FREQUENTLY ASKED QUESTIONS (FAQ)

How to recognize a fraud attempt by email, phone or SMS?

Hackers often send emails and SMS by inserting fake links and login forms or call on behalf of financial institutions.
Their purpose is to make you believe that you are visiting the legitimate website, to enter your password and thereby gaining control of your account.

Remember one simple rule: a financial institution will never send you an email containing a login or password change link, or SMS, or call you to ask you to confirm any details over the phone.

All details of your plastic payment cards, including your personal details, are confidential and our staff will never ask you to confirm them by email or SMS, or by phone, except when you call at our official phone numbers.

The clearest sign of a malicious email is the sense of urgency – hackers lie implying that a password has leaked and the like.

Another sign you may notice is the link you receive – it does not lead to the official website of our company, but elsewhere.

If you click on a link in an email or SMS and it takes you outside our website, this is clearly a fraud attempt - you must leave this website immediately and delete the email or SMS.

Who is responsible if I am misled by an email, SMS sent by hackers or a call?

The customer is responsible for their vigilance and for familiarizing themselves with the security recommendations we provide on our website.
If you send your password to a hacker, it is your voluntary act for which you are responsible.

What do phishing, vishing and smishing mean?

Phishing:
Online phishing is usually **an electronic message sent by electronic mail (e-mail)**. **The message looks as if sent from a trustworthy sender, e.g.: public/**municipal authority, bank, any type of merchants/companies performing various activities (provision of utility services, investment in cryptocurrencies, issuance of credit cards, etc.). The message may appear legitimate and contain the trademarks of the respective organization, and the email address of the sender may look like the email address of the legal entity on whose behalf it is sent. **The visual appearance of fake websites often resembles or is even a complete copy of the original website.** Fake websites can be identified by comparing the two web addresses – of the original and of the fake webpage. Letters of the web address of the original webpage may have been replaced with visually similar symbols, for example: the ‘o/O’ letter can be replaced with zero - ‘0’; the ‘l’ or ‘I’ letters can be replaced with one – ‘1’, etc.
Sometimes, phishing is made by senders that are individuals who often present themselves as: heirs of wealthy relatives, relatives of sick people and others. In most cases, messages on behalf of individuals are more easily recognizable as fake.

It is a standard practice for the message to direct to a fake website, stating various reasons to invite them to visit the website in question and to provide personal data such as: username and password to access their various accounts (most commonly: online banking applications;

online shopping and payment applications); bank account/ card number; PIN, expiry date or CVV of a bank card; etc.

IMPORTANT! ***Do not perform the actions that suspicious emails invite you to perform, including:***

- ***do not open random links and attachments;***
- ***do not provide information about the different applications you use and your access to them, especially if the applications are for: online banking, shopping and payment, i.e. those containing information about your plastic or electronic bank card****.*

Vishing:
Vishing (voice + phishing) is a phone call by which the fraudster, using your personal information from social networks, tries to deceive you to provide your personal data from the categories of those mentioned in the phishing carried out by using electronic messages by e-mail.

Smishing (SMS Phishing):
SMS phishing is another type of phishing attack in which fraudsters try to obtain your personal data through your mobile device by sending a text message (for example: pretending to be an employee of a bank or other official organization).

IMPORTANT! *We* ***do not require – at any time, under any circumstances and by any of the above communication means*** *-* ***telephone, e-mail, SMS, other text messaging applications****, your usernames; passwords to access your accounts (most often: in Online banking applications; online shopping and payment applications); bank account/ card numbers; PIN, expiry dates or CVV of bank cards; etc.*

In case of suspected phishing, vishing, smashing, please contact us – through our Call Center at our phone number: + 359 2 493 0108, or send a message to the following e-mail address: info@iuvo-group.com to request from our employee detailed information regarding your suspicions, and if necessary, to block your user account for access to our services or block the card provided to you by us.

A general rule in the various types of phishing attacks is that they do not attack technologies and applications, but ***rely on human weaknesses and emotions*** *- fear, panic, joy of receiving a prize in kind or cash, and seek* ***to provoke reckless actions that result in taking a quick decision and clicking on various 'buttons'*** *through which malicious persons can receive your personal data.*

Do I need to activate access to my location, microphone, camera and contacts on my device (mobile phone/ computer) in order to use your landing page and application(s) in relation to applying for and using your products?

By activating the accesses stated, you provide the opportunity to access your personal data, and the personal data of your relatives, people who are close to you and acquaintances. Since it is possible that you and the aforesaid persons may be identified, a number of adverse consequences may occur for you/ them. **Therefore, the assessment of whether to activate these accesses or not should be: informed, specific (for each individual application/website feature), taking into account the type and nature of the information contained on your device.**

Location access: If you provide access to your location, you can be tracked very easily, including additional information can be received such as: why you are at such location, what you are doing at the time, who you are with, and other information that could be used maliciously against you and your companions. The information about you is obtained in real time through the so-called GeoTag. GeoTag is a process where your location information is entered into the photos you take - at the time they are taken. This means that if you post the photos on social networks and they reach malicious persons - by downloading them from there, or by sending them directly to such a person, you can very easily be physically traced.

Example: *Your location is required for the use of: some social networks or their individual features; travel log applications; navigation applications; weather forecast applications, etc.*

Microphone access: By providing access to your device's microphone, it can be very easy to record your conversations as well as the sounds of your surroundings, and they can be recorded even when you are not using your device.

Example: *The following applications require access to your device's microphone: music applications; music performance recognition; voice recording, etc.*

Access to a camera/ gallery of photos and videos: By granting access to the camera/ gallery of photos and videos on your device, the content of your gallery can very easily be used for malicious purposes that you are not aware of, other than the purposes for which you have authorized access to them. In addition, the camera can capture photos and videos, even without your knowledge, which may leak on the Internet and be used to your detriment and to benefit malicious persons.

Access to contacts: By granting access to the contacts stored on your device, the personal data of your contacts (names, telephone numbers, e-mail) can very easily be used by malicious persons to send (on behalf of your contacts to third parties) unsolicited messages (spam), as well as send false messages by e-mail (phishing).

In view of and despite the above, you should consider that when you grant access to your device, this does not necessarily result in adverse consequences for you. Requiring access to the devices you use, to their features and the different types of information contained on your devices is necessary for the applications you use to function. When allowing access to your device, on a case-by-case basis, you should be guided by whether and what access is necessary for the use of the respective applications. Only in this way will you be able to control and reduce the risk of unlawful and improper use of your device and the personal data it contains about you and your relatives, friends and acquaintances.

How can I find out if the emails I receive on your behalf were actually sent by you?

The emails you receive are not sent by us when:

- **The title is so worded as to attract your attention and invites you to follow the link contained in the email or open an attached file**;

- **They create a sense of urgency and immediacy, and contain action instructions like the following**: *Due to unauthorized access to your account, you need to change your password. To do so, click on the following link*;

- **They were sent by a public email service** – such as yahoo.com, gmail.com, abv.bg, etc. As a rule, companies register and use their own domains rather than using public ones;

- **The domain address does not contain the name of our company** - you can check what the sender's email address is and whether it contains the name of our company or not by referring to the 'From' field, which displays the name chosen by the sender to see when you receive an email from them.

  Example of a fake email address for a company named FinBank: **FinBank**@poshta-abc.bg.

  Example of a valid email address for a company named FinBank: poshta-abc@**finbank**.bg.

  From the examples mentioned, it is evident that the valid email of the company named FinBank is the one that contains the name of the company in the domain address;

- **The displayed domain** contains: changed letters, added letters, characters, etc.;

- **The textual content of the message has many spelling, grammar, semantic and other errors**, usually due to a translation from a foreign language carried out using an automatic translator such as Google Translate.

When is a password secure?

We are witnessing breaches in the systems of global and Bulgarian companies and administrative bodies, as well as personal data leaks from those companies and bodies, including in the financial sphere.
As a result of in-depth analysis carried out by technology market leaders, it turns out that the old 'complex' passwords are no longer effective.

The rule to use a number, an uppercase letter, a symbol and more than 8 characters, which is well known to us, **is no longer the most secure one to create passwords**. The reason for reducing the security level of passwords created under this rule is that people consistently start creating passwords such as **'P@ ssword123"** that match the requirements of complexity, but are **very easy to guess** in a hacker attack. Very often, people use passwords that contain **their personal information**, which is also **easy to guess**.

Therefore, following best practices, **we recommend that you create easy to remember but difficult to guess passwords** containing a Pass Phrase – i.e., the **password should be a combination of words (phrase) that make sense to you**, such as: a **favorite phrase, proverb or a vivid, memorable phrase such as *'thepurplehorselikespears'* or a phrase from your favorite book.** A password created in this way allows it to be used for a longer period of time (for half/ one year) and not to be changed every 30/ 60/ 90 days, which is the most common practice.

When creating passwords for various personal purposes, we also advise you:

- To create passwords containing **more than 14 characters**, and if you wish, the combination of words can include numbers and/or symbols, but their use is not necessary;

- Do not record/ take photos of your access passwords;
- Do not send them via email, Viber, messenger, WhatsApp or other chat applications, or via SMS;
- Use two-factor authentication to protect your accounts;
- Do not share your password with others, including people who are close to you;
- Use password generation and management software if you fail to come up with reliable and unique passwords yourself;
- Replace your old password with a new one from time to time to minimize the possibility of accessing your account(s).

In the light of the foregoing, we use the following comparison for passwords:

Passwords are like toothbrushes – ***choose a good one, don't share it with anyone, change it regularly****.*

When is it safe to use websites?

As part of a group which have significantly contributed to the digitalization of the financial sector, we offer remote services to our customers by using web pages.

Based on the above, we would like to advise you:

- Always access our website by typing its address in the address field of your browser (search engine);
- Watch out for suspicious emails. **Do not click on links sent in an email or in attachments**. They may contain malware that could infect your computer;
- Never follow links in an e-mail sent to you on our behalf if **we have not informed you in advance that you will receive a link from us**, because such links lead to websites with suspicious web addresses that may require the provision of: your usernames; passwords for access to your accounts (most often: in online banking applications; in online shopping and payment applications); bank account/ card numbers; PIN, expiry dates or CVV of bank cards; other data related to your access and personal data;
- Regularly update the software on your device and the browser (search engine) you use;
- Never log into your accounts over public Wi-Fi networks;
- **Enable notification features where available when accessing your accounts from a device other than the one you usually use**. By doing so, you will be able to track unauthorized login to your accounts and you will have a greater opportunity to protect your personal data;
- Always choose a 'strong' password – see section 'When is a password secure?";
- In case of any doubts, please contact us.

When is a website secure?

When using the Internet, including for actions related to the use of your money, it is good to keep in mind the following:

- If **the web address typed in the URL address bar starts with** 'http**s**://", the presence of an **'s'** means that such website uses an encrypted, secure client-server communication connection. The absence of an **'s'**, i.e. when the website starts with 'http://', means that the website does not use a secure connection. Where a website does not use a secure connection, a malicious party may track or modify the information you send or receive through such website;

- **The presence in the browser search bar of an icon with a locked padlock image** – a locked padlock means that the page is secure because it uses a certificate to encrypt communication. The principle when issuing encryption certificates is that an individual certificate is issued for each website. When clicking on the padlock, a window with separate functions appears, and among them there is a function to see what the valid address of the website is, as well as information about the validity of the encryption certificate. Even in cases where an icon with an image of a locked padlock is available, we recommend always being careful when sharing information about you online;
- Beware of **dangerous websites that expose information you would share through them at risk**. Dangerous websites are identified by **a red warning message on the page** or **a red search bar** that can be used to identify that a particular website is dangerous;
- **Online purchases - do not shop through websites of unknown merchants and do not purchase brands that are not established in the market. Check the reviews of other customers** who have used the services of the respective merchant or have purchased goods from the specific brand. If the merchant's website lacks information about the merchant, contact information (email, phone, address) or contact form, this should be a warning to you that you may have come upon a non-existent merchant's website, and that the website was created by persons whose purpose is to obtain your personal data - bank account numbers and passwords, payment card numbers, etc. If you wish to use that merchant's services, despite of the fact that you are not able to contact it, it would be a good idea to try to make further checks on the merchant's existence (for example, by checking on the website of the Registry Agency – Commercial Register - https://portal.registryagency.bg/CR/Reports/VerificationPersonOrg using the merchant's business name) and on its reputation. Another indication of whether the person stated as a merchant is in good standing or not is the presence, respectively the absence, of delivery and return conditions of the goods and their nature. We also recommend that you keep a history of the transfers you made for the purchase of goods;
- Whenever you come upon **an overly tempting offer, be vigilant** because such offers are often intended to offer fake, poor-quality or non-existent goods, or are an attempt to defraud you – transfer of money and/or collection of your data – email addresses, passwords, bank card details and accounts;
- **Short (abbreviated) links** – when you come upon such a link, even if sent to you by an acquaintance or relative of yours, do not rush to open it before trying to find more information about the website to which the abbreviated link would redirect you. In the case where the abbreviated link is sent by an acquaintance or relative of yours, it is possible that their account has been improperly accessed by malicious persons who send short links from their account and to their contacts. **To check the website to which the short link leads, hover your mouse over the link without clicking on it**. In this way, the full and true address to which the short link would redirect you will be displayed, and you will be able to find out whether the web address was designed to harm you or not.

What is the nature and benefit of the two-factor authentication of my accounts?

The two-factor authentication of your accounts is a two-step verification method of your identity - the first step is a password to access your account, and the second step is an additional one-time code. Such a code is generated each time you log into your account and

can only be used once, and it is usually valid for a certain period of time after being generated. In this way, the one-time code ensures that your account cannot be accessed, even in case that an authorized person has found out your password, because they will not have the code generated for you and will not be able to enter it.

An example of cases of two-factor authentication is the possibility of two-factor account protection that some companies, such as Google, Facebook and others, provide to their users. Two-factor account protection is also introduced by most banks and banking institutions when money transfers are made through their electronic channels. In the above cases, in order to access your account or to order a payment to someone else's account through an online banking application, in addition to your password for accessing your account or your online banking, you will need to confirm your action via a mobile token or digital certificate and SMS code.

An additional protection code can be received by:

- **Short text message (SMS)** - you will receive a text message on your phone containing the code needed to log into your account;
- **Using applications designed to generate codes;**
- **Message to your e-mail.**

What are the risks for me if I use public Wi-Fi networks?

Public Wi-Fi networks, along with their advantages, have a number of disadvantages as well. Their advantages - they provide a convenient, easy and usually free-of-charge access to the Internet. Public Wi-Fi networks are particularly tempting for use by you when you want to save your mobile data, or by children whose Internet access is usually restricted by their parents.

The disadvantages of public Wi-Fi networks are less known, but at the same time they can lead to a number of adverse consequences for you, the effect of which can obliterate the effect of their above-mentioned benefits.

It is important to know that when using public Wi-Fi networks, access to them is also easy for people who want to harm other users, because through these networks your personal data can be most easily made public. In some cases, malicious persons create fake Wi-Fi networks designed to track the traffic of all users who want to use them.

If you wish to use a public Wi-Fi network, you should adhere to the following principles:

- Ensure that the respective website uses a secure connection – see section ‘When is a website secure?’;
- Do not access websites that require filling in of your personal data, such as: passwords, card numbers, etc., and do not log into your accounts;
- Do not allow sharing of data (documents, photos, etc.) from your smart devices while using a public Wi-Fi network, because any user of the network will be able to see them if they wish. Among the options to limit data sharing, there is usually the option – network discovery, which should also be disabled so that your device is not 100% visible on the public Wi-Fi network;
- Use the most up-to-date antivirus software possible;
- Clear cache and cookies from the browsers you use on your devices, and ensure that your browsers are up-to-date.

What are your domain addresses?

Our domain addresses are:

	In social networks:

https://iuvo-group.com/	Facebook: https://www.facebook.com/iuvo.group/ Instagram: https://www.linkedin.com/company/iuvo/ YouTube: https://www.youtube.com/@iuvo-group LinkedIn: https://www.linkedin.com/company/iuvo/

Be suspicious of the websites you visit and trust only the authentic ones!