# ЧЕСТО ЗАДАВАНИ ВЪПРОСИ (ЧЗВ)

## Как да разпозная опит за измама по мейл, телефон или SMS?

Хакери често пращат имейли, SMS или се обаждат от името на финансови институции, слагайки фалшиви линкове и форми за логин.
Целта им е да Ви накарат да повярвате, че сте на легитимния сайт, да си въведете паролата и с нейна помощ да придобият контрол над Вашия акаунт.

Запомнете едно просто правило: никоя финансова институция никога няма да Ви изпрати и-мейл с линк за логин или смяна на парола, нито SMS, нито ще Ви се обади, за да Ви кара да потвърдите каквито и да било данни по телефона.

Всички данни на Вашите пластмасови карти за разплащане, включително Ваши лични данни, са конфиденциални и наши служители никога няма да искат да ги потвърдите с мейл или SMS, нито по телефона, освен когато Вие звъните на нашите официални телефонни номера.

Най-ясният признак за фалшив мейл е усещането за спешност – хакерите лъжат с намеци за изтичане на парола и други подобни.

Друг признак е линкът, който получавате – той не води до официалния сайт на нашата компания, а другаде.

Ако кликнете на линк в мейл или SMS и той Ви води извън нашия сайт, това 100% е опит за измама – незабавно напуснете този сайт и изтрийте мейла или SMS.

## Кой е отговорен, ако се подлъжа по изпратен от хакери мейл, SMS или обаждане?

Клиентът има отговорност за своята бдителност и за това да се запознае със съветите за сигурност, които предоставяме на сайта си.
Ако изпратите на хакер Вашата парола, това е Ваше доброволно действие, за което отговорността е Ваша.

## Какво означават понятията фишинг, вишинг исмишинг?

**Фишинг (Phishing):**
Онлайн фишингът обикновено е **електронно съобщение, изпратено по електронна поща (имейл/ e-mail)**. **Съобщението прилича на такова от надежден изпращач, например: държавна/** общинска администрация, банка, всякакъв вид търговци, извършващи различни дейности (предоставяне на комунални услуги, инвестиции в криптовалути, издаване на кредитни карти, други). Съобщението може да изглежда легитимно и да съдържа запазените знаци на съответната организация, а адресът на електронната поща на изпращача да наподобява този на юридическото лице, от чието име се изпраща. **Визуалният облик на фалшивите сайтове често наподобява или дори е пълно копие на оригиналния сайт.** Разпознаването на фалшивите сайтове може да бъде извършено чрез съпоставка между двата адреса – на оригиналната и на фалшивата страница. Букви от адреса на оригиналната страница може да са заменени с визуално подобни символи, например: буквата „o/O“, да бъде заменена с нула - „0“; буквите „l” (ел) или „I“ (ай) с единица – „1“, и т.н.
Понякога, фишингът е с изпращачи физически лица, които често се представят като: наследници на богати роднини, роднини на болни хора и други. В повечето случаи, съобщенията от името на физически лица са по-лесно разпознаваеми като фалшиви.

Стандартна практика е съобщението да насочва към фалшив уеб-сайт, посочвайки различни причини, чрез които да ги подканят да посетят въпросния сайт и да предоставят лични данни като: потребителско име и парола за достъп до различни техни профили (най-често: в приложения за интернет банкиране; в приложения за онлайн пазаруване и разплащане); номер на банкова сметка/ карта; PIN, дата на валидност или CVV на банкова карта; други.

**ВАЖНО!** ***Не извършвайте действията, към които Ви подканват съмнителни електронни съобщения, в това число:***

- ***не отваряйте различни линкове и прикачени файлове;***
- ***не предоставяйте информация за използваните от Вас различни приложения и за достъпа Ви до тях, особено ако приложенията са за: интернет банкиране, пазаруване и разплащане, т.е. такива съдържащи информация за Вашата физическа или електронна банкова карта***.

**Вишинг (Vishing):**
Vishing (voice + phishing) е телефонно обаждане, с което измамникът, ползвайки Ваша лична информация от социалните мрежи, се опитва да Ви заблуди да предоставите Ваши лични данни от категориите на посочените при фишинга, извършван чрез изпозлване на електронни съобщения по електорнна поща.

**Смишинг (Smishing/ SMS Phishing):**
SMS phishing е друг вид фишинг атака, при която измамниците се опитват да се сдобият с Ваши лични данни през мобилното Ви устройство чрез изпращане на текстово съобщение (например: представяйки се за служител на банка или друга официална организация).

**ВАЖНО!** ***Ние <u>не изискваме – никога, при никакви обстоятелства и по никой от горепосочените комуникационни канали</u> – телефон, електронна поща, SMS, други приложения за текстови съобщения****, Ваши потребителски имена; пароли за достъп до Ваши профили (най-често: в приложения за интернет банкиране; в приложения за онлайн пазаруване и разплащане); номера на банкови сметки/ карти; PIN, дати на валидност или CVV на банкови карти; други.*

*При съмнение за осъществен, спрямо Вас, фишинг, вишинг, смишинг, задължително се свържете с нас - чрез Call Center на нашия телефонен номер: + 359 2 493 0108, или изпратете съобщение до следния наш адрес на електронна поща: info@iuvo-group.com, за да поискате от наш служител подробна информация относно Вашите съмнения, а при необходимост, и блокиране на Вашия потребителски профил за достъп до нашите услуги или блокиране на предоставената Ви от нас карта.*

*Общо правило при различните разновидности на фишинг атаките е, че те не атакуват технологии и приложения, а* ***разчитат на човешките слабости и емоции*** *- страх, паника, радост от получаване на предметна или парична награда, и се стремят* ***да предизвикат необмислени действия в посока бързо решение и кликване върху различни „бутони“****, посредством които недобросъвестните лица да получат Вашите личните данни.*

**Необходимо ли е да активирам достъп до локацията ми, микрофона, камерата и контактите на моето устройство (мобилен телефон/ компютър), за да използвам Вашите лендинг страница и приложение/я по повод кандидатстването за и ползването на Вашите продукти?**

Чрез активирането на изброените достъпи Вие предоставяте възможност за осъществяване на достъп до Ваши лични данни, както и до личните данни на Ваши роднини, близки и познати. Поради възможността за Вашата и на посочените лица идентификация е възможно за Вас/ тях да възникнат редица неблагоприятни последствия. **Затова, преценката дали да активирате посочените достъпи следва да бъде правена: информирано, конкретно (за всяко отделно приложение/ функционалност на сайт), съобразявайки се с вида и характера на информацията, която се съдържа на Вашето устройство.**

**Достъп до локация**: Чрез предоставен достъп до местоположението Ви може много лесно да бъдете проследен, в това число може да се получи и допълнителна информация като: причината да се намирате на съответното място, какво извършвате в конкретния момент, с кого сте, както и друга информация, която би могла да бъде използвана злонамерено спрямо Вас и Вашите спътници. Получаването на информацията за Вас се извършва в реално време чрез т. нар. GeoTag. GeoTag е процес, при който информация за локацията Ви се вписва в снимките, които правите - в момента на тяхното заснемане. По този начин, ако публикувате снимките в социалните мрежи и те достигнат до недобронамерени лица - чрез свалянето им от там, или при директното им изпращане до такова лице, много лесно можете да бъдете физически проследен.

**Пример:** *Вашето местоположение е необходимо за използването на: някои социални мрежи или отделни техни функционалности; приложения за отбелязване на места, които посещавате; навигационни приложения; приложения за метереологични прогнози и други*.

**Достъп до микрофон**: Чрез предоставен достъп до микрофона на Вашето устройство може много лесно да бъдат записвани Ваши разговори, както и звуците от заобикалящата Ви среда, като записването им може да бъде извършвано дори когато не използвате Вашето устройство.

**Пример:** *Достъп до микрофона на Вашето устройство изискват приложения за: музикални апликации; разпознаване на музикални изпълнения; запис на глас и други*.

**Достъп до камера/ галерия със снимки и видеоклипове:** Чрез предоставен достъп до камерата/ галерията със снимки и видеоклипове на Вашето устройство може много лесно съдържанието в галерията Ви да бъде използвано за злонамерени цели, с които не сте запознат, странични от целите, за които сте разрешил достъпа до тях. Освен това, камерата може да заснеме снимки и клипове, дори без Ваше знание, които е възможно да попаднат в интернет пространството и да бъдат използвани във Ваша вреда и за облагодетелстване на недобросъвестни лица.

**Достъп до контакти**: Чрез предоставен достъп до контактите, съхранени на Вашето устройство, личните данни на Вашите контакти (имена, телефон, електронна поща) могат много лесно да бъдат използвани от недобросъвестни лица за изпращане (от името на Вашите контакти до трети лица) на непотърсени съобщения (спам), както и за изпращане на лъжливи съобщения по електронна поща (фишинг).

**Предвид и въпреки горното, следва да имате предвид че когато предоставяте достъп до Вашето устройство, не е задължително това да води до неблагоприятни за Вас последствия. Изискването на достъп до използваните от Вас устройства, до техните функционалности и до съдържащата се в устройствата Ви различна по вид информация е необходимо, за да функционират използваните от Вас приложения**. При разрешаването на достъп до Вашето устройство, за всеки конкретен случай, следва да се ръководите от това дали и какъв достъп е необходим за използването на съответните приложения. Само така ще имате възможност да контролирате и намалите риска от неправомерно и недобросъвестно използване на Вашето устройство и на съдържащите се в него Ваши и на Ваши роднини, близки и познати лични данни.

## Как мога да се ориентирам дали имейлите, които получавам от Ваше име, наистина са изпратени от Вас?

Имейлите, които получавате, не са изпратени от нас, когато:

- **Заглавието е така формулирано, че да привлече Вашето внимание и Ви приканва да последвате, съдържащ се в имейла линк или да отворите прикачен към него файл**;

- **Създават усещане за спешност и неотложност, като съдържат и указания за действие, подобни на следното**: *Поради засечен неоторизиран достъп до Вашия профил, необходимо е да промените паролата си. За целта, последвайте следния линк*;

- **Са изпратени от публична имейл услуга** – такива са yahoo.com, gmail.com, abv.bg и други. Като правило, компаниите регистрират и използват собствени домейни, а не използват публични такива;

- **В домейн адреса не е посочено наименованието на компанията ни** - може да проверите какъв е имейл адресът на изпращача и дали в него се съдържа наименованието на компанията ни чрез справка в полето „От“, където се визуализира името, което изпращачът е избрал да виждате, когато получавате електронно съобщение от него.

  Пример за фалшив имейл адрес за компания, чието наименование е „FinBank“: **FinBank**@poshta-abc.bg.

  Пример за истински имейл адрес за компания, чието наименование е „FinBank“: poshta-abc@**finbank**.bg.

  От посочените примери е видно, че истинският имейл на компанията с наименование „FinBank“ е този, който съдържа наименованието на компанията в домейна;

- **Изписаният домейн** съдържа: сменени букви, добавени букви, знаци и други;

- **Текстовото съдържание на съобщението е с много правописни, граматически, смислови и други грешки**, дължащи се обикновено на превод от чужд език, извършен чрез използване на автоматичен преводач като „google translate“.

## Кога една парола е сигурна?

Ставаме свидетели на пробиви в системите на глобални и на български компании и административни органи, както и изтичане на лични данни от тези компании и органи, вкл. във финансовата сфера.
Като резултат от задълбочен анализ, извършен от технологичните лидери на пазара, се оказва, че старите „сложни“ пароли вече не са ефективни.

Правилото: цифра, главна буква, символ и повече от 8 символа, което всички добре познаваме, **вече не е най-сигурното за създаване на пароли**. Причината за намаляване нивото на сигурност на пароли, създадени по това правило е, че хората консистентно започват да създават пароли от типа **„P@ssword123“**, които съвпадат с изискванията за сложност, но са **изключително лесни за отгатване** при хакерска атака. Много често хората използват пароли, които съдържат **тяхна лична информация**, която също е **лесна за отгатване**.

Затова, следвайки добрите практики, **препоръчваме да създавате лесни за запомняне, но сложни за отгатване пароли**, съдържащи Pass Phrase – т.е., **паролата да е комбинация от думи (фраза), които имат смисъл за Вас**, като: **любима фраза, поговорка или ярка, запомняща се фраза от типа *„лилавиятконобичакруши“* или фраза от Ваша любима книга.** Създаването на парола по този начин, позволява тя да бъде използвана за по-дълъг период от време (за половин/ една година), а не да се сменя на всеки 30/ 60/ 90 дни, каквито са най-честите практики.

При създаването на пароли за различни лични цели Ви съветваме още да:

- Създавате пароли, които са с **повече от 14 символа**, като към комбинацията от думи, по Ваше желание, може да включвате цифри и/или символи, но използването им не е необходимо;
- Не записвате/ снимате паролите си за достъп;
- Не ги изпращате по имейл, вайбър, месинджър, уотсъп или други чат приложения, или чрез SMS;
- Използвате двуфакторна защита на профилите си;
- Не споделяте паролата си с други хора, включително с Ваши близки;
- Използвате софтуер за генериране и управление на пароли, ако сами не успявате да измислите надеждни и уникални пароли;
- Заместват старата си парола с нова, периодично, за да минимизирате възможността за достъп до вашия/те профил/и.

Предвид всичко по-горе, ние използваме следното сравнение за паролите:

*Паролите са като четките за зъби – **изберете си добра, не я споделяйте с никого, сменяйте я редовно**.*

## Кога използването на уеб сайтове е безопасно?

Като част от група със съществен принос за дигитализацията на финансовия сектор, ние предлагаме дистанционни услуги на своите клиенти като използваме уеб страници.
**Въз основа на горното, бихме искали да Ви посъветваме:**

- Винаги достъпвайте интернет страницата ни като изписвате нейния адрес в адресното поле на браузъра си (търсачката);

- Внимавайте за съмнителни имейли. **Не кликвайте върху връзки, изпратени с имейл или в прикачените файлове**. Те могат да съдържат злонамерен софтуер, който да зарази компютъра Ви;
- Никога не следвайте линкове в изпратено до Вас електронно съобщение от наше име, когато **не сме Ви информирали предварително, че ще получите линк от нас**, защото подобни линкове водят до сайтове със съмнителни адреси, които може да изискват предоставяне на: Ваши потребителски имена; пароли за достъп до Ваши профили (най-често: в приложения за интернет банкиране; в приложения за онлайн пазаруване и разплащане); номера на банкови сметки/ карти; PIN, дати на валидност или CVV на банкови карти; други данни, свързани с Ваши достъпи и лични данни;
- Редовно актуализирайте софтуера на Вашето устройство, както и браузъра (търсачката), който използвате;
- Никога не влизайте в своите профили през публични Wi-Fi мрежи;
- **Активирайте функциите за нотификации, където са налични, при достъпване на Вашите профили от устройство, различно от това, което обикновено използвате**. Така ще може да проследите неоторизирано влизане в профилите Ви и ще имате по-голяма възможност да защитите Вашите лични данни;
- Винаги избирайте „силна“ парола – вижте раздел „Кога една парола е сигурна?“;
- При каквито и да е съмнения, свържете се с нас.

## Кога един сайт е сигурен?

При използване на интернет, в това число за действия, свързани с използване на Вашите пари, е добре да имате предвид следното:

- Ако в полето за **URL адрес изписаният адрес започва с** “http**s**://”, наличието на **“s”** означава, че изписаният сайт използва криптирана, защитена комуникация клиент-сървър връзка. Липсата на **“s”**, т.е. когато сайтът започва с “http://”, означава, че сайтът не използва защитена връзка. Когато сайт не използва защитена връзка, някой недоброжелател може да проследи или промени информацията, която изпращате или получавате чрез съответния сайт;
- **Наличие в адресната лента на браузъра на икона с изображение на заключен катинар** – заключеният катинар означава, че съответната страница е сигурна, защото използва сертификат за криптиране на комуникацията. Принципът при издаване на сертификати за криптиране е, че за всяка конкретна интернет страница се издава индивидуален сертификат. При кликване върху катинара се появява прозорец с отделни функции, сред които има и функция да видите какъв е истинският адрес на сайта, както и информация за валидността на сертификата за криптиране. Дори да има икона с изображение на заключен катинар, препоръчваме винаги да внимавате при онлайн споделянето на информация за Вас;
- Внимавайте за **опасни сайтове, които излагат на риск информацията, която бихте споделили чрез тях**. Опасните сайтове се обозначават с **червен предупредителен надпис на страницата** или със **светеща в червено адресна лента**, чрез които може да разпознаете, че конкретният сайт е опасен;
- **Онлайн покупки – не пазарувайте през сайтове на неизвестни търговци и не закупувайте марки, които не са наложени на пазара. Проверявайте отзивите на други потребители**, използвали услугите на съответния търговец или закупували стоки от конкретната марка. Ако на сайта на търговеца липсват информация за търговеца, информация за контакт с него (имейл, телефон, адрес)

или контактна форма, това трябва да е сигнал за Вас, че може да сте попаднали на сайт на несъществуващ търговец, както и че сайтът е създаден от лица, чиято цел е да получат Ваши лични данни – номера и пароли за банкови сметки, номера на разплащателни карти и други. Ако желаете да се възползвате от услугите на търговеца, въпреки липсата на възможност за осъществяване на контакт с него, би било добре да се опитате да направите допълнителни проверки за съществуването на търговеца (например чрез справка по име в сайта на Агенция по вписванията – Търговски регистър - https://portal.registryagency.bg/CR/Reports/VerificationPersonOrg) и на реномето му. Признак за това дали посоченото като търговец лице е действащо или не може да бъде и наличието, съответно липсата, на условия за доставка и връщане на стоките и какви са те. Препоръчваме също да пазите история на направените от Вас преводи за закупуване на стоки;

- Винаги когато попаднете на **прекалено примамваща оферта, бъдете бдителни**, защото чрез тях често се стреми предлагането на фалшиви, некачествени или несъществуващи стоки, или се прави опит за измама – превод на пари и/или събиране на Ваши данни – имейл адреси, пароли, данни за банкови карти и сметки;
- **Кратки (съкратени) линкове** – когато попаднете на такъв линк, дори и изпратен Ви от Ваш познат или близък, не бързайте да го отваряте, преди да се опитате да научите повече информация за сайта, към който съкратеният линк би Ви пренасочил. В случая, когато съкратеният линк е изпратен от Ваш познат или близък, възможно е профилът му да е неправомерно достъпен от недоброжелателни лица, които изпращат от неговия профил и до неговите контакти кратки линкове. **За да проверите сайта, към който краткият линк води, задръжте курсора на мишката върху линка, но без да кликвате върху него**. По този начин ще се визуализира пълният и истински адрес, към който краткият линк би Ви препратил и така ще можете да се ориентирате дали адресът е създаден, за да Ви навреди или не.

## Каква е същността и ползата от двуфакторната защита на моите профили?

Двуфакторната защита на Вашите профили представлява способ за проверка на самоличността Ви на две нива – първото ниво е парола за достъп до профила Ви, а второто ниво е допълнителен еднократен код. Такъв код се генерира при всяко отделно влизане в съответния Ви профил и може да се използва само веднъж, като обикновено е валиден за определен период от време след генерирането му. По този начин, еднократният код гарантира, че профилът Ви няма да може да бъде достъпен, дори и при научаване на Вашата парола от недоброжелател, защото той няма да разполага с генерирания за Вас код и няма да може да го въведе.

Пример за случаи на двуфакторна идентификация е възможността за двуфакторна защита на профилите, която някои компании, от ранга на Google, Facebook и други, предоставят на своите потребители. Двуфакторна защита на профилите е въведена и от повечето банки и банкови институции, когато се извършват парични преводи през техните електронни канали. В посочените случаи, за да достъпите Ваш профил или за да наредите плащане към чужда сметка през приложение за интернет банкиране, освен Вашата парола за достъп до съответния Ви профил или до електронното Ви банкиране, ще е необходимо да потвърдите съответното Ваше действие чрез мобилен тоукън или цифров сертификат и SMS код.

Кодът за допълнителна защита може да бъде получен чрез:

- **Кратко текстово съобщение (SMS)** – на телефона си ще получите съобщение, чието съдържание е кодът, чрез който – след въвеждането му, да влезете в профила си;
- **Използване на приложения, създадени да генерират кодове;**
- **Съобщение до Вашата електронна поща.**

## Какви са рисковете за мен, ако използвам публични Wi-Fi мрежи?

Публичните Wi-Fi мрежи, наред със своите предимства, имат и редица недостатъци. Предимства – те са удобен, лесен и обикновено безплатен начин за използване на интернет. Публичните Wi-Fi мрежи са особено примамливи за употреба от Вас, когато искате да спестите Вашите мобилни данни, или от деца, чийто достъп до интернет обикновено е ограничен от родителите им.

Недостатъците на публичните Wi-Fi мрежи са по-малко известни, но в същото време могат да доведат до редица неблагоприятни за Вас последици, ефектът от които може да заличи ефекта на горепо сочените техни ползи.

Важно е да знаете, че когато използвате публични Wi-Fi мрежи, достъпът до тях е също толкова лесен и за лица, които желаят да навредят на останалите ползватели, защото чрез тези мрежи Вашите лични данни могат най-лесно да станат публично достояние. В някои случаи злонамерените лица създават фалшиви Wi-Fi мрежи, чиято цел е да проследяват трафика на всички потребители, които поискат да ги използват.

Ако желаете да използвате обществена Wi-Fi мрежа, добре е да спазвате следните принципи:

- Да се уверите, че сайтът използва защитена връзка – вижте раздел „Кога един сайт е сигурен?“;
- Да не отваряте сайтове, които изискват попълване на Ваши лични данни, като: пароли, номера на карти, други, както и не влизайте в своите профили;
- Да не разрешавате споделянето на данни (документи, снимки и други) от Вашите смарт устройства, докато използвате публична Wi-Fi мрежа, защото всеки ползвател на мрежата ще може да ги види, ако пожелае. Сред опциите за ограничаване споделянето на данни обикновено има и опцията – network discovery (откриваем в мрежата), която е добре също да бъде изключена, за да може устройството Ви да не бъде на 100 % видимо в публичната Wi-Fi мрежа;
- Използвайте възможно най-актуален антивирусен софтуер;
- Да почиствате кешираната памет и бисквитките от браузърите, които използвате на Вашите устройства, както и да се стремите браузърите Ви да са обновени с последна версия.

## Кои са Вашите домейн адреси?

Нашите домейн адреси са:

| | В социалните мрежи: |
|---|---|
| https://iuvo-group.com/<br>https://www.iuvo.bg/ | Facebook:<br>https://www.facebook.com/iuvo.bulgaria/<br>Instagram:<br>https://www.linkedin.com/company/iuvo/<br>YouTube:<br>https://www.youtube.com/@iuvo-group<br>LinkedIn:<br>https://www.linkedin.com/company/iuvo/ |

Бъдете мнителни към сайтовете, които посещавате, и се доверявайте само на истинските такива!