



Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Стефка Илиева

Длъжност :Учител НЕ в ЦОУД

Месторабота:ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ „ Киберсигурност “ “

С продължителност ...5 академичен час

Дата : 02.02.2026г.

Подпис:

Илияна Марчовска

Директор



Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Нина Иванова

Длъжност : Начален учител

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност5 .. академичен час

Дата : 02.02.2026г.

Подпис:

Илияна Марчовска

Директор





Основно училище „Любен Каравелов“ с. Трудовец
Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Мариана Георгиева

Длъжност : Начален учител

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение
на тема: „ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:

Илияна Марчовска

Директор





Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Величка Минковска

Длъжност :Учител природни науки

Месторабота:ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:

Илияна Марчовска

Директор





Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Преслава Динкова

Длъжност :Учител по български език и литература

Месторабота:ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност 5 академичен час

Дата :02. 02.2026г.

Подпис:
Илияна Марчовска

Директор



Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

На

Наталия Иванова

Длъжност :Учител по английски език

Месторабота:ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност 5 академичен час

Дата : 02.02.2026г.

Подпис:
Илияна Марчовска
Директор



Основно училище „Любен Каравелов“ с. Трудовец
Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Цонка Филипова

Длъжност :Учител по ФВС

Месторабота:ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:
Илияна Марчовска

Директор



Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Наталия Василева

Длъжност : Начален учител

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:

Илияна Марчовска

Директор



Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Лидия Христова

Длъжност : Учител по математика

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„Киберсигурност“

С продължителност ...5.... академичен час

Дата : 02.02.2026г.

Подпис:

Илияна Марчовска

Директор



Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Весела Павлова

Длъжност : учител ЦДО прогимназиален етап

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:
Илияна Марчовска
Директор



Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

На

Илияна Йошовска

Длъжност : учител история и цивилизация

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:

Илияна Марчовска

Директор





Основно училище „Любен Каравелов“ с. Трудовец
Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Ема Николова

Длъжност : начален учител

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:
Илияна Марчовска
Директор



Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Габриела Дишкова

Длъжност : учител ЦОУД

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:

Илияна Марчовска

Директор





Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Петя Семкова

Длъжност : Учител прогимназия ЦОУД

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:
Илияна Марчовска
Директор



Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Йонка Василева

Длъжност : ЗДУД

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г.

Подпис:
Илияна Марчовска
Директор





Основно училище „Любен Каравелов“ с. Трудовец

Вътрешна квалификация на педагогическите специалисти

УДОСТОВЕРЕНИЕ

на

Илияна Марчовска

Длъжност : Директор

Месторабота: ОУ „Любен Каравелов“ с. Трудовец

Участвала в обучение

на тема:

„ Киберсигурност “

С продължителност ...5..... академичен час

Дата : 02.02.2026г



Обучение по киберсигурност: Как да разпознаете измамен имейл

От Exercybe Training <no-reply@training.exercybe.com>

Дата Вт 23.12.2025 г. 19:13

До 2300114: ОУ "Любен Каравелов" - Трудовец <info-2300114@edu.mon.bg>



ОБУЧЕНИЕ ПО КИБЕРСИГУРНОСТ

за служители на ОУ "Любен Каравелов", с. Трудовец

Как да разпознаете измамен имейл

Фишинг имейлите са сред най-често използваните методи за кражба на пароли и данни за достъп. Те разчитат на бърза и емоционална реакция и на пръв поглед често изглеждат легитимни.

⚠️ Признаци, че имейлът може да е измамен:

1. Получавате съобщение, което не очаквате.
2. Името на подателя изглежда познато, но е подвеждащо или леко променено.
3. Домейнът на имейл адреса не съответства на организацията на подателя.
4. Съобщението съдържа прикачен файл (.zip, .rar, .7z, .exe, .js) или файл с непознато разширение.
5. Обръщението е общо и не е адресирано лично към Вас.

6. Създава усещане за спешност или тревога, за да Ви накара да реагирате веднага.
7. Изказът звучи неестествено, често заради машинен превод.
8. Съдържа връзка, водеща към фалшив или зловреден уебсайт.

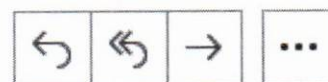
☒ **Как да се предпазите:**

- Не отваряйте прикачени файлове от подозрителни имейли.
- Не въвеждайте потребителско име и парола в уебстраници, отворени чрез връзки в имейли.
- Проверявайте връзките, като ги посочите с мишката, без да кликвате.
- При съмнение, посетете официалния уебсайт директно в брауъра.

Пример на реален фишинг имейл, който използва името и добрата репутация на финансова институция, за да подмами потребители да въведат данните си за вход във фалшив уебсайт:

Установена е подозрителна дейност -001111

К 2 Уни <kayla@pearlypersians.com>
To office@



5

7

Екипът Уни банк!

"Unicr bank" A.D., ние временно
6 затворихме акаунта Ви.

За да отключите акаунта, влезте във Вашия
Акаунт в Уни банк и следвайте
инструкциите.

<https://www.saudeviavel.pt/juoytvctly.html>

Click or tap to follow link.

8

Верификация



7

Уни банк сериозно се отнася към онлайн сигурността.

? Кой е правилният начин да разберете накъде води
връзка в получен имейл?

А) Ще кликна върху връзката.

Б) Ще я копирам и отворя директно в браузера.



ВНИМАНИЕ! ДЕЙСТВАЩА ИЗМАМА СЪС ЗАДЪРЖАНИ ПРАТКИ

Уважаеми info@abv.bg,

Бихме искали да Ви уведомим, че направихме два опита за доставка на Вашата пратка с номер **6012345678901**, но за съжаление бяха неуспешни.

Причината е, че посоченият адрес за доставка е непълен или грешен. Също така, липсва актуален телефонен номер, на който да се свържем с Вас за уточнение.

За да получите своята пратка, е необходимо да коригирате данните за доставка възможно най-скоро.

[Коригирай данните за доставка](#)

Важно! Това е автоматично съобщение. Моля, не отговаряйте на този имейл.

С уважение,
Екипът на Спиди

© 2025 Спиди. Всички права запазени.

1

Импортирано Премахване Добавяне

Потвърдете данните си

Моля, потвърдете данните, които Ви са предоставени. Ако има липсваща информация, моля, въведете я, преди да продължите.

* Пълно име
Име и фамилно

* Град
София

* Адрес
Улица и номер

* Личен код
1000

* Телефонен номер
088 123 4567

[Продължи](#)

2

Данни за доставка

Име:

Адрес:

Телефон:

Обобщение на плащането

Депозит (ДДС)	0.00 лв.
Такса доставка	0.51 лв.
Обща дължима сума	0.51 лв.

Актуализирайте Вашата карта

Сигурно плащане за осигуряване на пратката

* Номер на картата

* Валютност (MMBT)
MM / TT

* CVV Код

[Платете 0.51 лв.](#)

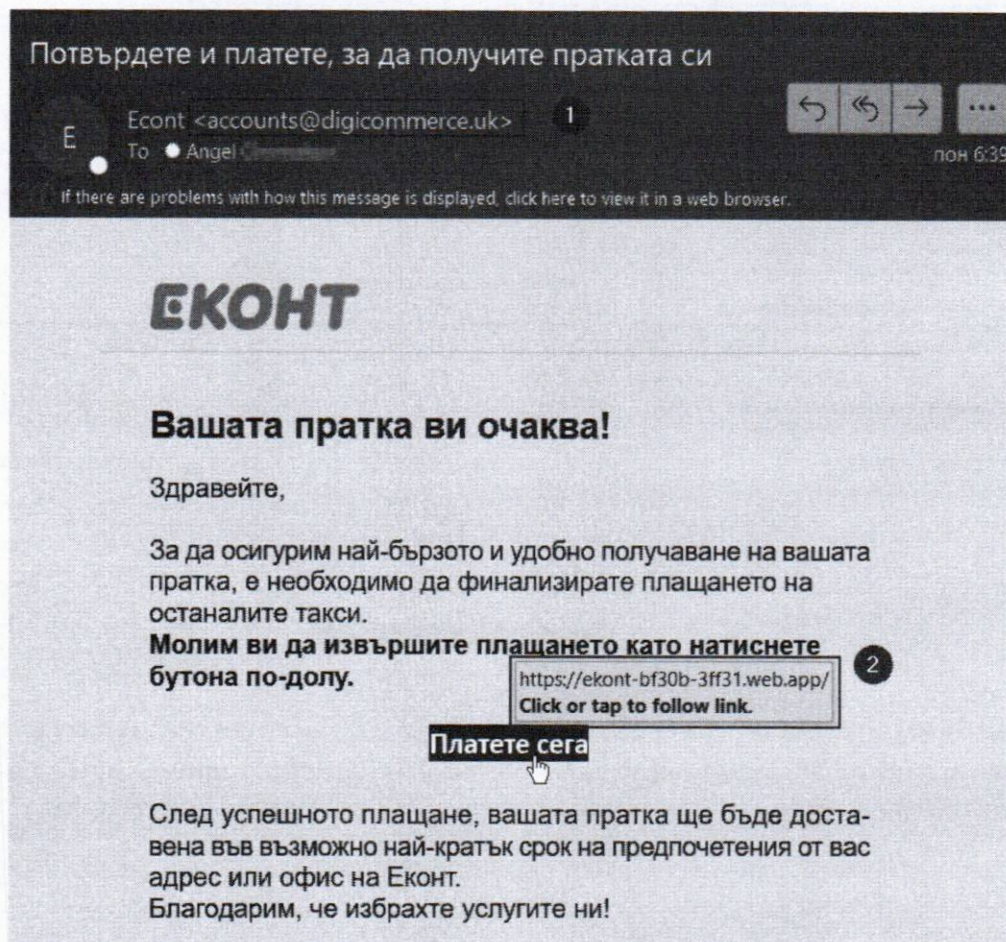
Показваме ви действаща за пореден месец измамна схема със задържана пратка поради сгрешен адрес за доставка или непълен телефонен номер. Измамната използва името на популярна куриерска фирма и се разпространява както по имейл, така и по SMS.

В конкретния пример, който показваме, става дума за имейл, който изисква от получателя да коригира данните си за доставка. Ако не обърнете внимание на несъответствието между подател, линк и компанията, за която се представят, линкът ще ви отведе до фалшива страница на куриера, на която да попълните личните си данни – имена, телефон, адрес. На следващата стъпка се отваря платежна форма за доплащане, където да попълните и данните от банковата си карта.

Ако го направите, освен личните ви данни от предходната стъпка, измамниците ще разполагат и с всичко необходимо, за да наредят превод до контролирана от тях сметка. В този момент, докато вие си мислите, че превеждате скромна сума пари на куриера, в действителност преводът е за съвсем друга сума и до друг търговец. Това се вижда в съобщението с допълнителния код, който получавате от вашата банка, и с който вие потвърждавате легитимността на превода.

Тази измама е многослойна и би могла да бъде разкрита на всяка от нейните стъпки, но големият брой подведени хора показва, че първоначалната заблуда на получателите се запазва до самия край, когато вече е твърде късно.

ФИШИНГ ИМЕЙЛ ОТ ИМЕТО НА ЕКОНТ С ЛИНК ЗА ПЛАЩАНЕ



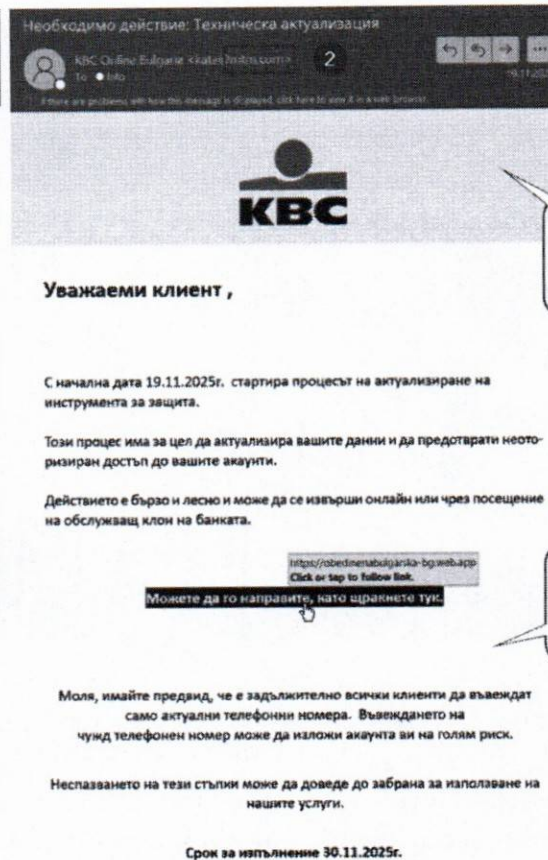
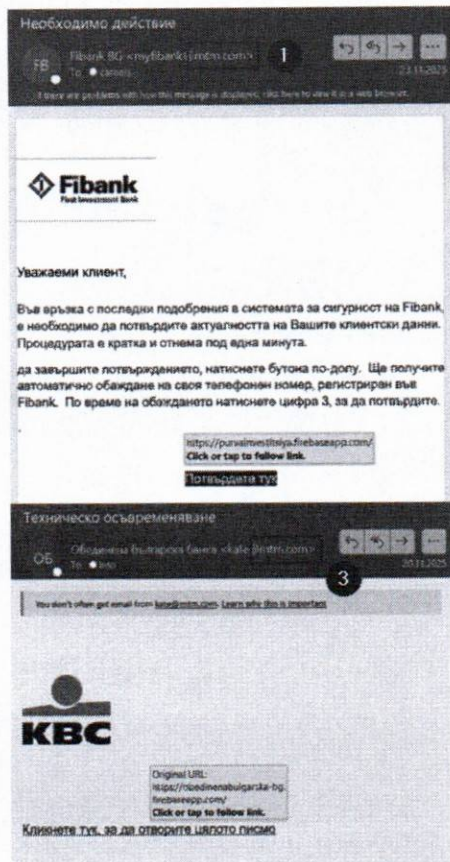
Куриерската компания Еконт е предпочитан местен бранд, който фишинг измамниците използват в опит да въведат в заблуждение неподготвени потребители, че куриерската им пратка изисква доплащане преди да бъде доставена.

Варианти на тази измама сме ви показвали и в предишни бюлетини. Текстът в тялото на имейла варира, но общото между всички остават маркираните на картинката полета за подател и линк в бутона. Това са типичните белези на почти всяка фишинг измама, по които лесно да бъде разкрита.

Вижда се, че адресът на подателя не отговаря на куриерската фирма. По същия начин и URL адресът в линка от бутона „Платете сега“ води до страница „web.app“, което не е каквото се очаква.

Отделно би било редно и да се запитаме до колко е реалистично куриерът да се свързва с нас по имейл с искане за доплащане. Само по себе си това е крайно нетипично и съмнително.

ФИШИНГ КАМПАНИЯ КЪМ БЪЛГАРСКИ БАНКИ ОТ MTM.COM



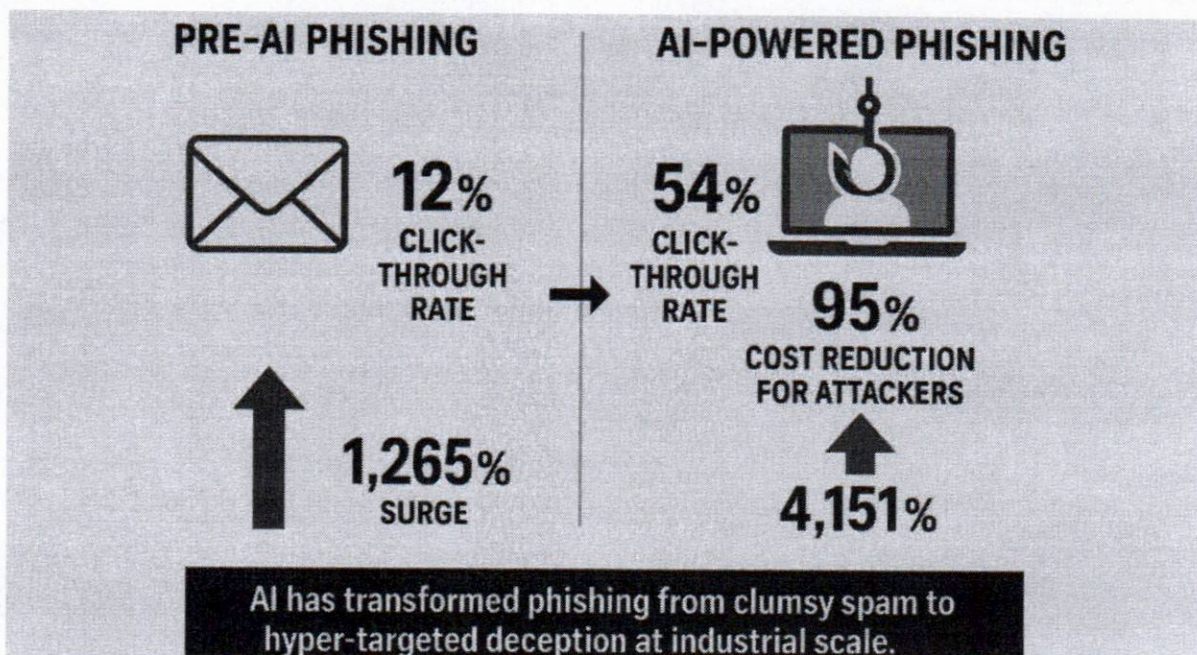
През изминалия месец попаднахме на фишинг кампания, насочена към редица български банки. Подателят е един и същ – mtm.com и във всеки имейл мнимите податели просто заменят заглавката „От“ с името на банката, за която искат да се представят.

Структурата на имейлите е сравнително проста – започват с картинка на логото на съответната банка, следва безлично обръщение като „Уважаеми клиент“ или изобщо липсва обръщение, след което подмамват получателите да последват посочения линк с манипулативна информация за актуализация или несъществуващ проблем.

Линковете, макар и различни на пръв поглед, водят до една и съща фалшива страница на представената банка. Променя се единствено логото в съответствие с това от кой линк е извикана страницата. Страницата има за цел да подведе жертвите на фишинг кампанията да въведат своите данни за вход в интернет банкирането, мислейки си, че се вписват в истинската страница на своята банка.

След първоначалното въвеждане на входните данни линкът се пренасочва към истинската страница на банката, където повторното въвеждане на данните да бъде успешно.

ОТ ЛОША ГРАМАТИКА КЪМ ФИШИНГ С ИЗКУСТВЕН ИНТЕЛЕКТ

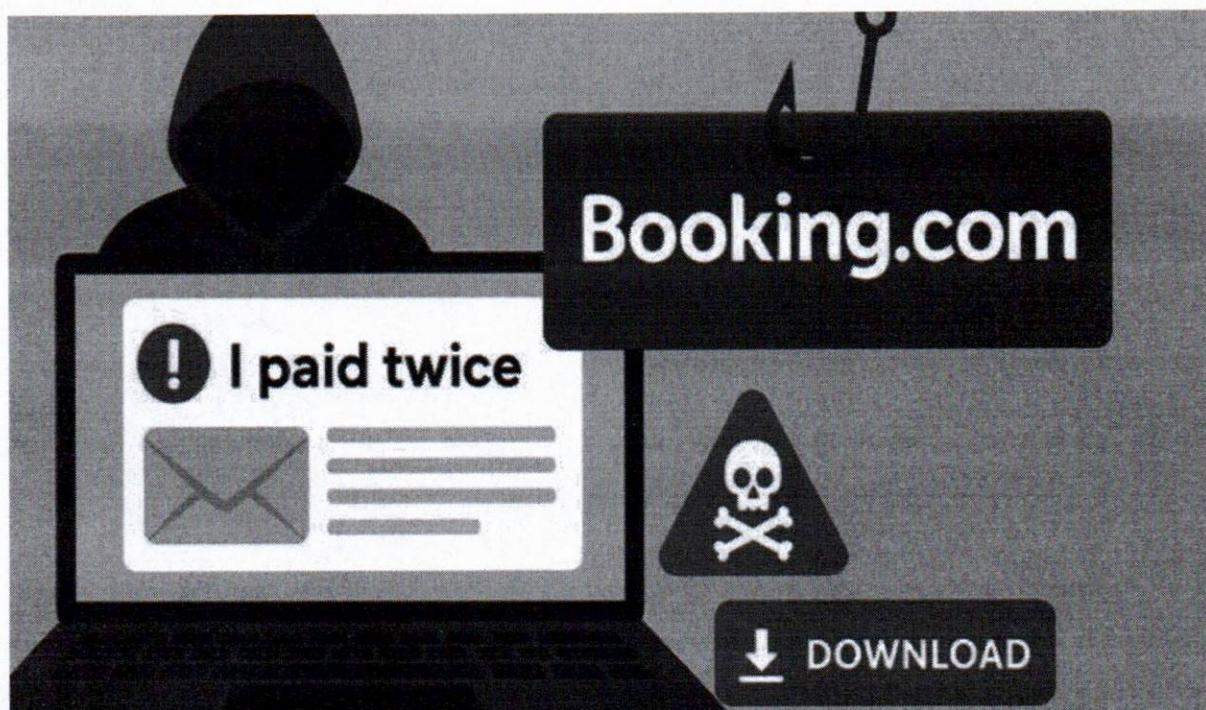


Фишингът остава една от най-разпространените и опасни тактики в киберпрестъпността, като често води до пробиви, финансови загуби и течове на данни. В България една от най-честите схеми – „Сменен IBAN“ – започва с фишингово съобщение, чрез което нападателите получават достъп до служебни имейли и подменят банкови данни в кореспонденцията. Днес фишингът вече не се ограничава до имейл – атаките се разпространяват чрез социални мрежи, търсачки и чат приложения.

Изкуственият интелект значително повишава качеството и мащаба на тези атаки. Лошата граматика вече не е признак за измама. AI създава безупречни, персонализирани съобщения, адаптирани към жертвата чрез данни от социални медии, изтекли бази данни и тъмната мрежа. Автоматизирани разговори имитират колеги или ръководители, докато deepfake гласове и видео надграждат убедителни телефонни обаждания и виртуални срещи, в които „мениджъри“ искат одобрение за преводи. LinkedIn също се превръща в удобен канал, тъй като корпоративните системи за сигурност рядко наблюдават директните съобщения там.

За защита се препоръчва внедряване на модерни решения за откриване на аномалии в поведението, устойчиви на фишинг методи за удостоверяване (включително биометрия и идентификационни данни, обвързани с устройство), обучение чрез симулирани атаки и принципи за достъп „нулево доверие“. Ключов извод: идентичността е най-ценната и най-уязвима цел, а само модернизирани стратегии могат да противодействат на вълната от AI-задвижвани заплахи.

CLICKFIX ФИШИНГ КАМПАНИЯ СРЕЩУ ХОТЕЛИ И ПОТРЕБИТЕЛИ

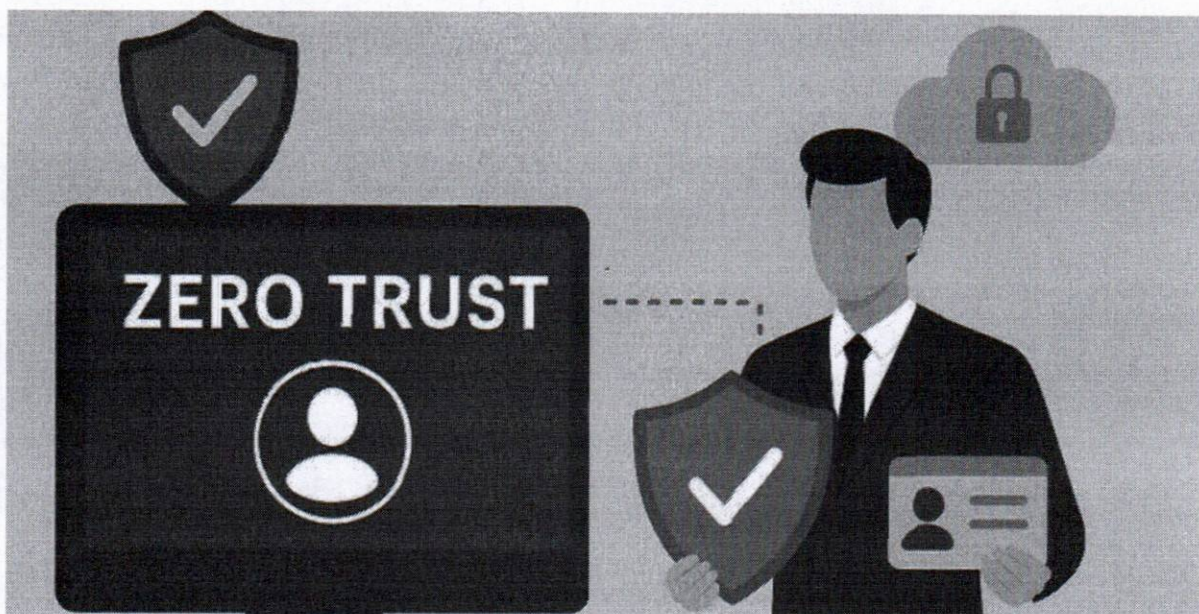


Киберкампания, насочена към хотелиерския сектор чрез атаки от типа ClickFix, довела до кражба на данни на множество клиенти. Кампанията, активна от пролетта до поне октомври 2025 г., използва компрометирани имейл акаунти на хотели, включително в Booking.com, както и съобщения в WhatsApp. Хакерите са разполагали с реални данни за клиенти и резервации, което е повишило достоверността на фишинг опитите.

Нападателите са използвали тактиката ClickFix, за да разпространяват зловерден софтуер за кражба на информация и за придобиване на идентификационни данни за платформи като Booking.com и Expedia. Събраните данни са били или продавани във форуми за киберпрестъпления, или използвани за директни измами. Открити са стотици активни зловердни домейни, поддържащи кампанията в продължение на месеци.

В много случаи хакерите изпращат съобщения от компрометирани хотелски акаунти, като понякога фалшифицират заглавката „От“, за да изглежда, че комуникацията идва от Booking.com. Темите включват резервации в последния момент или въпроси, свързани с гости, а линковете водят към пренасочвания, завършващи с ClickFix reCAPTCHA. Там потребителите са подмамени да копират PowerShell команда, която инсталира зловерден софтуер. Този софтуер събира чувствителна системна информация и изтегля допълнителни файлове, които активират инструмента за дистанционно управление PureRAT, позволяващ по-нататъшно проникване и контрол върху устройствата.

МОДЕЛЪТ НУЛЕВО ДОВЕРИЕ В КОРПОРАТИВНИТЕ МРЕЖИ

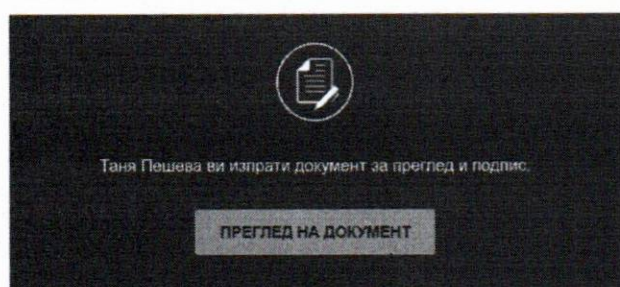
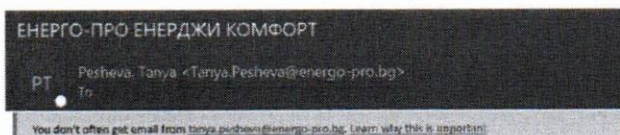


Моделът „нулево доверие“ представлява съвременен подход към киберсигурността, който отхвърля предположението, че вътрешната мрежа е по природа надеждна. Вместо еднократна проверка на входа, както при традиционния „замък и ров“, нулевото доверие изисква непрекъснато валидиране на идентичността, контекста и риска преди достъп до всеки ресурс. По аналогия с летищата, потребителят трябва да доказва кой е на всеки етап, а наблюдението за подозрителна активност е постоянно.

Подходът не е бързо или евтино решение – изисква преосмисляне на архитектурата, значителни ресурси и ясно дефиниране на рисковете. Организациите трябва да решат дали нулевото доверие е оправдано за тях или дали по-целенасочени мерки могат да дадат подобен ефект. Тенденции като дистанционната работа, облачните среди, сложните кибератаки и нормативните изисквания допълнително засилват нуждата от такъв модел.

С навлизането на AI рискът се увеличава, тъй като езиковите модели могат да бъдат манипулирани чрез недоверени данни. Това позволява атаки, които заобикалят филтри и защитни бариери. Затова защитата на AI трябва да следва вече познатите принципи на киберсигурността: проследяване на потока на данните, анализ на източниците и консуматорите, и разглеждане на моделите като потенциални „злонамерени играчи“. Ключово е и сегментирането – модели с високо доверие никога не трябва да бъдат изложени на недоверени входове. Нулевото доверие се основава на няколко основни принципа: силно управление на достъпа (IAM) и многофакторно удостоверяване, микросегментация за ограничаване на страничното движение, принцип на най-малките привилегии, непрекъснато наблюдение чрез IDS, SIEM и анализ на поведението, както и строга сигурност на всички устройства.

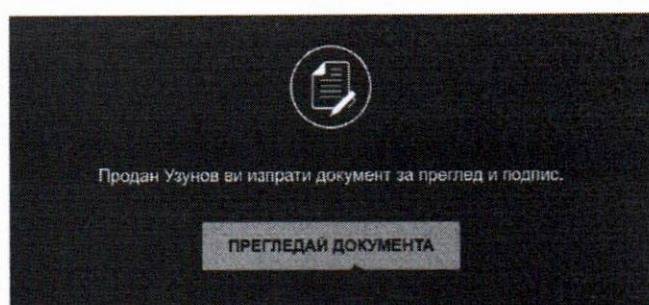
ВНИМАНИЕ! ИЗМАМНИЦИ СЕ ПРЕДСТАВЯТ ЗА ЕНЕРГО-ПРО И ТОПЛОФИКАЦИЯ СОФИЯ



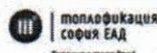
Tanya Pesheva
Regional Sales Director
Regions West and South Bulgaria

+359 885 119 610
tanya.pesheva@energo-pro.bg
www.energo-pro-energy-services.bg
2 Positano sq. | 1000 Sofia, Bulgaria
ENERGO-PRO Energy Services EAD

Original URL: <https://energopro.carrrd.co/>
Click or tap to follow link.



Продан Узунов
Ръководител отдел
Отдел "Производство на топлинна и електрическа енергия"
Дирекция "Експлоатационна дейност"
Т: +359 2 903 3213
М: +359 879 123 062
E-mail: p.uzunov@toplo.bg
Web: <http://www.toplo.bg>
Facebook: <https://www.facebook.com/www.toplo.bg>



Original URL: <https://toplobg.carrrd.co/>
Click or tap to follow link.

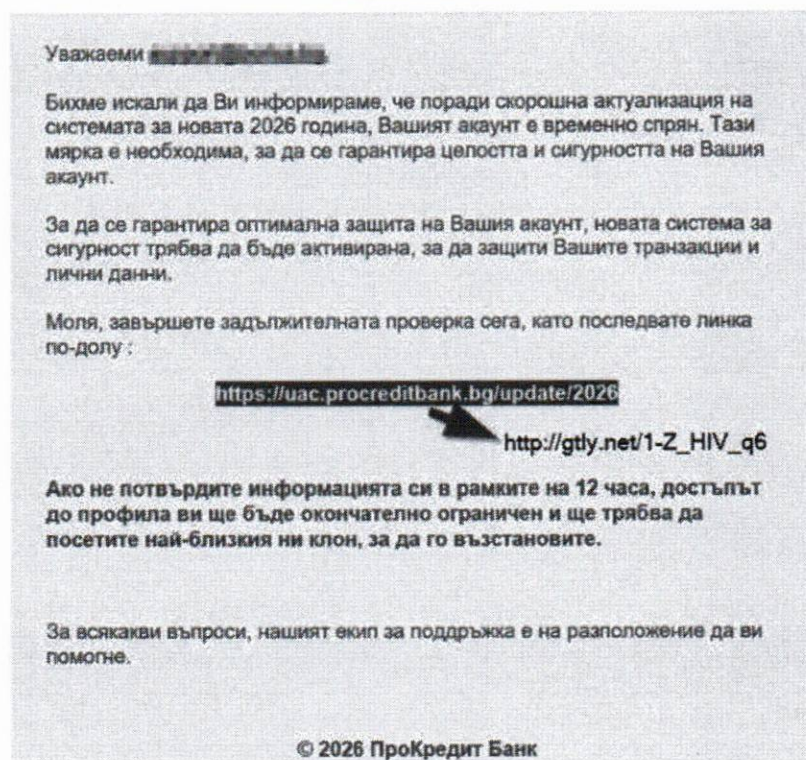
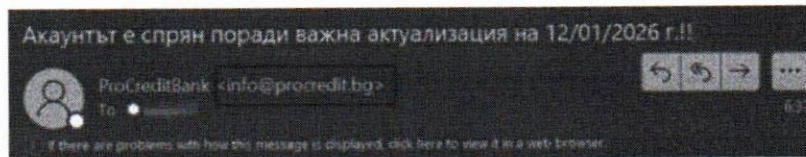
На картинките по-горе са показани два актуални фишинг имейла, които получихме с претенцията, че се изпращат от Енерго-Про и Топлофикация.

Видимо двата имейла следват еднакъв модел и зад тях стои един и същ човек, който чрез промяна на логото на имитираната компания се опитва да обхване по-широк кръг от потенциални жертви.

Измамата в тези имейли може да се разпознае по URL адреса. И в двата имейла линкът сочи към сайт с адрес "carrrd.co". Думите отпред „energopro“ и „toplobg“ умело прикриват действителния адрес.

Проверката ни показва, че този сайт е създаден съвсем скоро и е защитен със SSL сертификат, валиден за 3 месеца. Интересен момент в тази измама са адресите на подателите. В единия случай това е „energopro.bg“, а в другия – „toplo.bg“. Анализът на хедърите показва, че тези адреси не са подправени, което навежда на мисълта, че пощенските сървъри на тези компании може да са компрометирани и някой с нерегламентиран достъп да изпраща фишинг имейли от тях.

УМЕЛ ФИШИНГ ИМЕЙЛ ОТ ИМЕТО НА ПРОКРЕДИТ БАНК



Показвали сме ви множество фишинг имейли, имитиращи съобщения от банки. Всички те, повече или по-малко, съдържат типичните белези на фишинг измамата. И този не прави изключение, но ни направи впечатление адресът, от който е изпратен – info@procredit.bg.

Достатъчно близко до истинския за да изглежда достоверен, но все пак различен от легитимния домейн на банката – а именно „procreditbank.bg“.

Следва типичното обръщение по имейл адрес вместо по име. В допълнение, линкът от червения адрес в бутона умело прикрива действителната страница „gtly.net“. Следва допълнителен червен флаг – ултимативното изречение накрая, че достъпът ще бъде ограничен след 12 часа.

Всички тези белези са лесно разпознаваеми. Достатъчно е да знаем, че трябва да ги проверим.

META VERIFIED ОФИЦИАЛНА ПОКАНА ОТ META

Официална покана от Meta – Получете синята значка

MP Meta Platform <support@meta-business@fb.com>
To: @business

Официална покана от Meta – Получете синята значка

Уважаеми потребителю,

Вашата бизнес страница или профил е избран/а като подходящ/а за **Meta Verified** (синята значка).

Meta Verified е официалната програма за верификация на Meta. Тя потвърждава автентичността на вашия бизнес във Facebook и Instagram и повишава доверието на клиентите.

👉 За да получите синята значка, моля, завършете заявката за верификация до 24 часа след получаване на това съобщение чрез официалния линк по-долу.

<https://rebrand.ly/b1c399>
Click or tap to follow link.

👉 Верифицирайте своя акаунт тук: <https://www.facebook.com/meta-verified>

🌟 **Предимства на Meta верификацията**

- Показване на официалната синя значка
- Повече доверие и надеждност
- Защита срещу фалшиви акаунти и злоупотреба с самоличност
- Приоритетна поддръжка от Meta
- По-професионален външен вид в социалните мрежи

Акаунти, които отговарят на следните условия, получават предимство:

- Истински, проверени и легитимни бизнес
- Точна и актуална бизнес информация
- Редовна активност и спазване на правилата на Meta

С уважение,
Екипът на Meta Platforms

Meta Verified: Потвърдете самоличността си, за да получите синия верификационен знак

MF Meta For Business <9423kangel@rebrand.ly>
To: support

👉 Reply 👤 Reply All ➔ Forward ⋮

st 22.11.2023 12:40

🔔 Bank use problem, with this message is displayed. click here to view R in a web browser.

Уважаеми Администратор,

Вашата Бизнес Страница ✓
Готова за верификация

ID на страницата: 987654321098765

Проверете данните си, за да получите синия знак

Вашата страница е квалифицирана за официален син верификационен знак. Завършете процеса по верификация, за да потвърдите автентичността си и да получите знака.

Какво ви е необходимо за верификация:

1. Официални бизнес документи
2. Документ за самоличност на администратора
3. Уебсайт на компанията или друго онлайн присъствие

Original URL:
<https://rebrand.ly/pageverifs>
Click or tap to follow link.

ЗАПОЧНЕТЕ ВЕРИФИКАЦИЯТА

И Facebook, по подобие на X (Twitter), предлагат допълнително „тикче“ веднага след името на профила, което очаквано веднага беше използвано във фишинг кампании, възползващи се от така наречения „hype“. Подмамвайки потребителите с възторженото „вашият профил е избран“, измамниците се стремят да получат вашите данни за достъп. Потенциално и вашите данни от кредитната карта.

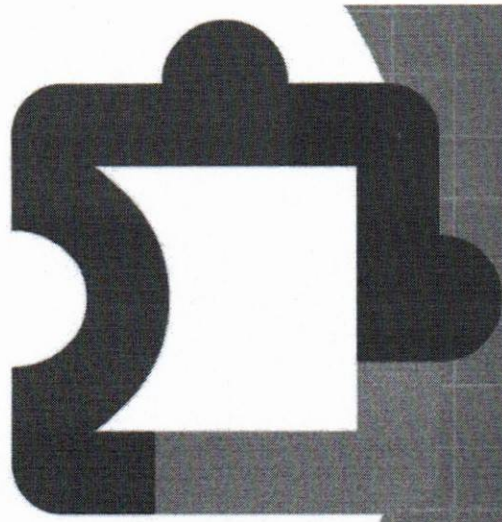
Засякохме няколко такива опита. Някои си приличат, други са напълно различни, но всички от различни податели и водещи до различни фалшиви страници, както се вижда от примерите.

При този тип измами трябва да знаем най-напред, че комуникацията между социална мрежа и вас би следвало да се провежда вътре в центъра за известия на самата платформа, а не по имейл. Не е типично, също така, платформата да ви изпраща линкове по имейл. А когато линкът и подателят не отговарят на очакваното, то имате всички основания да смятате, че полученият имейл е измамен.

В показаните примери се виждат въпросните типични белези на фишинг имейл. Неочакван имейл от Meta, но адресът на подателя е различен. Обръщението не е поименно. Текстът описва синия знак, но не го показва като картинка, за да не бъде засечен от защитните филтри на пощенските сървъри. Предлага се линк, но URL адресът води до различно място. В допълнение присъства и ултимативен изказ „завършете заявката за верификация до 24 часа“.

Обикновено е достатъчно наличието само на един от посочените белези, но тук имаме няколко, което ни дава допълнителна увереност, че тези имейли са измамни.

ВЪЗМОЖНО ЛИ Е РАЗШИРЕНИЯТА ЗА CHROME ДА ШПИОНИРАТ РАЗГОВОРИТЕ ВИ С ИЗКУСТВЕНИЯ ИНТЕЛЕКТ



Chrome Extension Spies on AI Chats

Киберексперти разкриха две зловредни разширения в Chrome Web Store, които са записвали разговори с ChatGPT и DeepSeek, както и данни за браузването, от над 900 000 потребители. Разширенията се представят като инструменти за работа с различни AI модели, но всъщност тайно изпращат съдържанието на чатове и URL адреси на отворени страници към сървъри, контролирани от нападателите. Тази практика е наречена „Prompt Poaching“ – кражба на AI заявки.

След инсталиране разширенията искат разрешение за събиране на „анонимни аналитични данни“, но реално извличат пълните разговори с AI чат ботове чрез анализ на елементи от уеб страниците. Данните се съхраняват локално и периодично се изпращат към външни домейни. За да прикрият дейността си, извършителите използват легитимно изглеждаща инфраструктура и AI платформи за хостване на политики за поверителност.

Освен зловредни разширения, изследователи установяват, че и легитимни разширения с милиони потребители, като Similarweb и Stayfocusd, също събират AI разговори, като това е описано в актуализираните им условия за ползване и политики за поверителност. Експертите предупреждават, че тази тенденция тепърва ще се разраства, тъй като подобни данни имат висока търговска стойност.

Потребителите се съветват да премахнат съмнителните разширения, да бъдат внимателни с разрешенията, които дават и да избягват инсталирането на инструменти от непознати източници, дори когато изглеждат официално препоръчани.

МНИМИ ПРОМОЦИОНАЛНИ СТРИЙМИНГ АБОНАМЕНТИ



Измамите със стрийминг абонаменти са все по-често срещани, особено сред потребители, търсещи евтино забавление. В т.нар. Dark Net често се появяват оферти като „доживотен Netflix Premium“ за няколко долара или пакетни абонаменти за популярни платформи на символични цени. Макар да изглеждат професионално оформени и надеждни, тези „онлайн магазини“ всъщност се основават на кражба на акаунти, злоупотреби с кредитни карти и измами.

Разследванията показват, че стрийминг акаунтите са сред най-търгуваните дигитални стоки в подземните пазари. Причината е проста – те се придобиват лесно чрез фишинг атаки, повторно използване на пароли и т.нар. credential stuffing, търсени са от широк кръг хора и могат да се препродават масово. В тези пазари акаунти за Netflix, HBO, Disney+ и други често се продават за между 5 и 15 долара, а понякога дори за под 3 долара – цена, която сама по себе си е сериозен сигнал за измама.

Често акаунтите са създадени или платени с компрометирани кредитни карти, което означава, че достъпът на купувача е временен или напълно неработещ. Обещанията за „доживотни“ абонаменти са напълно нереалистични, тъй като подобни услуги не съществуват легално. В много случаи достъпът се прекратява след дни, когато реалният собственик възстанови паролата си или платформата засече измамата.

Експертите предупреждават, че купувачите на такива оферти не само губят пари, но и неволно стават част от по-големи схеми за пране на пари и киберпрестъпления. Затова основният съвет е ясен: прекалено евтините и „вечни“ стрийминг абонаменти почти винаги са измама и трябва да бъдат избягвани.

ИЗМАМИ С КРИПТОВАЛУТИ С ПОМОЩТА НА AI



Европейските финансови регулатори предупреждават за рязко нарастване на измамите с криптовалюти, подпомагани от изкуствен интелект, които стават все по-трудни за разпознаване. В съвместно изявление Европейските надзорни органи (EBA, ESMA и EIOPA) посочват, че измамниците все по-често комбинират крипто схеми с AI технологии – от фалшиви инвестиционни платформи до deepfake видеа и гласове, имитиращи известни личности, институции или дори близки хора.

Според регулаторите изкуственият интелект значително повишава ефективността на тези измами. Чрез него престъпниците могат да създават убедителни фалшиви препоръки, да имитират банки и регулатори, да изграждат професионално изглеждащи фишинг сайтове и да автоматизират разговори, които се адаптират в реално време към реакциите на жертвата. Тези техники се използват широко при инвестиционни, романтични и имитационни измами, като целта е жертвите да бъдат подтикнати да изпратят криптовалута или да разкрият чувствителни данни.

Допълнителен риск е фактът, че криптотранзакциите са трудни за проследяване и обикновено необратими, което прави възстановяването на загубените средства почти невъзможно. Затова регулаторите обръщат внимание на ключови предупредителни сигнали: непоискани оферти с „гарантирана“ печалба, натиск за бързи и тайни действия, прехвърляне на разговори към криптирани приложения, линкове към непознати платформи и искания за лични ключове или идентификационни данни. Ако една оферта изглежда прекалено добра, спешна или потайна, най-вероятно става дума за измама.



ОНЛАЙН БАНКИРАНЕТО ПОД ПРИЦЕЛ ЗА ПОРЕДЕН МЕСЕЦ

Сигурност Известие – Информация за вашата сметка • Ref 1009680

F.I.B.A.N.K <info-f447@reise-fotos.de>
To • Central Office 22.10.2025

Отдел по сигурността
Служебно известие за сигурност

Известие за сигурност Дата: 22/10/2025

СИГУРНОСТ

Необходимо е потвърждение, за да продължите

Уважаеми/а клиент,

Регистрирахме необичайна активност, свързана с вашия профил. По съображения за сигурност достъпът може да бъде временно ограничен.

Необходимо е действие: За да възстановите пълния достъп до профила си, потвърдете самоличността си чрез официалния канал възможно най-скоро.

URL: https://eternitytime.events/home_en/

Официален адрес (в случай че бутонът не работи):
<https://www.verification.myfibaank/security>

Отворете страницата за сигурност

Внимание: Имате 24 часа, за да завършите това потвърждение. Ако потвърждението не бъде извършено навреме, достъпът до вашата сметка може да бъде прекратен.

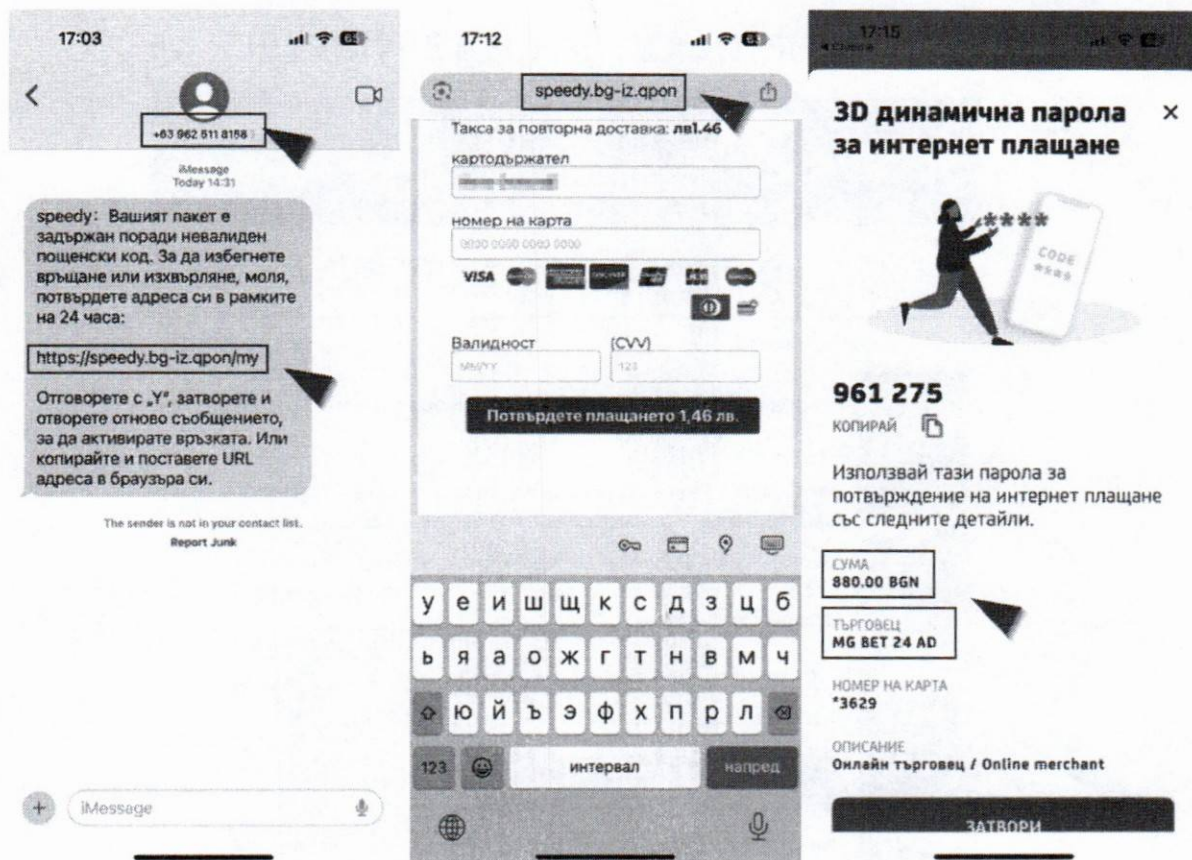
Това е автоматично съобщение. Моля, не отговаряйте директно на този имейл.
Отдел по сигурността — ул. Пример 1, София, 1000, България

Разпознаването на белезите на фишинг измамен имейл е лесно! Нужно е единствено да погледнете повторно.

На примера от този месец първоначално впечатление правят логото на банка, думите „сигурност“, „потвърждение“, „внимание“, „евентуално“ и „действие“.

Ако не избързате да кликнете веднага, а вместо това проверите адреса на получателя и адреса на линка от бутона, ще откриете видимото несъответствие с банката и нейните разпознаваеми адреси. На второ място остават вторичните белези като например несъответствието между търсеното потвърждение и необичайната активност, а именно как потвърждавайки самоличността си ще направите активността по-малко необичайна.

ВНИМАНИЕ! ДЕЙСТВАЩА ФИШИНГ ИЗМАМА ЗА ЗАДЪРЖАНА ПРАТКА ОТ SPEEDY



Засякохме опасна активна фишинг измама от името на куриерска фирма с претекст, че пратката ви е задържана поради невалиден пощенски код или сгрешен адрес.

На първата картинка е показано SMS съобщение, чийто автор се представя като "speedy:" На втори прочит се вижда номерът, от който е изпратено съобщението. Кодът +63 едва ли е от Спиди.

На втората картинка стигаме до линка. URL адресите се разглеждат отзад напред. Bg-iz.qpon е активният адрес, откъдето се зарежда страницата за плащане. Всичко преди това е за заблуда. На тази фалшива страница измамниците събират данните за картата и ги използват за нареждане на превод към сметката на търговец "MG BET 24 AD".

На третата стъпка се получава динамичен код от банкирането с важна информация за предстоящия превод. Ако не обърнете внимание на променената сума и търговеца, и потвърдите трансакцията, паричният превод се изпълнява, при това с ваше съдействие.

ИЗМАМЕН ИМЕЙЛ С ЛОГОТО И ИМЕТО НА ЕКОНТ



ЕКОНТ

Здравейте,

Има изпратена до Вас пратка с N:1054955369490, доставена на 02.09.2025г. в офис Велико Търново, ул. Полтава № 3Ж, тел: +359 62 810 487.

Очакваме Ви в офиса за получаване на пратката до 11.09.2025г.

Ако не потърсите пратката си в рамките на 7 работни дни от пристигането ѝ в офиса, тя ще бъде върната към подателя.

Пратката е с тегло: 1.000 кг., Номер на поръчка: 160, Описание на поръчка: Бонбони за растежа (3а 60 Дена)

Дължимата сума: 57,34 лв / 29,32 €.

Можем да ги съхраним за по-дълъг период срещу такса от 6,26 лв. с ДДС на ден, след съгласие от подател.

Може да проследите, да платите пратката си и да промените всяко условие на доставка [ТУК](#)

С уважение,

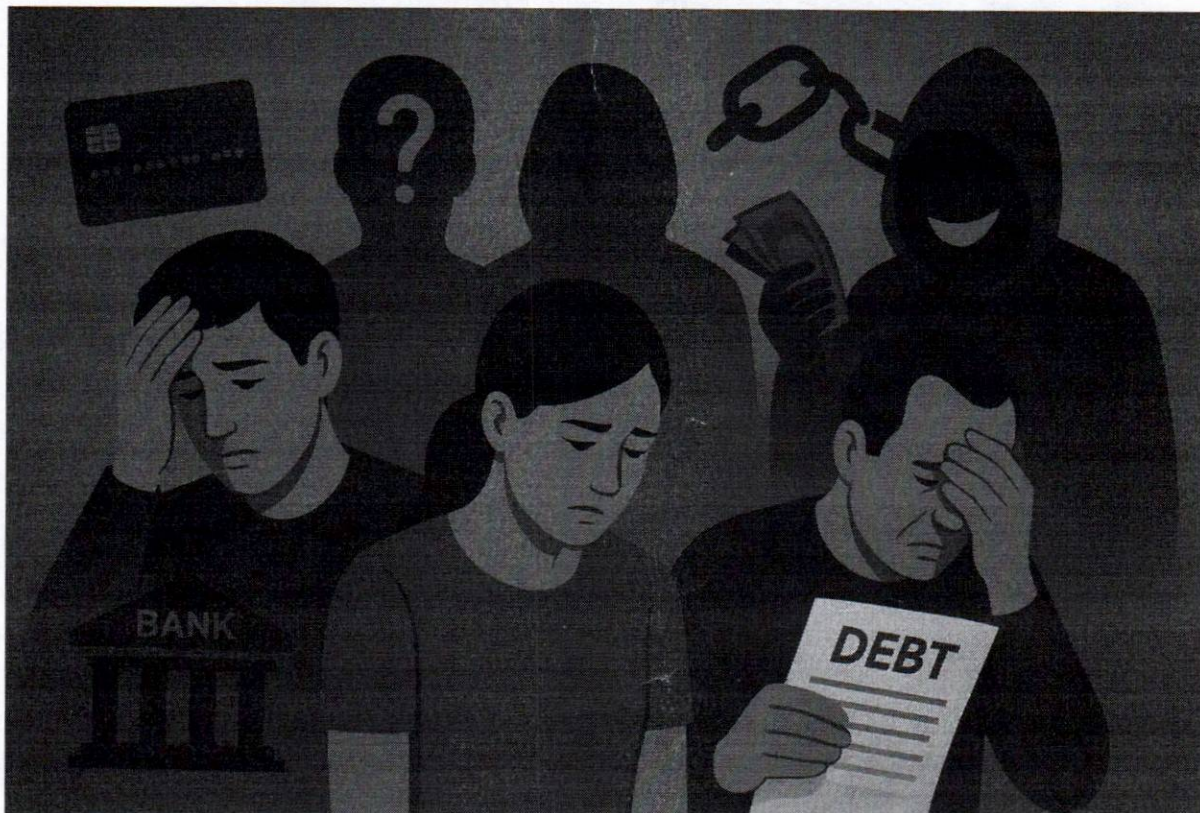
Еконт

Original URL:
<https://netingsending.netlify.app/>

Фишинг измамите с известия от куриерски компании запазват водещо място за пореден месец. От една страна онлайн пазаруването е нещо обичайно и статистически е много вероятно в този момент и вие да очаквате някаква пратка. От друга страна Еконт е сред най-големите куриерски компании в страната и не е изненадващо името и да бъде използвано в подобни опити за измама.

Както всеки друг фишинг имейл и този би могъл да се разпознае с проверка на подател и линк. Адресът на подателя се различава от очаквания за Еконт. В конкретния случай дори не си приличат. По същия начин и линкът показва URL адрес, различен от очаквания.

ОПАСНА ИЗМАМА С „ФИКТИВНИ“ КРЕДИТИ В БЪЛГАРИЯ

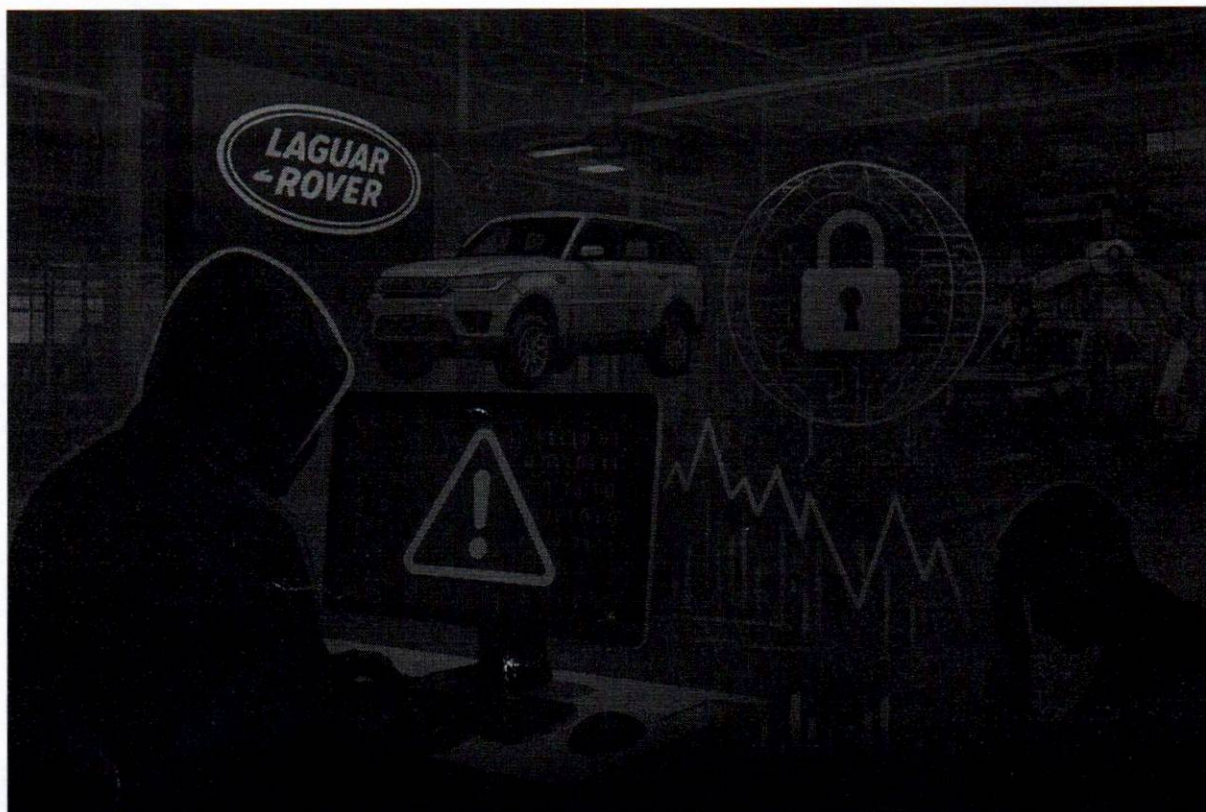


Схемата с т. нар. „фиктивни“ кредити е отново активна. За това разказват потърпевши след като са били подвеждани да изтеглят няколко бързи кредита с обещание за комисионна и договор за работа.

Измамниците в схемата се представят за консултанти в международна кредитна компания, които набирали персонал. Освен стандартния договор за работа те предлагали и „скрита“ схема за бърз старт на новите служители с голям процент комисионна от всеки нов кредит. Обещанието било новият служител да изтегли няколко кредита, за които да получи комисионна и допълнителен процент над договорената заплата, а фирмата да погаси кредитите им на следващия ден. По този начин заплата се увеличавала за всеки изтеглен кредит.

Подмамени от идеята за натрупване на по-голям процент над заплата след всеки усвоен кредит, жертвите бързали да минат през няколко кредитни компании и банки. Условието било това да се случи в един ден, за да се избегне отказ. След като съберат парите, жертвите ги предавали на мнимите служители, които им обещавали, че ще погасят всички вноски от тяхно име много скоро, а към договора им за работа щели да се натрупат нови допълнителни проценти. След като парите от кредитите били предадени, консултантите прекратявали всякаква комуникация с измамените „нови“ служители, а подписаните договори се оказвало, че били с фиктивни дружества и фиктивни данни. Изтеглените кредити, обаче, оставали реалност.

КИБЕРАТАКА СРЕЩУ JAGUAR LAND ROVER



Кибератаката срещу Jaguar Land Rover разклаща британската икономика.

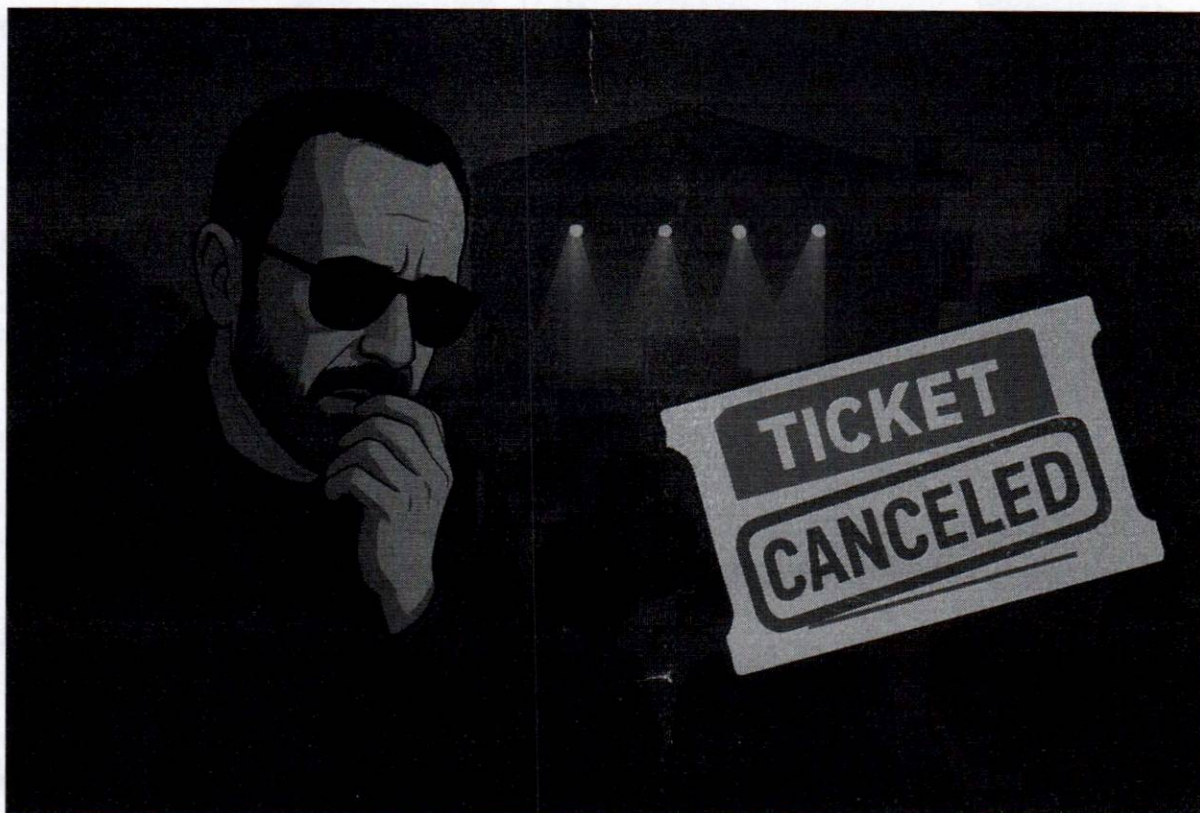
Масщабна кибератака срещу автомобилния гигант Jaguar Land Rover (JLR) през август 2025 г. е довела до щети от над 1.9 млрд. паунда, което я прави едно от най-вредните киберсъбития в историята на Обединеното кралство, според Британския център за кибермониторинг (СМС).

Инцидентът парализира вътрешните ИТ системи и производствените линии на JLR в заводите в Солихъл, Хейлууд и Уулвърхамптън, като спря напълно производството за седмици. Последниците засегнаха над 5000 свързани компании, включително доставчици и дилъри.

През септември във Великобритания са произведени с 27% по-малко автомобили, като JLR не е произвела нито един. Това е най-ниското ниво на производство от 1952 г. насам. Според експертите, атаката е показала колко уязвими са интегрираните вериги за доставки, тъй като сривът в един производител може да предизвика каскадни икономически ефекти.

СМС предупреждава, че системните киберрискове трябва да се разглеждат като заразни явления, които могат да се разпространят чрез споделена ИТ инфраструктура и да засегнат цели сектори. Макар и без преки жертви, атаката е нанесла тежки социално-икономически щети, включително загуба на работни места и засилване на регионалните неравенства.

ФАЛШИВ КОНЦЕРТ НА МИЛЕ КИТИЧ И СТОТИЦИ ИЗМАМАЕНИ



Стотици почитатели на сръбската звезда Миле Китич станаха жертва на измама с несъществуващ концерт в Габрово. Събитието, обявено за 10 октомври в спортна зала „Орловец“, било рекламирано широко в социалните мрежи и местните медии. Фенове купували билети по 60 лв. през платформата EraGo, убедени, че ще видят любимия си изпълнител.

В деня на концерта обаче залата била заключена, а по-късно се оказало, че никога не е имало сключен договор за събитието. Самият Миле Китич публикувал видео, в което предупредил феновете, че това е измама и той не е имал участие в организацията. Реалният му концерт по същото време се състоял в Горна Оряховица.

Зад фалшивото събитие стои фирма „Глобал Трансфер Сървиз“, регистрирана в София, чиито представители обещали връщане на парите, но до момента никой не е получил възстановяване.

Случаят е предаден на Комисията за защита на потребителите и прокуратурата в Габрово, а икономическата полиция вече извършва проверка. Измамените може да са до 2000 души, тъй като капацитетът на залата е 1800 места.



ОСНОВНО УЧИЛИЩЕ „ЛЮБЕН КАРАВЕЛОВ“ С. ТРУДОВЕЦ

ПОКАНА

ДО ПЕДАГОГИЧЕСКИТЕ СПЕЦИАЛИСТИ НА

ОУ „ЛЮБЕН КАРАВЕЛОВ“ С. ТРУДОВЕЦ

Уважаеми колеги,

Най-учтиво Ви каним на организирана вътрешноинституционна квалификация . Тя ще се проведе при следните условия:

Дата: 02.02.2026г.

Място: Учителска стая на ОУ „Любен Каравелов“ с. Трудовец

Тема: „ Киберсигурност “

Провеждащ квалификацията: Нина Иванова

№ по ред	Име и фамилия	Заемана длъжност	Подпис на лицето
1	Ивелина Веселинова Михайлова	Старши учител, НЕ	
2	Нина Емилова Иванова	Старши учител, НЕ	
3	Мариана Иванова Георгиева	Старши учител, НЕ	
4	Величка Вълчева Минковска	Учител, ПЕ	
5	Преслава Маринова Денкова	Учител, ПЕ	
6	Наталия Иванова	Старши учител, ПЕ	
7	Цонка Иванова Филипова	Старши учител, ПЕ	
8	Наталия Радкова Василева	Старши учител, НЕ в ЦОУД	
9	Лидия Цветкова Христова	Старши учител, ПЕ	
10	Весела Иванова Павлова	Учител, ПЕ в ЦОУД	
11	Илияна Георгиева Йошовска	учител, ПЕ	
12	Ема Ивайлова Николова	Учител, НЕ в ЦОУД	
13	Петя Пламенова Семкова	Учител, НЕ	
14	Габриела Цветанова Дишкова	Учител, НЕ	
15	Стефка Иванова	Учител, НЕ в ЦОУД	
16	Йонка Василева	ЗД УД	
17	Илияна Марчовска	Директор	

Карта за участие във вътрешноинституционална квалификация

Основно училище „Любен Каравелов“ с. Трудовец

Карта

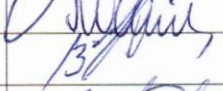
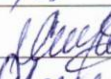
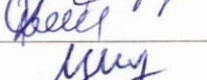
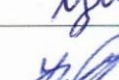
за отчитане на вътрешноинституционална квалификация за учебната 2025/2026 година

Тема на квалификационната форма/наименование на програмата за обучение:	„Киберсигурност“
Организационна форма на предлаганата квалификация:	Присъствена
Дата на провеждане:	02.02.2026г.
Място на провеждане:	Учителска стая
Време на провеждане в академични часове и минути:	Начален час: 08:30 ч.
	Краен час: 12:30 ч.
	Общо времетраене на формата: 225 мин. /5 квалификационни часа/
Работни материали:	• работни листа
Място, където се съхранява пакета документация от проведената квалификация:	Класъор за вътрешноинституционална квалификация за учебната 2025/2026 година
Ръководител/отговорник за провеждането на квалификацията	Нина Иванова
Участници – общ брой от тях:	17 участници

Приложение: Списък на участниците в квалификационната форма

Карта за участие във вътрешноинституционална квалификация

Приложение: Списък на участниците в квалификационната форма

№ по ред	Име и фамилия	Заемана длъжност	Подпис на лицето
1	Ивелина Веселинова Михайлова	Старши учител, НЕ	
2	Нина Емилова Иванова	Старши учител, НЕ	
3	Мариана Иванова Георгиева	Старши учител, НЕ	
4	Величка Вълчева Минковска	Учител, ПЕ	
5	Преслава Маринова Денкова	Учител, ПЕ	
6	Наталия Иванова	Старши учител, ПЕ	
7	Цонка Иванова Филипова	Старши учител, ПЕ	
8	Наталия Радкова Василева	Старши учител, НЕ в ЦОУД	
9	Лидия Цветкова Христова	Старши учител, ПЕ	
10	Весела Иванова Павлова	Учител, ПЕ в ЦОУД	
11	Илияна Георгиева Йошовска	учител, ПЕ	
12	Ема Ивайлова Николова	Учител, НЕ в ЦОУД	
13	Петя Пламенова Семкова	Учител, НЕ	
14	Габриела Цветанова Дишкова	Учител, НЕ	
15	Стефка Иванова	Учител, НЕ в ЦОУД	
16	Йонка Василева	ЗД УД	
17	Илияна Марчовска	Директор	