Online Scams

Precautions

1. Phishing email scams

Phishing scams are based on communication made via email or on social networks.

In many cases, cyber criminals will send users messages/emails by trying to trick them into providing them valuable and sensitive data (login credentials – from bank account, social network, work account, cloud storage) that can prove to be valuable for them.

- Check the validity of the email
- Do not open links
- Report, block the email
- Do not give any personal information

2. The Royal/Prince scam

A typical Royal/Prince scam involves **an emotional email, letter, text message or social networking message** coming from a scammer (which can be an official government member, a businessman or a member of a very wealthy family member – usually a woman) who asks you to give help in retrieving a large sum of money from a bank, paying initially small fees for papers and legal matters. In exchange for your help, they promise you a very large sum of money.

- Do not respond
- Report and delete
- Do not send any money
- Do not click on any link
- Do not give any information

3. Greeting card scams

If you open such an email and click on the card, you usually end up with malicious software that is being downloaded and installed on your operating system.

If this happens, your computer will start sending private data and financial information to a fraudulent server controlled by IT criminals.

- Check if it from a trusted source that you know
- Do not open the cards if you don´t know the source
- Do not click on any link

5. Bank loan or credit card scam

- People can be easily scammed by “too good to be true” bank offers that might guarantee large amounts of money and have already been pre-approved by the bank.

Ask yourself:

“How is it possible for a bank to offer you such a large sum of money without even checking and analyzing your financial situation?”

- Watch your accounts closely and monitor your online transactions
- Take advantage of free consumer protection services
- Sign up for free credit monitoring

5. Lottery scam

A lottery scam comes as an email message informing you that you won a huge amount of money and, in order to claim your prize or winnings, you need to pay some small fees.

- Carefully look at the source
- Do not click on any link
- Do not give your personal details
- Report and delete

6. Hitman scam

This type of online scam may come in various forms, such as the one threatening that they will kidnap a family member unless a ransom is paid in a time frame provided by the scammers.

To create the appearance of real danger, the message is filled with details from the victim's life, collected from an online account, a personal blog or from a social network account.

Do not put your personal information over social media.

Do not panic but report and block

7. Online dating (romance) scams

A romance scam usually takes place on social dating networks, like Facebook, or by sending a simple email to the potential target, and affect thousands of victims from all over the world.

- Do not respond
- Check the source and report
- Unsubscribe if signed up mistakenly (the unsubscribe button is usually located at the bottom of the email message)
- Do not give any personal information
- Do not download anything

8. Fake antivirus software

We all saw at least once this message on our screens: “*You have been infected! Download antivirus X right now to protect your computer!*”

Many of these pop-ups were very well created to look like legitimate messages that you might get from Windows or any other security product.

- Make sure you **do not click** on pop-up windows that annoyingly warn you’ve been infected with a virus.
- Remember to always apply the existing updates for your software products and install **only legitimate software programs from verified websites.**

9. Facebook impersonation scam (hijacked profile scam)

As much as it connects you with friends and families Facebook may also expose for scams.

- Do not accept friend requests from people you don’t know
- Do not share your password with others
- When logging in, use two-factor authentication
- Avoid connecting to public and free Wi-Fi networks
- Keep your browser and apps updated

10. Make money fast scams (Economic scams)

Cybercriminals will lure you into believing you can make **money easy and fast on the internet**. They'll promise you non-existent jobs, including plans and methods of getting rich quickly.

- Never wire money to a stranger
- Do not give out information like SSN
- Never click email hyperlinks
- Use tough-to-crack password
- Install antivirus and spyware
- Do not shop from unfamiliar websites
- Do not download from pop ups
- Visit only safe websites
- Only donate to known charities

11. Travel scams

These scams are commonly used during hot summer months or before the short winter vacations, for Christmas or New Year's Day.

Here's how it happens: you receive an email containing an amazing offer for an exceptional and hard to refuse destination (usually an exotic place) that expires in a short period of time which you can't miss.

If it sounds too good to be true, it might look like a travel scam, so don't fall for it!

12. Bitcoin scams

If you (want to) invest in Bitcoin technology, we advise you to be aware of online scams. Digital wallets can be open to hacking and scammers take advantage of this new technology to steal sensitive data.

The most common online scams to watch out for:

- Fake Bitcoin exchanges
- Ponzi schemes
- Everyday scam attempts
- Malware

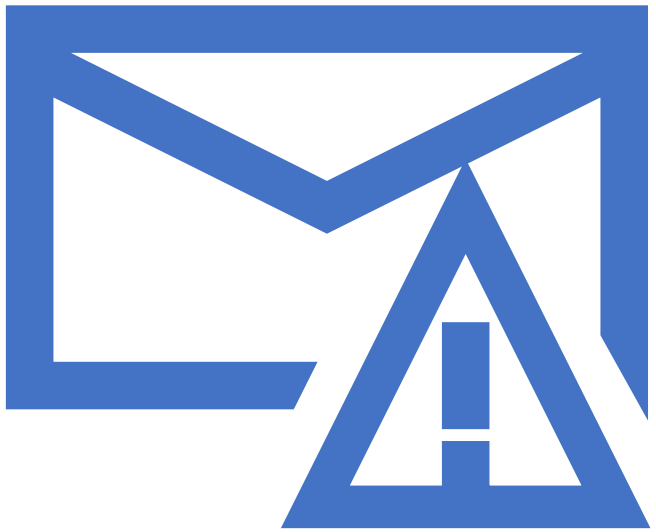
So, avoid such sites and never put your personal information

13. Fake news scam

These are misleading resources and content found online, making it impossible for people to distinguish between what's real and what is not.

- Access/read only reliable sources of information coming from friends or people you know read regular feeds from trusted sources: bloggers, industry experts, in order to avoid fake news.

- Use tech tools such as **Fact Check** from Google or **Facebook's tool** aimed at detecting whether a site is legitimate or not, analyzing its reputation and data.



14. Fake shopping websites

If you spot a great online offer which is “too good to be true”, you might be tempted to say “yes” instantly, but you need to learn how to spot a fake shopping site so you don’t get scammed.

- Strange URL’s
- A strange selection of brands
- Broken language
- Strange contact information
- Prices are ridiculously low.
- Horrible design.

If you see the above signs, do not use the sites and do not give any personal information

15. Loyalty points phishing scam

Many websites have a loyalty program to reward their customers for making different purchases, by offering points or coupons. This is subject to another online scam because cybercriminals can target them and steal your sensitive data

The most common attack is a **phishing scam** that looks like a real email coming from your loyalty program, but it’s not.

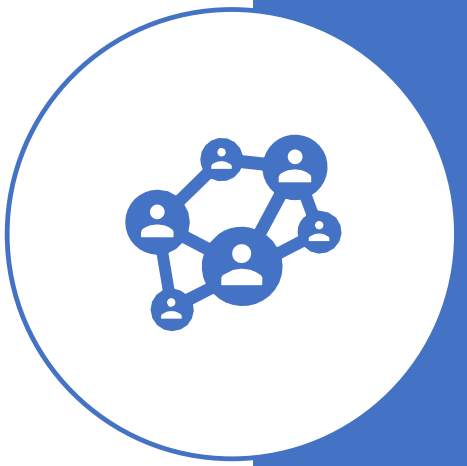
Always avoid unfamiliar sites and do not give away your information

16. Job offer scams

They use fake and “attractive” job opportunities to trick people.

To protect yourself from job offer scams, it’s very important to:

- Do thorough research about the company and see what information you can find about it
- Check the person who’s been contacted you on social media channels
- Ask for many details and references and check them out
- Ask your friends or trustworthy people if they know or interacted with the potential employee



17. SMS Scamming (Smishing)

Smishing (using SMS text messages) is a similar technique to phishing, but instead of sending emails, malicious hackers send text messages to their potential victims.

How does this happen? You receive an urgent text message on your smartphone with a link attached saying that it's from your bank and you need to access it in order to update your bank information or other online banking information.

Be careful about these SMS you receive and **don't click on suspicious links** that could redirect to malicious sites trying to steal your valuable data.

18. Overpayment Online Scam

This works by getting the potential victim **“to refund”** the scammer an extra amount of money because he/she send too much money. The offer will often be quite generous and bigger than the agreed price. **The overpay (extra money)** is to cover the costs of shipping or certain custom fees.

- Do not transfer extra money to someone you don’t know, especially if he/she wants to overpay. A legitimate buyer won’t do that.
- Also, do not transfer money to a fake shipping company or some private shipping agent
- Do not provide personal information to people who don’t show a genuine interest in buying your item.
- Do not send the product to the buyer until the payment was completed and received in your bank account.

19. Tech Support Online Scams

These tech “experts” pretend to know everything about your computer, how it got hacked and many other details that help them gain your trust and convince victims to fall prey for their scams.

- Do not trust phone calls coming from people pretending to come from tech “experts”, especially if they are requesting for personal or financial information;
- Do not provide sensitive data to them or purchase any software services scammers may suggest
- Do not allow strangers to remotely access your computer and potentially install malicious software
- Make sure you download software apps and services only from official vendor sites
- Always have an antivirus program installed on your computer,