WiFi network that is accessible to everyone when accessing the Internet Bank.
b) Have a separate card specifically for online payments.
c) Use a credit card - many of them offer purchase insurance.
d) When using the mobile app, activate automatic notifications so you get real-time information about transactions made from your card account.

This multiple-choice test can help assess understanding financial journey and the lessons learned from his experiences.

* Correct answers

1.C 2.F 3.A 4.D 5.E

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and National Agency (NA). Neither the European Union nor the NA can be held responsible for them.

References

1. Lietuvos nacionalinis radijas ir televizija, 2024, “Netikėtai išpopuliarėjusi internetinė parduotuvė „Temu“ – proga pigiai apsipirkti ar piktavalių oazė?”; Available at: https://www.lrt.lt/naujienos/mokslas-ir-it/11/2177783/netiketai-ispopuliarejusi-internetine-parduotuve-temu-proga-pigiai-apsipirkti-ar-piktavaliu-oaze
2. Lietuvos nacionalinis radijas ir televizija, 2021, “Internetinei parduotuvei apgavus per 240 asmenų, vienas nukentėjusiųjų žinios dėl tyrimo nesulaukia trejus metus”; Available at: https://www.lrt.lt/naujienos/verslas/4/1534184/internetinei-parduotuvei-apgavus-per-240-asmenu-vienas-nukentejusiuju-zinios-del-tyrimo-nesulaukia-trejus-metus
3. Bankas “Citadelė”, 2020, “Apsipirkimas internetu ir internetiniai sukčiai: dažniausios pirkėjų klaidos”; Available at: https://www.cblgroup.com/lt/media/press-releases/2020/mistakes-when-shopping/
4. Delfi.lt, login.lt, 2022, “Saugus apsipirkimas internete: kaip atpažinti, ar svetainė nėra tik sukčių apgaulė?”, Available at: https://www.delfi.lt/login/technologijos/naujienos/saugus-apsipirkimas-internete-kaip-atpazinti-ar-svetaine-nera-tik-sukciu-apgaule-89493481

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and National Agency (NA). Neither the European Union nor the NA can be held responsible for them.