



Safer Internet Day 2026

**ИНФОГРАФИКИ НА ГРУПИ ОТ 8-11 КЛАС
ИЗГОТВЕНИ В ЧАСОВЕТЕ ПО ИТ**

Анатомия на онлайн измамата: „Скуатинг“



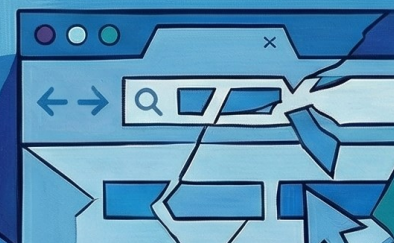
Какво е „Скуатинг“?

Техника, при която се използват имена, наподобяващи популярни платформи, за въвеждане в заблуда.



Психологически трик: Спешност

Фрази като „Само днес!“ целят да предизвикат прибързани действия без обмисляне.



Грешно изписване: „Facebok-Market“

Липсваща буква в името на известна марка в сигурен знак за злонамерен сайт.



Провери преди да кликнеш

Винаги проверявайте легитимността на домейна в адресната лента, преди да въведете данни.



Общ подател

Използването на неясно име като „Reklama“ е типичен белег за автоматизирана измамна кампания.

Фишинг капан: Анатомия на измамата с Netflix

Елементи на фишинг съобщението



Фалшив подател "Netflix"

Измамниците изполават името на популярни услуги, за да спечелят незабавно доверие.



Психологически натиск за плащане

Съобщението твърди, че абонаментът е спрял поради проблем, за да предизвика паника.

Механизъм на измамата

ЛИНК

Призив за действие чрез линк

Изисква се кликане върху външна връзка за "повторно активиране" на профила.



Кражба на картови данни

Крайната цел е потребителят сам да въведе данните от банковата си карта.

Как да разпознаем “Спуфинг” атака?

КОМПОНЕНТИ НА ИЗМАМАТА



Вид: “Спуфинг”

Техника за маскиране на комуникация от неизвестен източник като доверена и позната.



Фалшив подател

Използва се адресът “admin@tvoeto-daskalo.bg”, за да се създаде илюзия за легитимност.

ЧЕРВЕНИ ФЛАГОВЕ В СЪОБЩЕНИЕТО



Фалшива спешност

Твърдението за “технически проблем” цели да предизвика бърза и недомислена реакция.



Опасната стъпка: Потвърждение

Изискването на вход в системата чрез предоставен външен линк е сигурен белег за измама.



Anatomy of a Typosquatting Scam

IDENTIFYING THE SQUATTING TECHNIQUE



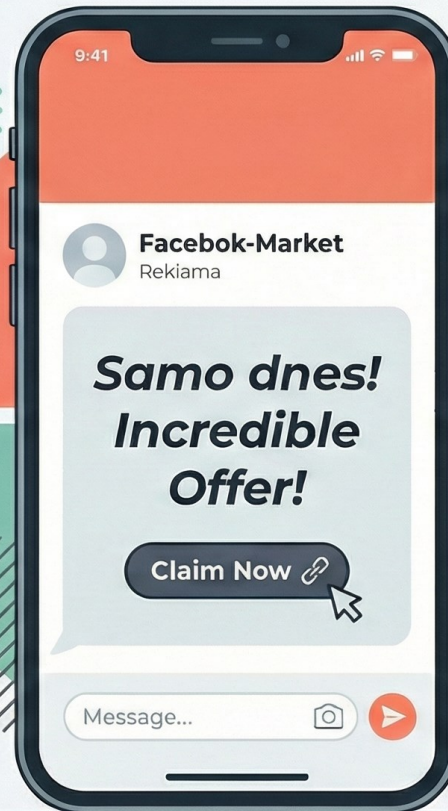
Domain Typosquatting

Attackers use slight misspellings of famous brands, like 'Facebok-Market', to deceive users.



Deceptive Sender Aliases

The use of a generic sender name like 'Reklama' (Advertisement) masks the true source.



PSYCHOLOGICAL RED FLAGS



The Urgency Trap

Using 'Samo dnes' (Only today!) creates false pressure to bypass critical thinking.



Malicious Call-to-Action

Fraudulent messages pair 'incredible' offers with direct links to steal credentials or data.



Анатомия на Смишинг Измама: Как да не станете жертва

Какво е „Смишинг“?

Фишинг атака, проведена чрез текстово съобщение (SMS), целяща кражба на лична информация.



Изкуствена спешност (30 минути)

Поставянето на кратък срок цели да провокира паника и необмислени действия.

Фалшив подател:
„BG-Post-Alert“

„Пратката Ви е
задържана...“

Измамниците използват имена, които имитират легитимни институции, за да спечелят доверие.

Опасната връзка
[link]

Кликването върху линка води до фишинг сайтове за събиране на адреси или банкови данни.

Анатомия на онлайн измамата: Как работи „Скуатингът“?

Този анализ разглежда конкретен пример за измамно съобщение (тип „скуатинг“), разпространявано чрез социалните мрежи. Инфографиката деконструира елементите на съобщението, за да покаже как хакерите използват визуални трикове и психологически натиск.

ПРИЗНАЦИ НА ИЗМАМАТА

Тип: „Скуатинг“ (Cybersquatting)

FACEBOOK

FACEBOOK

Злоупотреба с имена на известни марки чрез лека, незабележими промени в изписването.

Подвеждащ подател

Reklama

Използване на общи имена като „Reklama“, за да се прокрие реалната самаличност.

Умишлена правописна грешка

FACEBOOK

FACEBOOK

Използването на „Facebook“ вместо „Facebook“ е ясен сигнал за измамен уебсайт.

През измислените имена често се скрива истинската цел на измамника – измама.

Обещанието за нисък ценен пробив на гостната мрежа.

Използването на хвърляне на пари с плаващи селово налягане на хвърляне, улеснява дейността.

Звучието на „мисловен селово“ за да се убеди.

Промислите на „сложени елементи“ съобщения на призоваване към злобреден софтуер.

МЕХАНИЗЪМ НА КАПАНА

Фалшива спешност

САМО ДНЕС!

Фраза като „Само днес!“ целят да предизвикат паника и прибързано действие.

Опасни линкове

Обещанието за „невероятна промоция“ служи за примамка към злобреден софтуер.

ЗЛОБРЕДЕН СОФТУЕР

НЕВЕРОЯТНА ПРОМОЦИЯ

Анатомия на Смишинг Измама: Как да разпознаем измамните съобщения

Детайли на измамното съобщение



Вид: Смишинг

Фишинг атака, извършена чрез текстово съобщение (SMS) за кражба на лични данни.



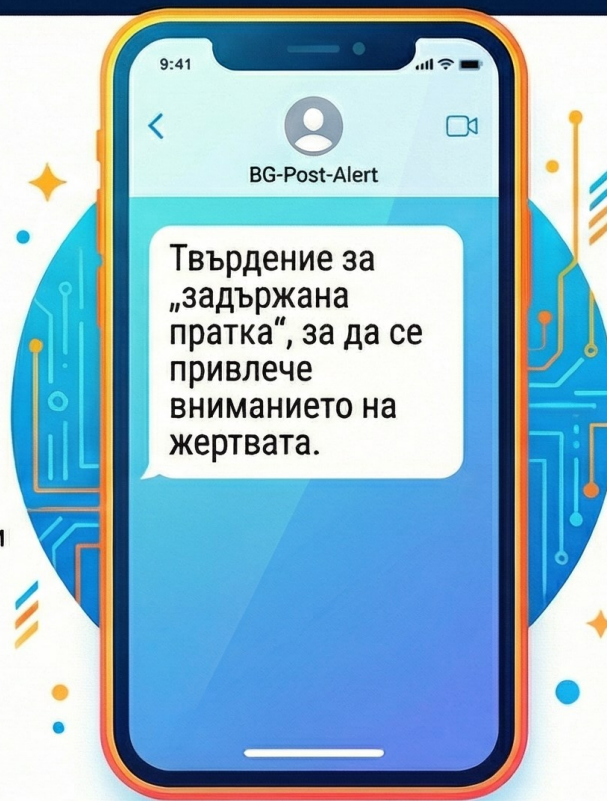
Подател: „BG-Post-Alert“

Измамниците използват имена, имитиращи легитимни институции като Български пощи.



Текст на съобщението

Твърдение за „задържана пратка“, за да се привлече вниманието на жертвата.



Критични червени флагове



Подозрителен линк

Изискване за кликане върху външна връзка за „потвърждение на адрес“.



Искуствена спешност

Поставяне на кратък срок (30 минути) за принуждаване към необмислени действия.



Подозрителен линк

Използване на страха, че пратката ще бъде върната на подателя.

Анатомия на измамата: Как да разпознаем „Смишинг“

Тази инфографика разглежда конкретен пример за фишинг атака чрез SMS (смишинг), маскирана като известие от пощенска услуга. Тя деконструира съобщението, за да покаже как измамниците използват фалшива самоличност и чувство за спешност, за да откраднат данни.

Анатомия на фалшивото съобщение



Подател: „BG-Post-Alert“

Използване на име, имитиращо официална институция, за да се спечели незабавно доверие.



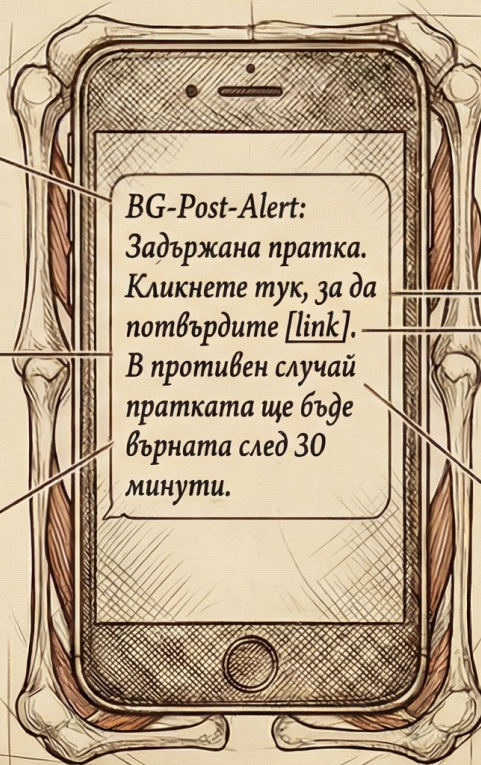
Вид: „Смишинг“

Фишинг атака, извършена чрез текстово съобщение (SMS) за подвеждане на потребителя.



Твърдение за задържана пратка

Използване на ежедневен сценарий (получаване на колет), за да се привлече вниманието.

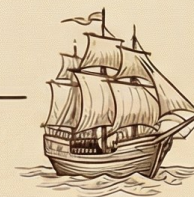


Психологически капани



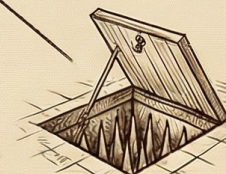
Създаване на изкуствена спешност

Поставяне на краен срок от 30 минути за принуждаване към необмислени действия.



Заплаха от негативни последствия

Предупреждение, че пратката ще бъде върната, ако не се реагира веднага.



Опасната връзка

Основната цел на измамата е да ва накара да кликнете върху несигурен уеб адрес.

Anatomy of a Spoofing Attack: The Classroom Trap

The Deceptive Setup



Email Spoofing

Forging a sender's identity to make an email appear as if it came from a trusted source.



Impersonating Authority

Using a relatable alias like "Mr. Math Teacher" to lower the recipient's defenses.



Routine Social Engineering

Using common themes like "upcoming test topics" to create a false sense of necessity.

The Email Element



Sender: "Mr. Math"



Context: "Test Topics"



File: "syllabus.exe"

The Reality Check



Unverified/Forged Identity



Bait for Social Engineering



Potential Malware/Virus

Hi Class, here's the new syllabus with test topics. Please review.

- Mr. Math



test-syllabus.exe



Suspicious File Names

Attackers label dangerous files with helpful-sounding names like "test-syllabus.exe" to encourage clicks.

The Malicious Attachment

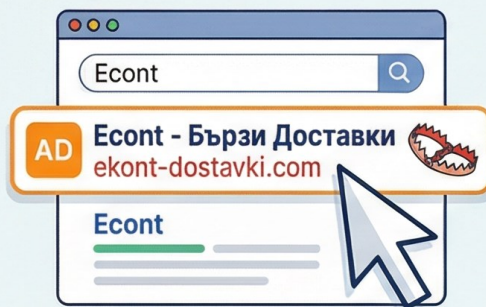
Be wary of documents ending in ".exe," which indicates an executable program rather than a text file.

Пазете се от капани: Скуатинг и Скиминг



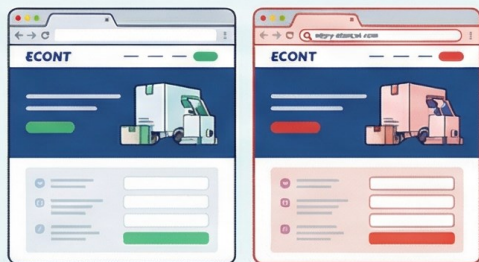
Информирайте се за две често срещани схеми за финансова измама и кражба на данни.

„СКУАТИНГ“ В ИНТЕРНЕТ



Фалшиви реклами в търсачките

Търсенето на позната марка (напр. Econt) може да изведе на първо място платена реклама към измамен сайт.



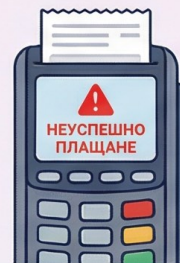
Измамен домейн: ekont-dostavki.com

Сайтът изглежда идентичен с истинския, за да подведе потребителя да въведе своите данни.

„СКИМИНГ“ ПРИ ПЛАЩАНЕ НА МЯСТО

Скрити устройства под щанда

Продавачът взима картата и я прекараа през невидимо устройство, преди да използва истинския терминал.



„Плащането не мина“

Сигнал за измама: „Плащането не мина“

Измамникът твърди, че има проблем, за да оправдае повторното прекарване на картата през скимиращо устройство.

ПАЗЕТЕ СЕ ОТ „СКИМИНГ“ НА POS ТЕРМИНАЛ

Скриване на устройството

Продавачът прекарва картата през терминал под щанда, далеч от погледа на клиента.

Малки квартални магазини

Тези обекти са най-честата локация за извършване на този тип злоупотреби.

Фалшиво съобщение за грешка

Твърди се, че транзакцията „не е минала“, за да се оправдае повторно прекарване на картата.

Скиминг (Skimming)

Незаконно копиране на информация от магнитната лента на банкова карта.

Мисия: Киберсигурност – Пази своя Дигитален Инвентар!

В България кибератаките нарастват по сложност, с над 1000 атаки седмично, използващи психологически натиск, AI и спуфинг за източване на средства.

КАПАНИТЕ: Как ни атакуват?

Спуфинг и Вишинг



Психологическа манипулация



Създаване на спешност, страх или фалшив авторитет за блокиране на логичното мислене.

1020+



България е подложена на по-висок интензитет на кибератаки от средното за Европа през 2024 г.

Сравнение на Атаки

Тип Атака	Основен Канал	Цел на Престъпниците
Омшинг	Електронна поща (Email)	Кражба на данни за достъп и банкови карти
Вишинг	Телефонни обикания	Директен трансфер на пари или пазаруване на интернет
Смшинг	SMS и мобилни приложения	Кликване върху зловерни линкове и „потвърждение“ на акаунт

ТВОЯТА БРОНЯ: Как да останеш защитен?

Прекъсни и Провери



Винаги затваряйте симителни обикания и набирайте официалния номер на банката сами.

Паролите са Твое Лично Право

Никол легитимна институция няма да поисква парола, ПИН или СУС код на телефона или имейл.

Двустепенна Верификация (2FA)



Активирайте 2FA и напавяйте пароли над 10 знака с комбинация от символи за максимална сигурност.

а

Внимание: Популярни финансови капани

Дигитални измами: "Скуатинг"

Google Ads

Рекламен капан в Google

Първият резултат при търсене често е платена реклама, водеща към фалшив уебсайт.

Измата "ekont-dostavki.com"

Сайтът копира визията на оригинала, за да заблуди потребителя да въведе данни.

Физически измами: "Скиминг"

Скрит POS терминал

Измамниците използват устройства под щанда, които не са видими за клиента.

Оправданието "Не мина"

Продавачът изисква повторно прекарване на картата, за да копира данните ѝ.

Смишинг: Как да разпознаем и спрем SMS измамите

Психологическите механизми на текстовите измами и конкретни стъпки за защита

Психологическите „бутони“ на измамниците



Изкуствена спешност и страх

Съобщенията често съдържат заплахи за блокиран достъп или глоби, за да предизвикат паническа реакция.



Злоупотреба с авторитет

Нападателят имитират банки (ОББ, Уникредит), държавни институции (НАП, ГДБОП) или познати брандове за моментално доверие.



Принципът на реципрочност

Предлагането на „награда“ или „педаръчна карта“ цели да подтикне потребителя да върне услугата, предоставяйки данни.



Златни правила за защита



Провери, преди да кликнеш

Задържете мишката върху линка (или огледайте домейна), за да видите реалния адрес на сайта.



Банките никога не искат пароли чрез SMS

Легитимните институции няма да поискат ПИН кодове или данни за карти чрез текстово съобщение.



Активирайте 2FA и филтри

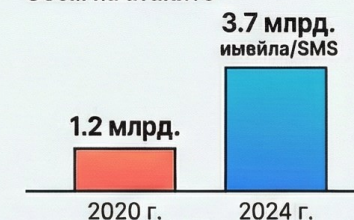
Използвайте двуфакторна аутентикация и проложения за блокиране на спам като Truecaller или Hiya.

Мащабът на заплахата и ръста на измамите (САЩ)

Финансови загуби



Обем на атаките



Масови сценарии в България

Speedy, Econt



Фалшиви куриерски доставки и топ такси

Теърдеиил за задържана претка ипл неплатена такса от 2-5 еуро за пътица.



36% от атаките не са по имейл

Нараства броят на измамите чрез S&IS, Viber, WhatsApp и социалии мрежи.



Сценарият „Грешен номер“

Невпнино начало на разговор, който постепенно преминава към предложени за инвестиции в криптовалути.

Внимавайте за „Смишинг“: Анатомия на една SMS измама

Смишингът е форма на киберизмама, при която се изпращат подвеждащи SMS съобщения от името на известни организации. Целта е да се подмами жертвата да плати фалшиви такси или да предостави лични данни чрез зловредни линкове.

Признаци на измамата

Маскиран подател

Измамниците често използват общи имена като „Tvoiat_operator“, за да вдъхнат фалшиво доверие.

1000 ЛВ.

Обещание за лесни пари

Типичен сценарий е съобщение за голяма печалба (например 1000 лв.) от томбона, в която сте участвали.

Механизъм на „Капана“

Изискване на авансово плащане

Изискването на „такса за обработка“ (например 20 лв.), за да получите наградата си, е сигурен знак за измама.

Зловредни линкове

Съобщението съдържа кратък линк, който води към фишинг сайт за кражба на данни или пари.

КИБЕРСИГУРНОСТ 2025: НАВИГАТОР ЗА БЕЗОПАСНОСТ НА УЧЕНИЦИ И РОДИТЕЛИ

Светът на технологиите се развива бързо, но с него растат и рисковете. Докато киберпрестъпността нанася щети за милиарди, проектът Be@CyberPro предлага ресурси за обучение на младежи, учители и родители, за да превърне интернет в по-безопасно място чрез знание и критично мислене.

СЪВРЕМЕННИТЕ ЗАПЛАХИ В ДИГИТАЛНИЯ СВЯТ



Годишни загуби
Киберпрестъпността нанася огромни икономически щети на световната икономика всяка година.



Новата ера на Deepfake измамите

Новата ера на Deepfake измамите
През 2025 г. престъпниците използват подправен глас и видео за кражба на данни.



Хроничен недостиг на експерти

Незаети работни места
в сферата на киберсигурността.



ЗЛАТНИ ПРАВИЛА ЗА ЗАЩИТА И ПРЕВЕНЦИЯ

Активирайте 2FA и силни пароли



Двухфакторната автентикация
с критична бернера срещу неправилен достъп до лични профили.

Проверка по втори канал



Винаги потвърждавайте
Винаги потвърждавайте съмнителни обаждания или съобщения чрез официален телефонен номер.

Учене чрез преживяване с Be@CyberPro



с Be@CyberPro
Интерактивни игри и онлайн курсове помагат на учениците да разпознават рисковете в реално време.

Бърза проверка на основните измами и начините за противодействие

	Фишинг (Email/SMS)	Не отваряйте линкове; влизайте само през официални сайтове.
	Фалшив онлайн магазини	Сверявайте домейна и търсете независими отзиви за търговеца.
	Телефонни измами	Институциите никога не искат пари или пароли по телефона.

‘Киберсигурност за МСП: Наръчник за защита и устойчивост’



КРИТИЧНИ МЕТОДИ ЗА ЗАЩИТА

- ✓ Използване на двуфакторно удостоверяване (2FA)
- ✓ Филтриране на пакети
- ✓ Криптирани протоколи



СПУФИНГ: ИЗМАМАТА КАТО ОРЪЖИЕ

Какво представлява спуфингът (Spoofing)?
Киберзаплаха, при която нападателят се представя за друго лице, устройство или услуга с цел кражба на данни.



ВНИМАВАЙТЕ ЗА „БАНКОВИ СЛУЖИТЕЛИ“

Чест сценарий е телефонно обаждане за „хакнат акаунт“ с цел получаване на кодове за достъп.

ОСНОВНИ ВИДОВЕ СПУФИНГ АТАКИ



IP СПУФИНГ

Фалшифициране на IP адреса, за да изглежда трафикът от сигурен източник.



EMAIL СПУФИНГ

Изпращане на съобщения от фалшив адрес, имитиращ доверен подател.

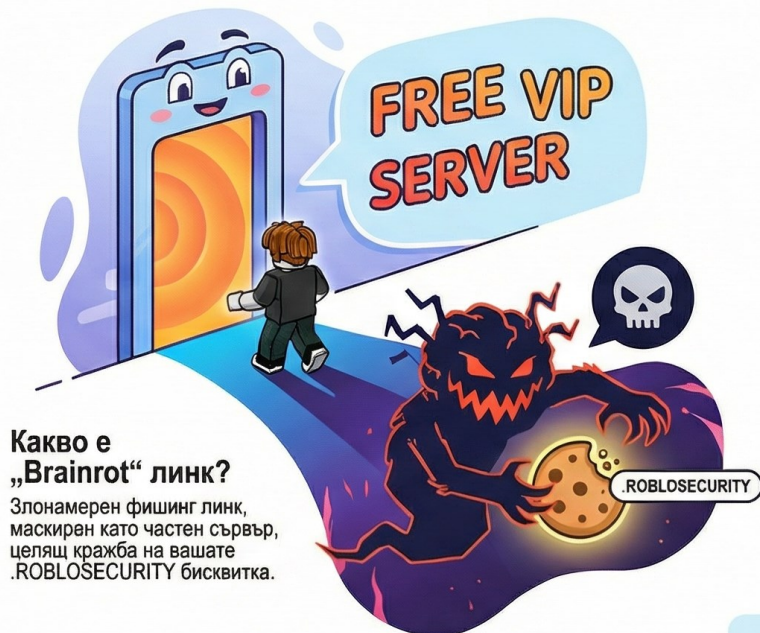


DNS СПУФИНГ

Промяна на DNS адреси за пренасочване на потребителите към фалшиви сайтове.

Пази своя Roblox акаунт: Пътеводител за защита от „Brainrot“ и фишинг измами

Заплахата: Как работат „Brainrot“ измамите?



Какво е „Brainrot“ линк?

Злонамерен фишинг линк, маскиран като частен сървър, целящ кражба на вашата ROBLOSECURITY бисквитка.

Тайпоскуатинг и фалшиви домейни

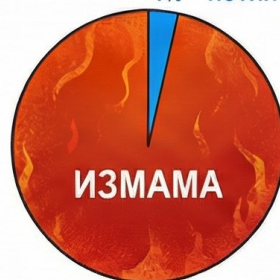
roblox.com

roblox-api.xyz

Измаминците използват визуално подобни адреси за да ви подмамат.

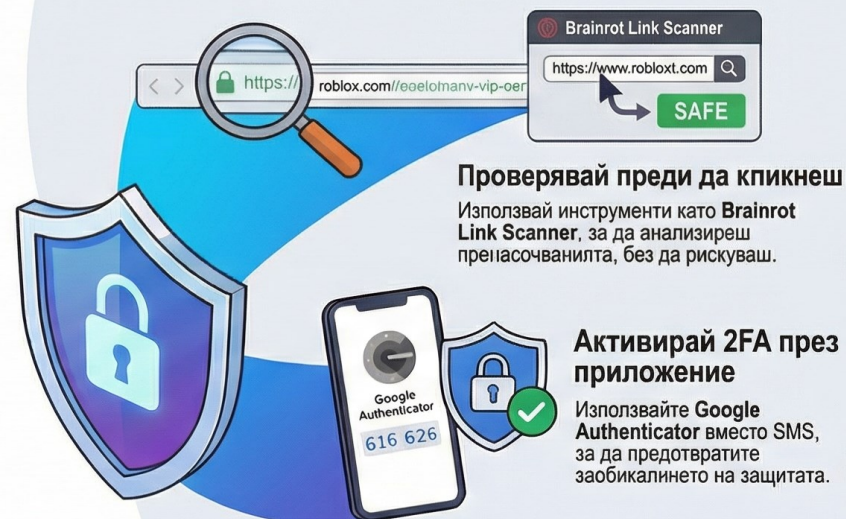
99% от „Free VIP“ линковете в TikTok са измама

1% – ИСТИНСКИ



Почти всички публично споделени линкове за безплатни сървъри са капани за кражба на вкаути.

Твоят щит: Стратегии за сигурност

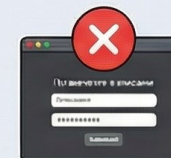


Проверявай преди да кликнеш

Използвай инструменти като Brainrot Link Scanner, за да анализириш пренасочванията, без да рискуваш.

Активирай 2FA през приложение

Използвайте Google Authenticator вместо SMS, за да предотвратите заобикалянето на защитата.



Правилото за „повторното вписване“

Ако вече сте вписани в Roblox, логитимен линк НИКОГА няма да иска паролата ви отново.

Тип на адреса	Официален (Безопасен)	Измамен (Опасен)
Основен Домейн	Основен Домейн: roblox.com	Основен Домейн: roblox.com, roblox.gg
Имейл подател	Имейл подател: no-reply@roblox.com	Имейл подател: noreply@accounts-roblox.com
Линк за сървър	Линк за сървър: съдържа privateServerLinkCode	Линк за сървър: завършва на .exe или .xyz

Анатомия на една измама: Какво е „Смишинг“?

Елементи на „Смишинг“ съобщението



Какво е „Смишинг“?

Фишинг атака, извършена чрез SMS, целяща кражба на пари или лични данни.



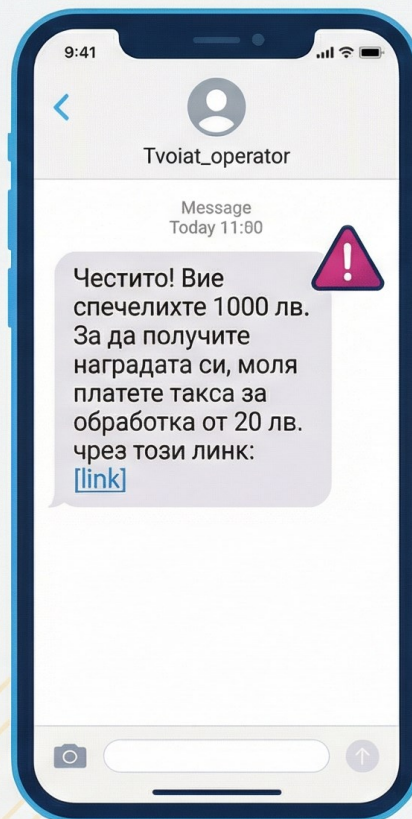
Фалшив подател

Използване на подвеждащи имена като „Tvoiat_operator“ за изграждане на измамно доверие.



Психологическа примка

Обещание за голяма печалба (1000 лв.), която приспива бдителността на потребителя.



Червени флагове за опасност



Искане на предварително плащане

Изискването на „такса за обработка“ (20 лв.), за да получите наградата, е сигурен знак за намама.



Съмнителни хипервръзки

Наличието на линк ([link]) за плащане в текстово съобщение е критичен риск.



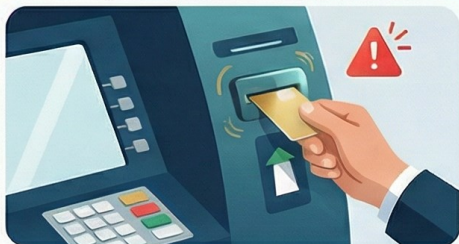
Използване на латиница

Официалните институции в България рядко комуникират важна финансова информация на латиница.

Защитете парите си: Как да разпознаем и предотвратим банкоматни измами

Скимирането на банкомати е сериозна заплаха, при която престъпници използват скрити устройства (скимери), за да копират данни от банкови карти и ПИН кодове. Научете как да ги разпознавате и какви стъпки да предприемете за защита.

Как да разпознаем скимиращо устройство?

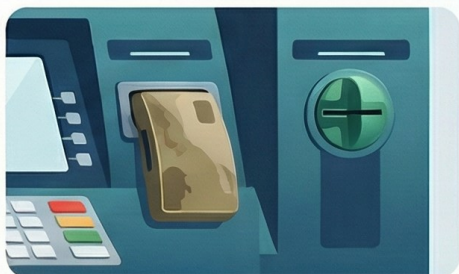


Размърдайте частите на банкомата

Преди употреба хванете слота за карта и клавиатурата – ако са хлабави или се движат, може да е поставен скимер.

Оглеждайте се за скрити камери

Проверявайте за малки отвори над екрана или клавиатурата, които могат да крият миниатюрни лещи за запис на ПИН када.



Проверете слота за карта

Скимерите често изглеждат обемни, с различен цвят или материал от останалата част на банкомата.

Правила за сигурност и защита



Винаги покривайте клавиатурата с ръка

Дори да не виждате камера, покриването на ПИН кода с другата ръка е най-ефективната защита.

Използвайте банкомати на сигурни места

Машините вътре в банковите клонове са по-сигурни и под постоянно видеонаблюдение.



EMV чип технологията е по-сигурна

Картите с чип са значително по-трудни за клониране в сравнение с тези, използващи само магнитна лента.

Бърз наръчник за действие при съмнение за измама



Свържете се с банката

Използвайте официален номер на гърба на картата. Незабавно блокиране на ометката.



Подайте сигнал в полицията

Поискайте еходящ номер на жалбата (PIR). Официален документ, необходим за възстановяване на средства.



Проверете извлеченията

Следете историята на трансакциите си редовно. Помага за ранно откриване на нерегламентирани тегленни.

Как да се предпазим от скиминг: Наръчник за сигурност при ползване на банкомат

Научете се да разпознавате скиминг заплахите и как да защитите личните си средства чрез технологични и физически мерки.

Физическа проверка и превантивни навици



Проверете за необичайни елементи

Опитайте леко да разклатите клавиатурата или слота за карта, за да откриете фалшиви накладки.



Покривайте клавиатурата при въвеждане на PIN

Това предпазва кода ви от скрити микрокамери, често монтирани над клавиатурата или екрана.



Избирайте сигурни локации

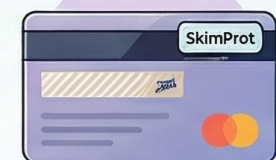
Използвайте банкомати в добре осветени райони или вътре в банкови клонове с видеонаблюдение.



Технологична защита и реакция

Използвайте EMV чип технология

Чип картите са много по-трудни за копиране от тези само с магнитна лента.



Защитни стикери (SkimProt)

Тези стикери блокират достъпа до магнитната лента, насочвайки банкомата да чете само защитения чип.



Бърза реакция при инцидент

При съмнение незабавно блокирайте картата и входиайте формуляр за оспорване на трансакции в банката.

Статистика на жертвите на скиминг и финансови загуби (2022 г.)



Над **1.6**
милиона
души
Жертви на
скиминг



~**1.4**
милиарда
долара
Глобални
финансови загуби

Ръст на измамите
(2019-2023)

АНАТОМИЯ НА ЕДНА ФИШИНГ ИЗМАМА

Този инфографичен модел анализира конкретен пример за „фишинг“ съобщение. То имитира официално предупреждение от Instagram, целящо да притисне потребителя да кликне върху опасна връзка под предлог, че акаунтът му ще бъде изтрит.



Фалшив подател (admin@instagram.com)

Измамниците често използват имена, които изглеждат официални, за да спечелят доверието на жертвата.



Психологически натиск и спешност

Съобщението залашва с „окончателно изтриване“, за да провокира паника и необмислени действия.



Капанът: Зловредната връзка

Основната цел е потребителят да кликне върху [линк], където данните му могат да бъдат откраднати.



КАКВО ПРЕДСТАВЛЯВА ТОЗИ „ФИШИНГ“?



Какво е фишинг?

Измамен метод за събиране на пароли чрез маскиране като легитимна институция.



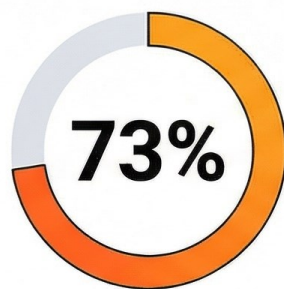
Претекст за нарушение на условията

Използва се фалшиво обвинение за нарушаване на правилата като оправдание за проверката.



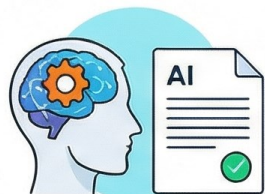
Фишингът през 2025-2026: Как да разпознаете и докладвате модерните измами

Новите лица на измамата



от пробивите започват с фишинг

Социалното инженерство остава водещата причина за кибер инциденти в световен мащаб.



AI премахва езиковите грешки

През 2026 г. атаките са по-убедители, защото AI генерира перфектно написани текстове без граматически дефекти.



Quishing: Опасността в QR кода

Скенирането на кодове от фактури или паркинг зони може директно да зарази мобилното ви устройство.

BEC (Business Email Compromise)



BEC (Business Email Compromise)

Кражба на средства чрез фалшиви фактури към счетоводители.

Omni-channel Phishing



Omni-channel Phishing

Комбиниране на имейл, SMS и обаждане за по-голяма достоверност.

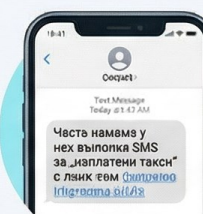
SaaS Harvesting



SaaS Harvesting

Кражба на пароли за облачни услуги като Google, Outlook и Slack.

Как да се защитите в България



Схеми с „Еконт“ и „Български пощи“

Честа измама у нас включва SMS за „наплатени такси“ с линк към фалшива платежна страница.



Докладвайте, не просто трийте!

В Outlook и Gmail напалавайте бутона „Report Phishing“, за да обучите филтрите на системата.



Изполавайте FIDO2 и биометрия

Традиционните SMS кодове вече са узвнми; хардуерните ключове за сигурност предлагат най-добра защита.

КИБЕРСИГУРНОСТ: КАК ДА РАЗПОЗНАЕМ И СПРЕМ ФИШИНГ АТАКИТЕ

ЧЕРВЕНИТЕ ФЛАГОВЕ: КАК ДА РАЗПОЗНАЕТЕ ИЗМАМАТА



Анализирайте подателя и линковете

Проверявайте внимателно домейна (напр. „novo.com“ вместо официалния на банката) и задръжте мишката над линка, за да видите реалния адрес.

<https://vsw.novo.com/>



Търсете психологически натиск

Фалшивите имейли често използват заплахи за блокиране на акаунт „до 24 часа“ или обещават „неочаквани награди“.



Общо и безлично обръщение

Легитимните институции обикновено се обръщат към вас по име, а не с „Уважаеми клиент“.

СРАВНЕНИЕ

ФИШИНГ (ИЗМАМА)

Подател:
Публичен или
грешен домейн



Тон:
Паника и
спешност



Данин:
Искат пароли
или ПИН кодове

ЛЕГИТИМЕН ИЗТОЧНИК

Официален
корпоративен
домейн



Тон:
Информативен
и спокоен



Данин:
НИКОГА не искат
чувствителни
данни

ВАШАТА ЦИФРОВА КРЕПОСТ: РЕАКЦИЯ И ПРЕВЕНЦИЯ



Незабавни стъпки при пробив



1. Запазете доказателства
(скрийншоти)



2. Сменете паролите



3. Изолирайте
устройството от
интернет.



Силата на 2FA и обучението

Обучените служители намаляват
риска от пробив до 70%, а
двуфакторната автентикация спира

99.9%
от атаките.



Правилото за архивиране

Пазете архивите (backups)
на отдолна покоя или в
облака, за да не бъдат
заразени при атака.

ВАЖНИ КОНТАКТИ В БЪЛГАРИЯ



Сигнализирайте на властите
Изпратете сигнал до ГДБОП
„Киберпрестъпност“ на
email@prectalnoct.bg



Национални ресурси за помощ
Свържете се с Националния CERT
(cert.bg) или КСП при проблеми с
онлайн търговци.

КИБЕРСИГУРНОСТ: ПЪТЕВОДИТЕЛ ЗА ЗАЩИТА ОТ ФИШИНГ И ОНЛАЙН ИЗМАМИ

Този инфографичен материал обединява експертни съвети от институции (НАП, БНБ) и технологични лидери за борба с фишинга. Фокусът е върху психологическите трикове на измамниците и техническите мерки за изграждане на киберустойчивост.

КАК ДА РАЗПОЗНАЕТЕ „ВЪДИЦАТА“?



ФАЛШИВО ЧУВСТВО ЗА СПЕШНОСТ

Измамниците често използват думи като „срешно“, „важно“ или заплахи за блокирани сметки.



ПОДОЗРИТЕЛНИ АДРЕСИ И ЛИНКОВЕ

Винаги проверявайте написания имейл адрес за леки размивания (напр. „nra-bg.org“ вместо „nra.bg“).



НЕОБИЧАЙНИ ИСКАНИЯ ЗА ДАННИ

Институции като БНБ или НАП никога не изискват пароли или данни за карти по телефона.

ЗЛАТНИ ПРАВИЛА ЗА КИБЕРЗАЩИТА



<https://www.nra.bg/respion-URL-адрес-в-долния-ляв-ъгъл>

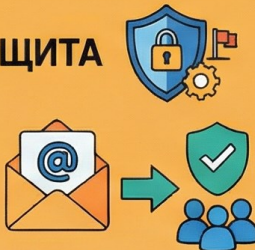
ПРОВЕРЕТЕ ЛИНКА, ПРЕДИ ДА КЛИКНЕТЕ

Задръжте курсора върху линка, за да видите реалния URL адрес в долния ляв ъгъл.



ИЗПОЛЗВАЙТЕ МНОГОФАКТОРНА АВТЕНТИКАЦИЯ (2FA)

Това е критичен слой защита, който спира достъпа, дори ако паролата ви е открадната.



ДОКЛАДВАНЕТО Е ПОБЕДА

Бързото докладване на съмнителен имейл предпазва цялата организация от по-нататъшни щети.



ПРЕСТАВИТЕЛНИ О ТАНИНА



ФОЛЕНКОР ПОВСЯКЕ

Измамниците на върху линка за вашата киберсикурност



ПРЪБИТЧНО ПОБЕДА?:

Бързото докладване на съмнителен имейл предпазва цялата организация от по-нататъ



ДОКЛАДВАНЕТО Е ПОБЕДА

Бързото докладване на съмнителен и предпазва цялата организация.

МЕТРИКИ ЗА УСПЕХ ПРИ ТРЕНИРОВЪЧНИ СИМУЛАЦИИ ЗА КИБЕРСИГУРНОСТ

МЕТРИКА	ЗНАЧЕНИЕ ЗА СИГУРНОСТТА	ЦЕЛ
СТЕПЕН НА ДОКЛАДВАНЕ	Показва активната бдителност на екипа	Колкото по-висока, толкова по-добре
ВРЕМЕ ЗА ДОКЛАДВАНЕ	Определя скоростта на реакция на SOC	Трябва да намалява с времето
ПОВТОРНО КЛИКВАНЕ	Показва нуждата от индивидуално обучение	Трябва да клони към нула

КИБЕРСИГУРНОСТТА Е НОВАТА МОДА: КАК ДА НЕ СЕ „ХВАНЕТЕ НА КУКИЧКАТА“

РАЗПОЗНАВАНЕ НА ФИШИНГ АТАКАТА (КАПАНИ ЗА МОДНИ ЖЕРТВИ)

Психологически натиск
и спешност



Маманиците използват думи за паника и заплахи, за да ви накарат да действате импулсивно.

Телефонни измами
от „служители на БНБ“



БНБ никога не се обажда с предложения за кредити или искания за парични преводи по телефона.

Визуални измами и
фалшиви линкове



Проверявайте за малки грешки
(напр. „paypa1“) и линса на „s“ а https://.
Диволег в о детайните!

Първо провери,
после клики



Посочете линка с мишката, за да
видите равния адрес в долния
ъгъл, преди да кликнете.

ПРАВИЛА ЗА КИБЕР-ЗАЩИТА (ВАШИЯТ CYBER-CHIC КОМПЛЕКТ)

Докладването е
истинската победа



Не просто трийте! Докладвайте ведиага на ИТ отдела
или банката. Това в вашият момент на слава!

Пазете се от
„албански вируси“



Никога не отваряйте архиви от непознати и не
въвеждайте ПИК или данни за харти в имейн форми.

Рекорден ръст на дигиталния „сквотинг“: Как да защитите бранда си

Дигиталният „сквотинг“ достигна рекордни нива през 2025 г., като киберпрестъпниците използват имитиращи домейни за фишинг и разпространение на зловреден софтуер. С 68% ръст на споровете за домейни от 2020 г. насам, защитата на марката вече изисква проактивен подход.

Мащабът на заплахата и методите на атака



6 200
спора за домейни
през 2025 г.

Това е най-онсокипт брой, записван
някога от Световната организация за
интелектуална собственост.



\$4,8
милиона
средна цена на атака
Толкова струва средно на една
компания фланинг инцидент,
валючително възстановяването
и репутационните щети.



Сложни тактики за имитация



Използване на
„login“

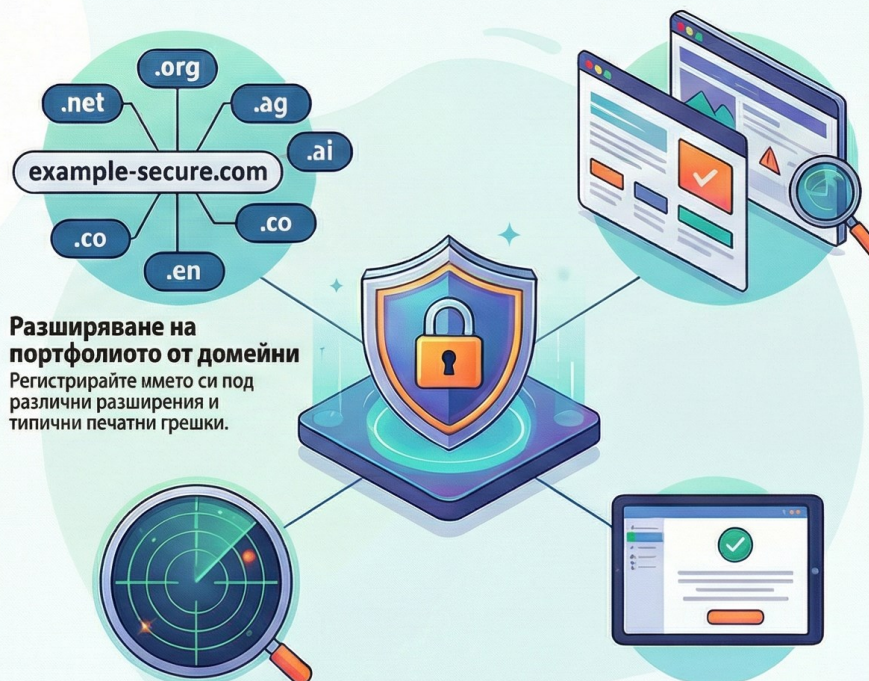


Грешни при
изписване и
хомографи



Визуалне сходни
символи

Стратегии за проактивна защита



**Разширяване на
портфолиото от домейни**
Регистрирайте името си под
различни разширения и
типични печатни грешки.

Постоянен мониторинг на заплахите

Следете за нови регистрации, които
приличат на вашия бранд, и проверявайте
издадените сертификати.

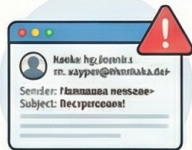
Образование на крайния потребител

Обучавайте клиентите как да
разпознават легитимните ви канали
за плащане и поддръжка.

Пазете се от фишинг: Пътеводител за дигитална безопасност



3 Червени флага на измамата



Подозрителен подател

Проверете дали имейл адресът съвпада точно с официалния домейн на компанията.



Изкуствена спешност

Фрази като „Акаунтът ви ще бъде блокиран до 24 часа“ целят да предизвикат паника.



Безлични обръщения

Легитимните институции обикновено ви адресират по име, а не с „Уважаеми клиенте“.

Над 80% от пробивите в сигурността включват фишинг. Измамниците използват психологически натиск и фалшиви идентичности (банки, курнери, държавни институции), за да откраднат лични данни и финансови средства.

Сравнение на основните канали за атака

Тип атака	Канал на комуникация	Основен инструмент
Зловредни линкове, прикачени файлове...	Фалшиви известия, SMS линкове...	Психологически натиск, имитация на глас...
Зловредни линкове, прикачени файлове.		
Зловредни линкове, прикачени га файлов...		

План за защита и действие

Кликнете тук

<http://anvson-calls.com>

Проверявайте линковете без клик

Задръжте курсора върху линка, за да видите реалния URL адрес в долината ъгъл.



Активирайте 2FA

Двуфакторната автентикация е най-сигурният начин да защитите акаунтите си от кражба.



Използвайте официални канали

При съмнение затворете и се обадете на официалния номер от сайта на институцията.

A cartoon illustration of a fisherman with a beard and a blue cap, wearing an orange shirt and blue overalls, sitting in a wooden boat. He is holding a fishing rod with a large fish on the line. The boat has a small cabin with two windows and a chimney. The background shows a blue sky with white clouds and blue water.

Атака върху човешкото доверие

[illegible]

3. Как да разпознаем фалшивата примамка



4. Твоята „защитна екипировка“



Двухфакторна аутентикация (2FA)

Викато използвате втора фактор – например, кодът от смартфонът (телефон, iPad) или лъч, вместо сте (биометрия), съд за еднократна употреба и др.



Използване на официални приложения

Найразличните компании и провайдери предлагат официалните мобилни приложения (напр. Zubease Mobile) или затворените iOS/Android приложения.



Проверка на линковете

Преди киноване проверете дали сайтът започва с „https://“ и не е свързан на линк от някоя друга продажба, на измамниците могат да копират и това.

5. Какво да правиш, ако си се „хванал“



Незабавно блокиране

Блокирайте базовите си карти и достъпа до онлайн блокирането чрез мобилното приложение или по телефона.

Смяна на пароли

Променете паролите за всички акаунти, които може да са компрометирани, като използвате слепи и уникални комбинации.

Докладване на властите

Подайте сигнал в отдел „Киберпрестъпност“ към ГДБОП или в национални център за безопасност в интернет.

(Психологически тактики и ИИ заплахи)

(Психологически тактики и ИИ заплахи)

Да образова потребителите относно психологическите тригери на фишинга и как да се защитават чрез съвременни методи в ерата на изкуствения интелект.

ИИ – Генераторът на перфектни измами
ИИ създава фишинг кампании за 5 минути, които е по-убедителна от човешката.

Най-честият тригер (62.5%), карещ жертвата да действа импулсно под патиса за оремн.

Двуфакторна автентикация (MFA)
Най-мощната бернера, авото скоро демона,
дври ако перклата е отарадната.

Излинска занчахл за бловирели авоунти или
правии последица, за да предизвика палинка.

Подминео хрех анкност или анбипнтство с
обошения за награди или неочаквани нечабкя

Ванята спарайте в мислете, когато усетите
синна емоция (сгрез или възненение)

Сравнение на ефективността на ИИ срещу човешките физични усилия.	
Време за подготовка	16 часа
Успеваемост (забвуда)	24% по-висока
Брой съобщения дневно	3.4 милиарда

Психология на фишинга: Зад маската на „легитимната фасада“

Трите стълба на
фишинг психологията

Социално инженерство
и „Легитимната фасада“

Чувство за спешност (Urgency)

Пригоска жертвата да действа
издадени, страничнически
за логическо разсъждение или
проверка.

82.54%

71.42%

Чувство за
спешност

Страх чрез
халлаха

Предизвикване на страх (Fear)

Наб-силният психологически
сигнал, често заловяващ
заплахи за блокирани сметки
или правни последици.

Изкушение чрез желание (Desire)

Експлоатира любопитството
или алчността чрез обещания
за награди, вълнители или
безплатни услуги.

Маскиране на намеренията

Изманиците имитират
корпоративен стилет, лог и
стих, за да създадат илюзия за
доверие.

Емоционална убойка

Комбинацията от силна емоция
и доверие действа като „убойка“
срещу рационални подкъд.

Маскираните на намеренията

Степената на успех се утвърждава,
когато имейлет имитира
вотрешен стрел като Човешки
ресурс или ИТ.

Рекорден ръст на дигиталното „сквотинг“: Новата вълна от кибер заплахи

МАЩАБЪТ НА ПРОБЛЕМА

6 200

6 200 официални спора
за домейни през 2025 г.

Това е най-високият брой
спорова, регистриран някога
от Обветовната организация
за интелектуална
собственост (WIPO).



ЧЕТИРИТЕ МЕТОДА НА АТАКА



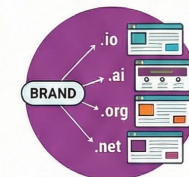
ТАЙПОСКВОТИНГ (Typosquatting)

Разчита на правописни грешки, които
потребителите често допускат при
написване на марката в браузъра.



КОМБОСКВОТИНГ (Combosquatting)

Добавяне на пореждачки думи към
вегитимното име на марката,
например „deals“, „login“ или „support“.



TLD СКВОТИНГ (Top-Level Domain)

Регистрация на същото име под
различни разширения, особено
популярните в момента .io и .ai,
както и .org или .net.



ХОМОГРАФСКИ АТАКИ (Homograph attacks)

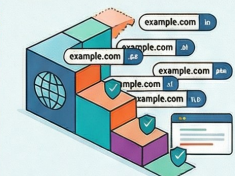
Наполизация на визуално идентични
символи от различни азбукки (напр.
корилица вместо патиница), за да
наглежда фалшивият домейн автентичен.

ТРИ СЪТЪПКИ ЗА КОРПОРАТИВНА ЗАЩИТА



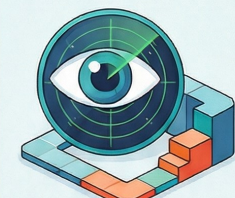
68% ръст на инцидентите
спрямо 2020 г.

Бързото разрастване на дигиталното
присъствие е довело до мащабно
увеличение на злоупотребите с
търговски марки за последните 5
години.



РЕГИСТРАЦИЯ НА ВАРИАЦИИ

Проактивно регистриране на общи
грешки при напосване, хибридни
имена и различни регионални
разширения (.de, .cn, .co.uk).



ПОСТОЯНЕН МОНИТОРИНГ

Непрекъснато наблюдение на нови
регистрации на домейни и нападени
сертификати, които съпадат при
наподобават вашата марка.

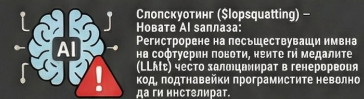
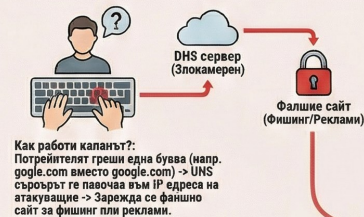


ОБУЧЕНИЕ НА КЛИЕНТИТЕ

Информирание на потребителите как
да разпознават официалните хапала
за комуникации и портали за плащане.

Тайпоскутинг: Изкуството на подвеждащия домейн

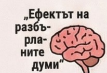
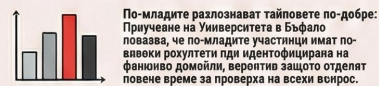
Какво е Тайпоскутинг?



Основни техники за намама



Статистика и Ефективност

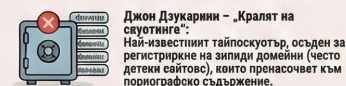
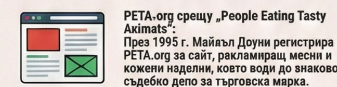
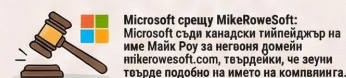


„Ефектът на разбърканите думи“:
Милкът ни неспо разчете думи с разменени вътрешни букви, което прави пермутациите (като „microsoft.com“) едот от най-трудните за забелязване грешки.



.COM е основната мишена:
Над 82% от злонамерените регистрации използват разширението .com, тъй като потребителите автоматично го добавят към имената на марките.

Известни случаи от историята



Как да защитите своя бизнес и себе си?



Защитна регистрация на домейни:
Регистрирайте превантивно най-честите правописни грешки и вариации на вашия домейн, преди злонамерени лица да го поправят.



Използвайте инструменти за проверка:
Инструменти като CIRCL, Typosquatting Finder (използва 21 алгоритъма) и DNSTwister помагат за откриване на вече регистрирани имитации на домейни.



UDRP Процедури (ICANN):
Унифицираната политика за разрешаване на спорове позволява на собствениците на марки да си върнат злонамерено регистрирани домейни чрез административен процес, вместо скъп съдебен дела.