



ОНЛАЙН ФИНАНСОВИ ИЗМАМИ И ИЗМАМНИ СХЕМИ В СВЕТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ

БЪДЕТЕ БДИТЕЛНИ И СЕ ПАЗЕТЕ

Онлайн финансовите измами и измамни схеми не са нещо ново, но изкуственият интелект (ИИ) ги направи по-умни и по-трудни за разпознаване. Престъпниците вече използват фалшиви съобщения и уебсайтове, фалшиви профили на знаменитости и дори генерирани от ИИ гласове или видеоклипове, които приличат на Вашия банкер, Вашите приятели или Вашето семейство, за да Ви подведат.

Те често се свързват с Вас чрез социални мрежи, приложения за съобщения, имейли и неочаквани обаждания, които звучат реалистично.

Може да се сблъскате с рискове като финансова загуба, кражба на самоличност и емоционален стрес. Бъдете внимателни и следвайте тези ключови съвети, за да сте в безопасност:



Бъдете бдителни за съществуващи онлайн финансови измами и измамни схеми, задвижвани от ИИ, напр. представяне за друг човек, фишинг, инвестиционни и застрахователни измами и дори романтични измами и измамни схеми. За да научите повече за различните видове измами и измамни схеми вж. [стр. 5](#), 6 и 7.

Както и за измами и измамни схеми, специфични за криптоактивите, вижте специалния разяснителен документ за измамите и измамните схеми с криптоактиви ([PDF](#)).



Разпознавайте предупредителните знаци:

Научете се да разпознавате подозрително поведение, съобщения или оферти (вж. [стр. 2](#));



Пазете се:

Защитете личните си данни (вж. [стр. 3](#)) и



Научете какво да правите, ако станете жертва на измама или измамна схема (вж. [стр. 4](#)).



Предупредителни знаци



Обещание, което изглежда твърде хубаво, за да е истина.



Неочаквано обаждане от непознат номер.



Спешно искане за пари или лична информация, включително от някой, който се представя за член на семейството, приятел или дори публична личност.



Искане за поемане на контрол над устройството Ви, да изтеглите приложение, да сканирате QR код или да кликнете върху връзка.



Искане за лична информация или банкови данни (например пароли, номера на кредитни карти, идентификационни данни за интернет банкиране или кодове за сигурност).



Искане за плащане чрез непроследими методи (напр. криптоактиви, подаръчни карти, банкови преводи или предплатени дебитни карти).



Подозрителен или неправилен имейл адрес или връзка (напр. правописни грешки в URL адрес или необичайни уеб адреси).



Прикачен файл от неизвестен източник, по-специално .exe, .scr, .zip или Office файл с активирани макроси (.docm, .xlsm).



Лоша граматика или форматиране в официално изглеждащ документ, въпреки че ИИ може да позволи на измамниците да маскират тези недостатъци по-ефективно.



Уебсайт, който изглежда професионално, но няма потвърдени данни за контакт или информация за регистрация на дружество.



Интонация, която звучи неестествено, липсват паузи и изглежда прекалено гладка или роботизирана. Обърнете внимание на „клонирането на глас“, въпреки че речта, генерирана от ИИ, също може да звучи много естествено.



Видеоклипове, при които гласът може да звучи роботизирано или прекалено гладко, движенията на устните и изразенията на лицето могат да бъдат несъответстващи на речта, или фонът, осветлението и сенките могат да бъдат непоследователни. Това често са генерирани от ИИ видеоклипове (дълбоки фалшификации; *deepfakes*).

Стъпки за самозащита

1

Никога не споделяйте лична или банкова информация:

Законните дружества никога няма да поискат Вашите ПИН кодове, пароли, идентификационни данни за интернет банкиране или кодове за сигурност по имейл, текстови съобщения, социални мрежи или телефон.

2

Направете пауза и помислете, преди да действате:

Не бързайте да изпращате пари, да споделяте информация или да кликвате върху връзки-измамниците умишлено създават усещане за неотложност (напр. ИТ проблеми с Вашата банка, спешни обаждания, включващи Вашите приятели и членове на семейството, заплашителен език и т.н.). В случай на съмнения, дори и незначителни, не действайте; прекратете обаждането и внимателно проверете източника или самоличността.

3

Проверете внимателно източника/самоличността:

- Винаги проверявайте откъде идват съобщенията, обажданията, имейлите и връзките- дори ако изглеждат официални, сякаш идват от приятел или Вашето семейство или дори публична личност. Например, обадете се или пишете на семейството и приятелите си, като използвате известен номер чрез надежден канал; потърсете правописни грешки, странни URL адреси или липсващи индикатори за сигурност (напр. проверете дали връзката към уебсайта включва „s“ в „HTTPS“, за да се уверите, че уебсайтът е защитен, и проверете за добавени или липсващи букви в името на дружеството).
- Не отваряйте връзки от непоискани съобщения, инсталирайте само официални приложения чрез надеждни магазини за приложения и не сканирайте непознати QR кодове.
- Съгласувайте със семейството си „безопасна дума“- тайна фраза, която можете да използвате, за да потвърдите самоличността си, ако някой с познат глас Ви се обади със спешно искане за пари и твърди, че е член на семейството (напр. родители, сестра/брат, дете).
- Използвайте проверени данни за контакт, за да се свържете директно с дружеството или физическото лице и никога не разчитайте на информацията за контакт, предоставена от предполагаемия измамник (напр. потърсете името на дружеството самостоятелно, използвайте проверени бизнес указатели, предварително потвърдени методи за контакт). Измамниците могат да твърдят, че са лицензирани или да имитират уебсайта на лицензирано дружество. Проверете дали Вашият национален финансов орган е издал предупреждения или дали те са включени в списъка I-SCAN на IOSCO (iosco.org/i-scan/). За доставчиците на криптоактиви проверете дали са лицензирани в ЕС (напр. проверете регистъра на ESMA (www.esma.europa.eu/)).

4

Обърнете внимание на потенциалните трикове с ИИ:

С напредването на технологиите за ИИ, измамните схеми стават по-убедителни от всякога- дори и с най-добрите съвети за сигурност. Ако нещо Ви се струва необичайно или забележите някой от предупредителните знаци, описани по-горе, спрете и преоценете.

5

Никога не инсталирайте софтуер за отдалечен достъп и не споделяйте екрана си:

Банките и финансовите институции никога няма да поискат това от Вас.

6

Поддържайте устройствата и профилите си сигурни:

Използвайте силни и уникални пароли, пазете ги в тайна и избягвайте повторното използване на едни и същи идентификационни данни на различни платформи. Разрешете многофакторното удостоверяване, когато е възможно. Поддържайте софтуера и антивирусната си защита актуални и активирани.

7

Бъдете предпазливи с неочаквани и ограничени във времето инвестиционни възможности:

Ако звучи твърде хубаво, за да е истина, вероятно не е истина.

8

Помислете, преди да споделяте информация в социалните мрежи:

Чат групи, форуми, публикации в социалните мрежи и снимки могат да бъдат ценни източници на знания за измамниците. Разкриването на твърде много информация за себе си или за Вашите инвестиции може да Ви направи лесна мишена.

Какво да направите, ако сте станали жертва на измама или измамна схема



Незабавно спрете операцията:

За да блокирате всякакви по-нататъшни преводи към подозрителни сметки и да избегнете допълнителни загуби. Прекратете всякакъв контакт с измамниците - игнорирайте техните обаждания и имейли и блокирайте подателя.



Свържете се с Вашата банка или финансово дружество:

Информирайте незабавно Вашата банка или финансово дружество чрез официалните канали за контакт, за да проучите възможностите за замразяване или отмяна на операции.



Променете паролите си на всички Ваши устройства и приложения/уебсайтове:

Измамниците купуват изтекли пароли онлайн и ги изпробват на множество профили. Промяната само на една парола не е достатъчна; не забравяйте да промените всички пароли, така че измамниците да не могат да ги използват повторно.



Докладвайте и предупреждавайте:

Докладвайте за инцидента на полицията или на Вашия национален финансов орган (<https://www.fsc.bg/>) и информирайте Вашата мрежа (напр. приятели и семейство), за да повишите осведомеността. Тези действия могат да Ви помогнат да защитите себе си и другите.



Пазете се от измами със „стая за възстановяване“ (recovery room):

Измамникът може да се свърже с Вас, знаейки, че сте жертва на предишна измамна схема, като твърди, че е публичен орган (напр. полиция, данъчен или финансов орган и т.н.) и предлага да възстанови загубените Ви пари срещу такса. Това често е поредният опит за измама. Не забравяйте: това, че веднъж сте били измамени, не Ви предпазва от това да бъдете измамени повторно.

ВИДОВЕ ОНЛАЙН ФИНАНСОВИ ИЗМАМИ И ИЗМАМНИ СХЕМИ, ЗАХРАНВАНИ ОТ ИИ



ИЗМАМА С ПРЕДСТАВЯНЕ ЗА ДРУГ ЧОВЕК И ИЗПОЛЗВАНЕ НА ДЪЛБОКА ФАЛШИФИКАЦИЯ (DEEP FAKE)

Получавате неочаквано обаждане от някого, който твърди, че е Вашата банка, публичен орган (например полиция, данъчен или финансов орган и т.н.), разпространител на застрахователни продукти, ИТ компания или дори член на семейството. Обажданият се може да Ви подкани да прехвърлите средства, за да ги запазите в безопасност, позовавайки се на подозрителна активност по Вашата сметка или застрахователна полица. Те могат също така да поискат от Вас да разкриете банковите си данни (напр. номер на платежна карта, идентификационни данни за интернет банкиране или пароли), да кликнете върху връзка или да инсталирате софтуер, като претендира, че той може бързо да реши проблема. Обажданият се може да използва фалшифициран номер, често съвпадащ с телефонния номер на Вашата банка, за да изглежда легитимен (спуфинг).

Измамниците могат да използват ИИ, за да създават фалшиви видеоклипове, изображения или аудио, които имитират нечий глас (напр. на Вашия банкер или на член на семейството), лице (напр. на знаменитост) или движения. **Това е известно като „дълбока фалшификация“ (deepfake).**

Какво може да се случи:

Споменавайки лични данни и създавайки усещане за неотложност, измамникът Ви подмамва към действия, които не сте възнамерявали да предприемете - като например изпращане на пари към сметката му, кликуване върху злонамерена връзка или инсталиране на зловреден софтуер на Вашето устройство. Това може да даде на измамника директен достъп до Вашите банкови идентификационни данни. С тази информация той може да промени паролата Ви, да влезе в банковата Ви сметка и да открадне парите Ви. Не забравяйте: само защото обажданият се знае лични данни за Вас, не означава, че той/тя е надежден/на.



ФИШИНГ И СОЦИАЛНО ИНЖЕНЕРСТВО

Получавате имейл или съобщение, което изглежда сякаш идва от Вашата банка или финансово дружество и Ви предупреждава за „подозрителна активност“ по сметката Ви. Логото, оформлението и езикът изглеждат професионално и съобщението може да се появи в същата връзка като други разговори от Вашата банка. Съобщението Ви подканва да кликнете върху връзка, за да потвърдите профила си или да нулирате паролата си. Връзката води до фалшив уебсайт, който изглежда идентичен с Вашето интернет банкиране. Без да го осъзнавате, въвеждате данните си в уебсайт, предназначен да открадне Вашата лична информация.

Измамниците използват ИИ, за да създават убедителни фишинг съобщения, като анализират данни от социалните мрежи, за да идентифицират жертвите си и да адаптират съдържанието за всяка цел.

Какво може да се случи:

Измамникът достъпва банковата Ви сметка и краде парите Ви или създава фалшив профил с личните Ви данни, за да извърши измама.



ИНВЕСТИЦИОННА ИЛИ ЗАСТРАХОВАТЕЛНА ИЗМАМНА СХЕМА

Виждате реклама в социалните мрежи или уебсайт, популяризираща „възможност за инвестиции за ограничен период от време с ниски рискове“ или „отстъпка за ограничен период от време“ за застраховка от добре познато дружество. Рекламата съдържа снимка на знаменитост и препоръки, които често са фалшиви. След като изразите интерес, като кликнете върху връзка или попълните формуляр, с Вас се свързват и Ви пренасочват към платформа или канал за съобщения, където получавате професионално изглеждащи съвети и документи. Насърчават Ви да инвестирате малка сума, последвана от по-големи суми, или да платите премията в това, което изглежда като защитена сметка.

Измамниците използват инструменти с ИИ, за да направят тези фалшиви предложения или имейли много убедителни и трудни за откриване. Те също така използват ботове за социални мрежи, захранвани от ИИ, за да създават фалшиви профили, които взаимодействат с Вас, разпространяват невярна информация и симулират реално поведение, за да спечелят доверие и да повлияят на Вашите решения.

Какво може да се случи:

След като се опитате да изтеглите парите си или да направите искане, контактът спира да отговаря. Откривате, че дружеството не съществува или че рискът, който сте застраховали, не е покрит. След това осъзнавате, че сте изпратили пари директно на измамник като част от измамна схема. За съжаление, не можете да получите парите си обратно, а Вашите лични и финансови данни могат да бъдат използвани за извършване на по-нататъшни измами (напр. подписване на договори от Ваше име, което може да доведе до загуба на още повече пари).



РОМАНТИЧНА ВРЪЗКА С ЦЕЛ ИЗМАМА И ИЗМАМНА СХЕМА

С Вас са се свързали в социалните мрежи, приложения за запознанства или по телефона/текстово съобщение от някой, когото не сте срещнали в реалния живот. Този човек участва в чести, лични и романтични разговори, изграждайки доверие, използвайки фалшиви профили. С течение на времето разговорът се измества към пари или финансови възможности, като например инвестиции в криптоактиви с обещания за висока възвръщаемост и нисък риск. Лицето Ви моли да прехвърлите пари по сметка или Ви напътства към създаване на сметка и извършване на малък първоначален депозит, за да изглежда схемата легитимна, преди да Ви насърчи да инвестирате повече.

Измамниците използват ИИ, за да генерират фалшиви профили, да идентифицират жертвите си в социалните мрежи/приложенията за запознанства, като използват данни, които сте предоставили, или да използват чатботове за генериране на съобщения.

Какво може да се случи:

Измамникът измъква колкото се може повече пари, след което прекъсва всякаква комуникация и изчезва. Измамният инвестиционен уебсайт или приложение се премахват от мрежата, което Ви оставя без достъп до предполагаемите инвестиции. В допълнение към финансовите загуби, личната информация, която сте споделили, може да бъде използвана за атака срещу Вашите приятели и семейство или за кражба на самоличност, което може да има финансови или правни последици за Вас (напр. измамникът може да направи покупки, да вземе заеми от Ваше име или може да бъдете подведени под отговорност за дългове или престъпления, извършени от Ваше име, докато не бъде доказано противното).



ИЗМАМНА СХЕМА ПРИ ЗАКУПУВАНЕ

Попадате на атрактивна оферта/предложение за покупка в онлайн платформа за търговия. Дружеството, което предлага офертата, иска плащане извън официалната платформа, като твърди, че използва „сигурна система за плащане“, и Ви изпраща връзка, за да завършите покупката. Връзката Ви пренасочва към измамна страница за удостоверяване на банка, която имитира официалния уебсайт на банката и използва нейното лого и дизайн, така че въвеждате данните си за онлайн банкиране, за да извършите плащането.

Измамниците използват ИИ, за да създават силно убедителни фалшиви банкови уебсайтове, потвърждения на поръчки и фактури. ИИ им помага да имитират тона, брендирането и стила на реални дружества. В някои случаи те използват чатботове с ИИ, за да отговорят на въпроси и да направят офертата да изглежда по-правдоподобна.

Какво може да се случи:

Плащането чрез връзка от трета страна заобикаля защитите на платформата за търговия. Измамникът, който получи информация за вход в банковата Ви сметка, ще откраде парите Ви.