The holiday season brings a lot of joy, companionship and good wishes. In order for you to be safe and maintain a good mood during this time, we have prepared the most common traps and online scams and tips on how to protect yourself from them. Protect your and other people's personal data and enjoy this holiday season carefree!

1. Do all greeting cards contain only good wishes?

Christmas and New Year's are the time when we send and receive numerous greetings both from our loved ones and from various senders. However, some messages may contain viruses, malware, and are most commonly used for phishing. Phishing refers to Internet fraud in the form of fake e-mail messages that appear to be sent by legitimate organizations (for example, a bank or online shopping site) and that trick the recipient into sharing personal, financial or security information. In this way, fraudsters gain access to usernames, passwords or credit card information. In such emails, you are most often asked to download an attached document or click on a link.

Therefore, caution is recommended before opening attachments or clicking on links found in messages, especially if the message comes from an unknown sender and if the text is full of spelling mistakes.

If the sender is suspicious, do not open the email.

Also pay attention to the file extensions in the attachment - do not open attachments with unusual extensions such as .jar, .ace.

If you received a suspicious link in your email, hover over the URL, but don't click - you should see the correct URL to be redirected to. If it looks suspicious or ends in .exe, .js or .zip, don't open the link!

2. Relaxed group photo or problem?

Christmas time is a time of parties, receptions and travel. Post your and other people's photos/videos on social networks without thinking and asking? Do you have your privacy settings set so that everyone can see everything you post? Think about whether it's smart - content that you wouldn't want your parents, boss or work colleague to see, don't post it on the internet.

If you post photos or videos featuring other people, you should ask them if they agree with such posting

Pay special attention to photos of children and minors - protect them!

Avoid posting photos of children and minors or limit the visibility settings of the post to only your friends

3. Is every discount really a good discount?

The holiday mood and shopping for Christmas gifts can be spoiled by fake online shops whose goal is to steal personal

information and make financial gains. Big discounts can really be tempting and everyone's goal is to save, but to make sure you're buying from a trusted online store, follow these tips:

Beware of "too good offers" on unverified online shops

Make sure that the merchant's name and registered office, telephone number and e-mail address are listed on the website

Use verified online stores. You can check the credibility of the internet domain at the following link:

https://www.scamadviser.com/

Research reviews before you buy

Do not send copies of your ID cards and bank cards

If you pay by card, when purchasing, pay only through a secure payment service provider

Only pay when connected to a secure connection - avoid free or open WiFi

Only pay on a secure device - regularly update your operating system and security software

4. Happy waiting for a package to your home address or uncertainty on your current account?

The delivery service informed you that you received the package and in order to receive it at your home address they sent you a link to pay the fee? During the holiday season and the increased number of online purchases, an increased activity of fraudsters who send false notifications about the package received via e-mails and call for payment in order to deliver the package to you was noticed. You will notice a fake notification by the text that often contains spelling mistakes and the e-mail address that does not match the official e-mail address of the delivery service, therefore:

Check the sender's email address

Do not open suspicious links that invite you to pay a fee

Do not enter or send personal data and card number

Permanently delete email

5. Install smart

Do you want to have an imaginative and personalized greeting card to send to friends and family? There are many free Christmas card maker apps on the market today, and to make sure you don't install a virus or malware with the app, follow these tips:

Read the description of the application (if it contains errors, it should be suspected)

Before installing the application, read what data is collected, how long it is kept and how it will be used

Download applications only from official online application stores

Warn children not to download applications themselves

Plus tip: if you often use credit cards for online shopping, it is advisable to set up notifications for every transaction you make in real time, all so that you can spot potential unauthorized use of your card and be able to react and contact the bank in a timely manner.