АНАТОМИЯ ФИШИНГОВОГО ПИСЬМА

Это письмо скрывает 8 красных флагов.

Большинство замечают только 2.
А вы найдёте все?

Inbox

URGENT: Account suspended in 24 hours 1

Nimbus Bank Security 2 09:41
<alerts@nimbus-secure-help.net> 3
reply-to: verify@acc-support.xyz 4

Dear Customer, 5

We detected unusual sign-in activity on your account. Verify your identity within 24 hours or your account will be permanently locked. 6

Verify my account

http://nimbus.com.login-check.xyz/verify 7

Statement_Sept.pdf.html 48 KB 8

Nimbus Bank Security Team

1 Давление по времени
Срочность — классический приём фишинга, чтобы заставить действовать без раздумий.

2 Подозрительный отправитель
Название выглядит достоверно, но его легко подделать.

3 Сомнительный домен
Используется похожий домен (typosquatting), а не официальный.

4 Отдельный reply-to
Письмо приходит с одного адреса, а ответы уходят на другой — частый признак фишинга.

5 Общее обращение
Вместо вашего имени — шаблонное “Dear Customer”.

6 Угрозы
Манипуляция блокировкой аккаунта, чтобы вызвать панику.

7 Поддельная ссылка
Адрес выглядит как официальный, но ведёт на сторонний домен.

8 Опасное вложение
Файл с двойным расширением .pdf.html может содержать вредоносный код.

ВАШ РЕЗУЛЬТАТ

Сколько флагов вы нашли? ? ? ? ? ? ? ? ?

@lionsoulbatyshchikov

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

02/20

Что такое фишинг?

Это поддельное сообщение, которое маскируется под человека или сервис, которому вы доверяете, чтобы вы передали что-то ценное.



the bait

письмо

Выглядит как реальное сообщение от банка, начальника или службы доставки.

the hook

ловушка

Ссылка, вложение или просьба ответить — всё это приводит к реальному ущербу.

the target

ЖЕРТВА

Нужен всего один клик от одного человека.

На что они охотятся?

Пароли
Passwords

Деньги
Money

Доступ к устройствам
Device access

Личные данные
Identity

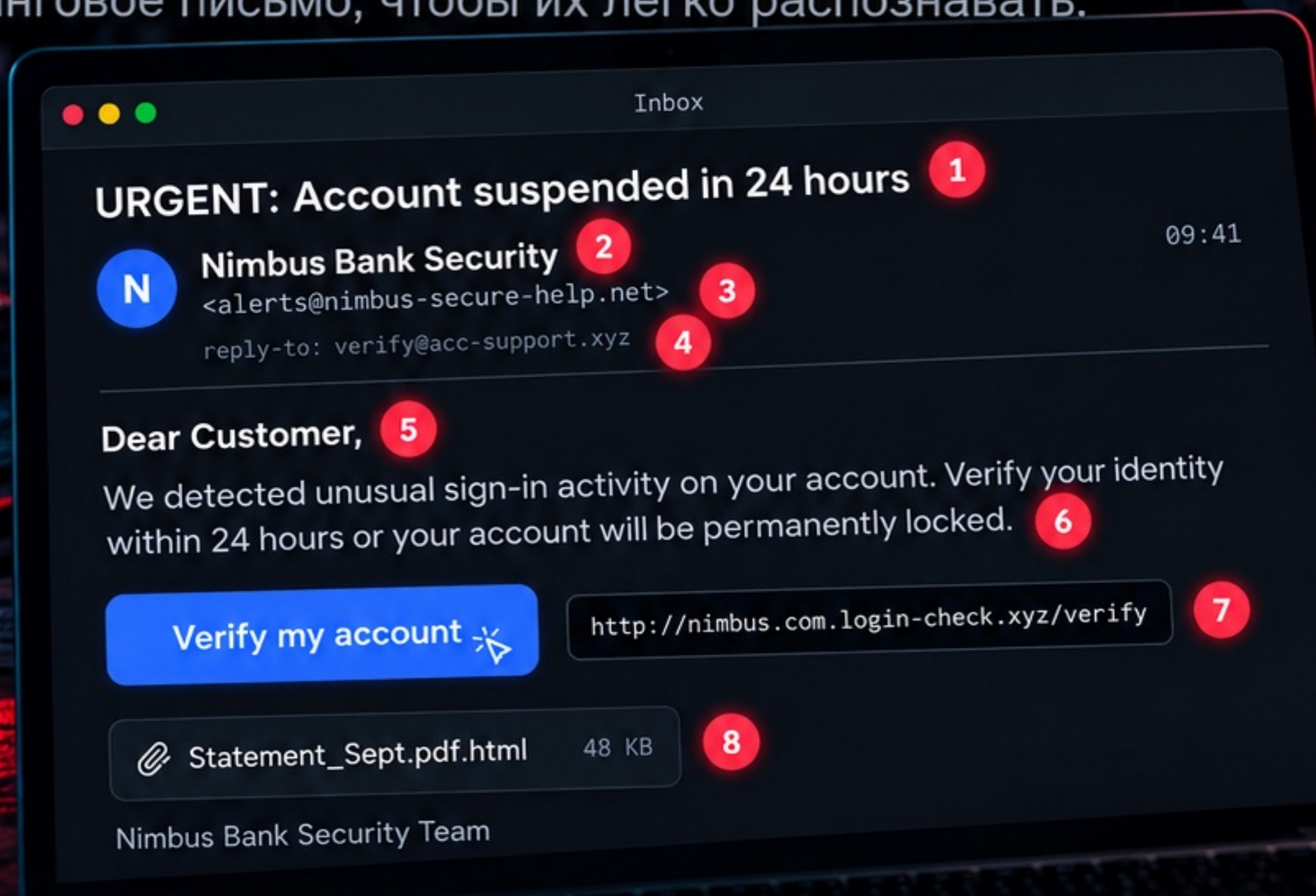
@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

03/20

Анатомия фишингового письма

Разбираем, из каких элементов состоит типичное фишинговое письмо, чтобы их легко распознавать.



1 Срочная тема (Urgent subject)

Создаёт давление и заставляет действовать быстро, без анализа.

2 Поддельное имя отправителя

Выглядит как официальный бренд (например, банк).

Nimbus Bank Security

3 Похожий домен (Lookalike domain)

Используется поддельный домен, похожий на настоящий.

`nimbus-secure-help.net`

4 Скрытый reply-to

Письмо приходит с одного адреса, а ответы уходят на другой.

`verify@acc-support.xyz`

5 Шаблонное обращение

Вместо вашего имени — общее «Dear Customer».

Dear Customer,

6 Угрозы и давление

Сообщение о блокировке аккаунта в течение 24 часов.

7 Подозрительная ссылка

Адрес выглядит как официальный, но ведёт на сторонний домен.

`nimbus.com.login-check.xyz`

8 Замаскированный файл

Файл с двойным расширением .pdf.html может содержать вредоносный код.

Statement_Sept.pdf.html

@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

04/20

Срочная тема в письме

Цель — вызвать панику. Напуганный мозг сначала кликает, а думает потом.



Входящие · 5 непрочитанных

Что их выдает?

Nimbus Bank · 09:41 · Срочность
СРОЧНО: Аккаунт будет заблокирован через 24 часа
Подтвердите свою личность, чтобы избежать блокировки.

ParcelNow · 10:12 · Страх потери
Не удалось доставить посылку. Оплатите €1.99, чтобы перенести доставку

CEO · Mark · 11:26 · Авторитет
Нужно срочно обработать этот платёж до 17:00
Это приоритет.

Rewards Team · 12:03 · Жадность
Поздравляем! Вы выиграли подарочную карту €500
Заберите свой приз прямо сейчас.

Drive Share · 12:18 · Любопытство
Кто-то поделился файлом Salaries_2026.xlsx
Откройте доступный файл.

1 Срочная тема (Urgent subject)

Создает давление и заставляет действовать быстро.

2 Поддельное имя отправителя

Выглядит как официальный бренд (например, банк).

3 Похожий домен

Используется домен, похожий на настоящий (nimbus-secure-help.net).

4 Скрытый reply-to

Письмо приходит с одного адреса, а ответы уходят на другой.

5 Замаскированный файл

Файл может иметь двойное расширение (.pdf.html) и содержать вредоносный код.

КАК ПРОВЕРИТЬ

Реальные компании почти никогда не дают вам несколько часов на реагирование. Сделайте паузу и откройте официальное приложение или сайт самостоятельно, чтобы проверить.

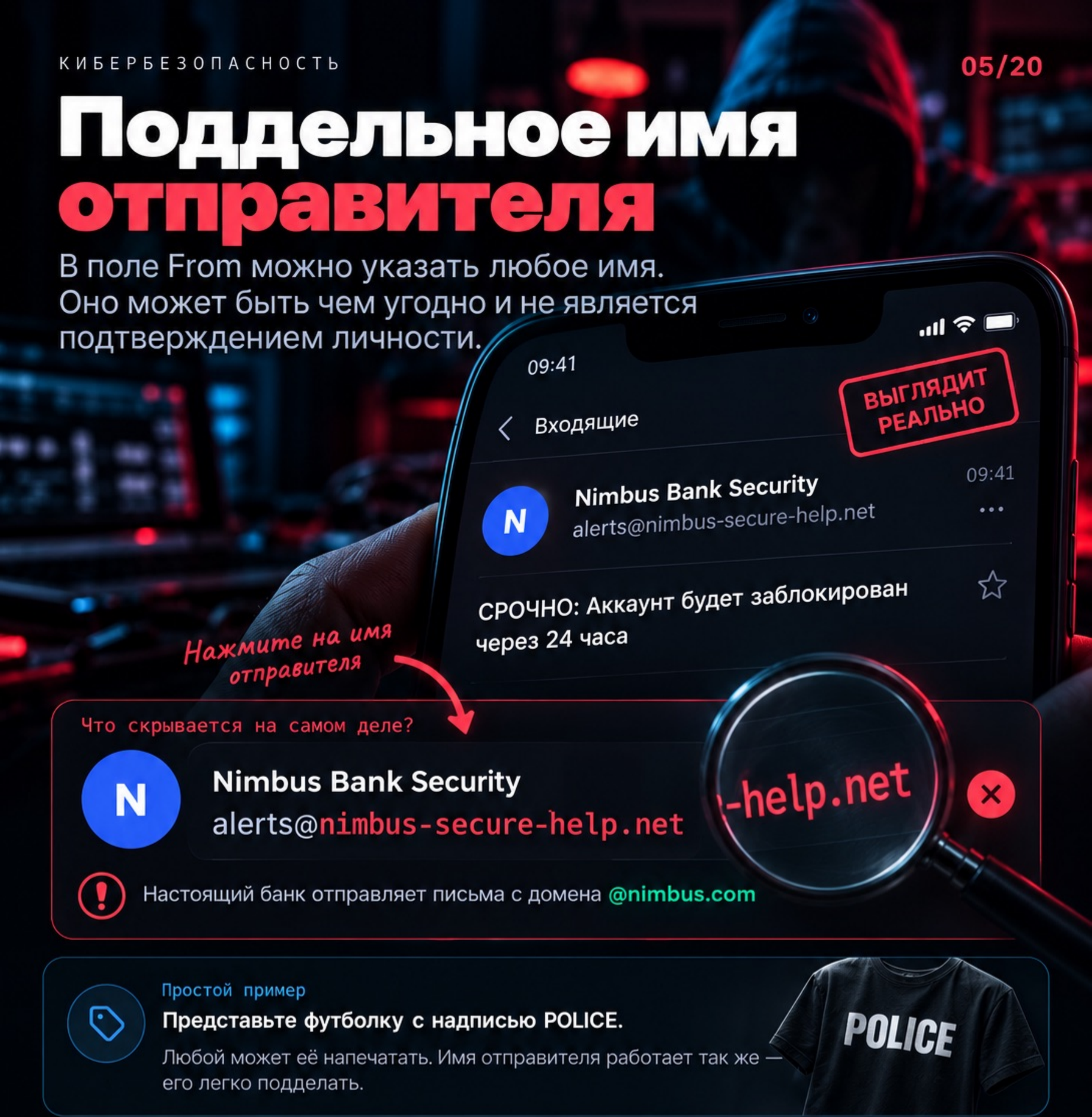
@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

05/20

Поддельное имя отправителя

В поле From можно указать любое имя. Оно может быть чем угодно и не является подтверждением личности.



Простой пример

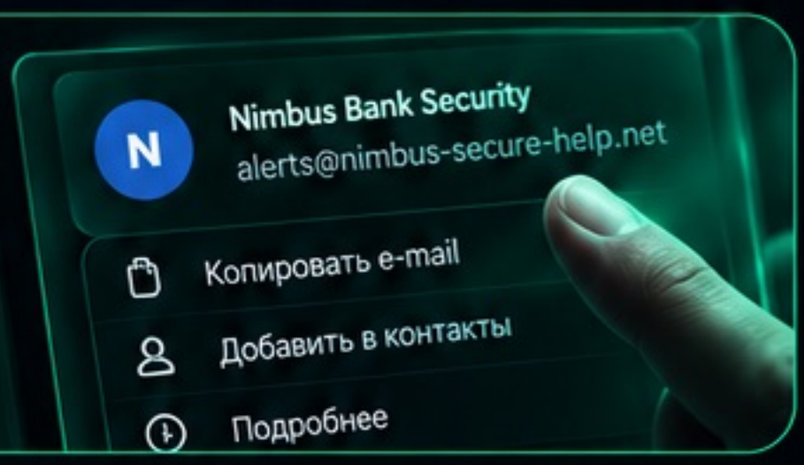
Представьте футболку с надписью POLICE.

Любой может её напечатать. Имя отправителя работает так же — его легко подделать.

Как проверить

Нажмите или кликните на имя отправителя,

чтобы увидеть полный email-адрес. На телефоне он часто скрыт по умолчанию.



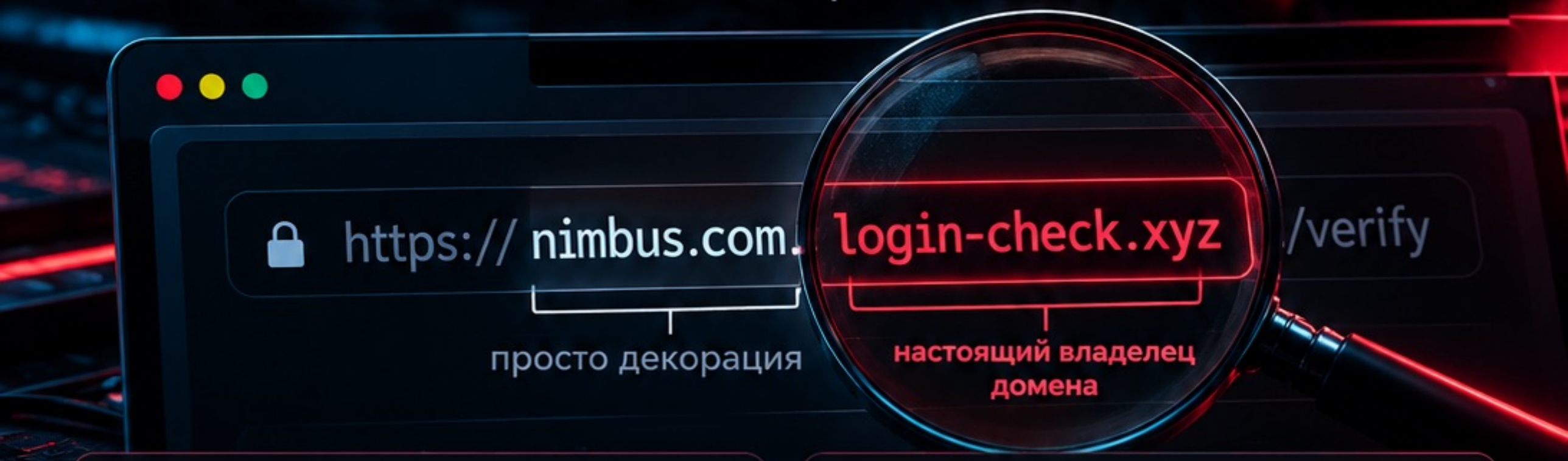
@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

06/20

Похожий домен

Злоумышленники регистрируют домены, которые почти не отличаются от настоящих. Смотрите внимательно.



Замена буквы

✗ nimbsu.com

✓ nimbus.com

Похожие буквы

✗ nirnbus.com

✓ nimbus.com

Цифра вместо буквы

✗ n1mbus.com

✓ nimbus.com

Дополнительные слова

✗ nimbus-secure-help.net

✓ nimbus.com

Другой домен верхнего уровня

✗ nimbus.co

✓ nimbus.com

Посторонний символ

✗ nïmbus.com

✓ nimbus.com

КАК ПРОВЕРИТЬ

Найдите **первую** одинарную косую черту (/).
Всё, что находится прямо перед ней (например, nimbus.com),
— настоящий домен.

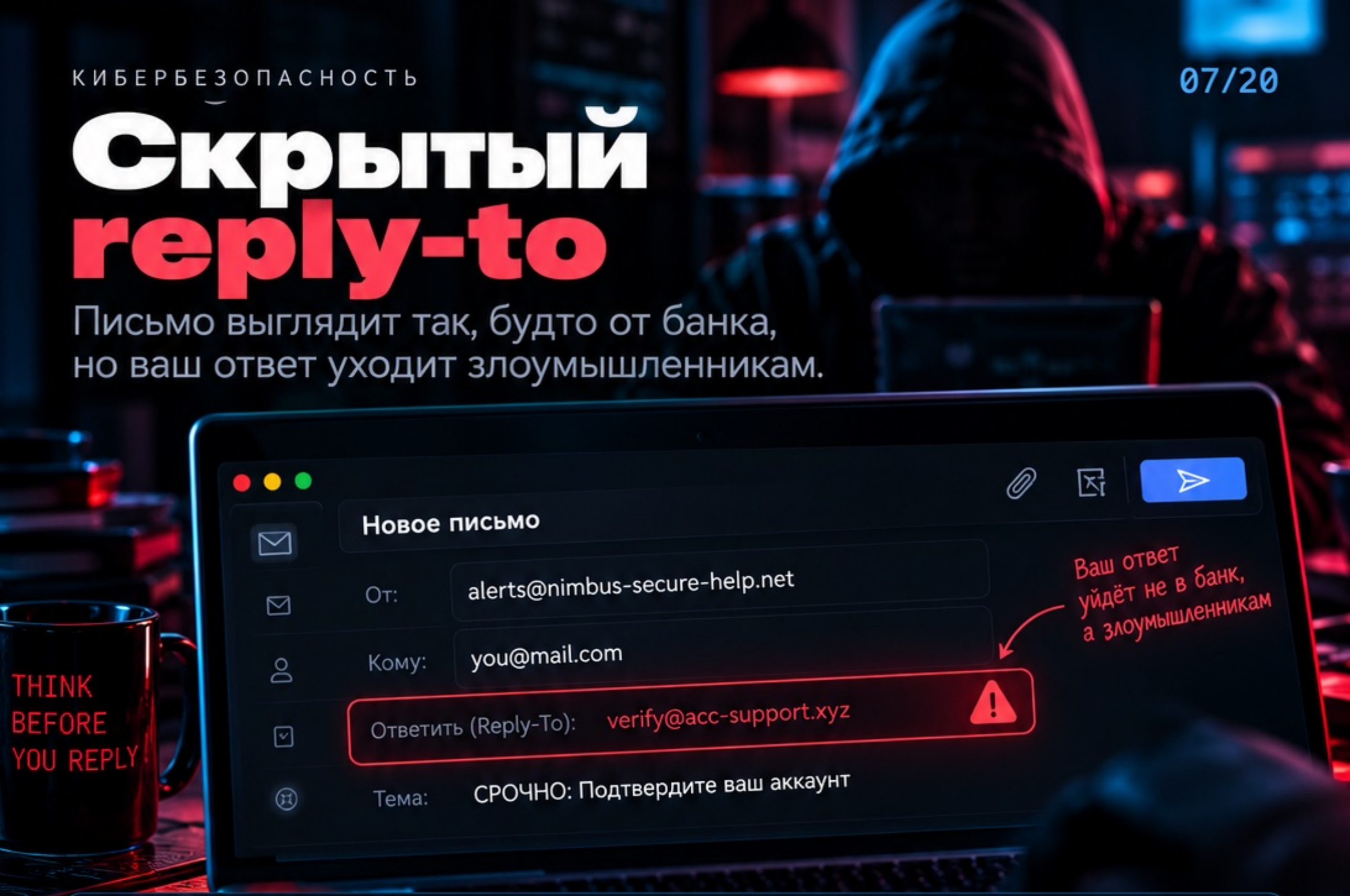
@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

07/20

Скрытый reply-to

Письмо выглядит так, будто от банка,
но ваш ответ уходит злоумышленникам.



Как это работает?



Зачем им ваш ответ?

Так вы продолжаете диалог с атакующими — они могут прислать поддельные счета, ссылки, запросить подарочные карты или коды.



Как проверить?

Перед тем как ответить, проверьте поле **Reply-To** или поле **Кому (To)**. Оно должно совпадать с настоящим отправителем.



@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

08/20

Типовое приветствие

Ваш банк знает, как вас зовут.
Массовые письма так не выглядят.

✕ ФИШИНГ

От: alerts@nimbus-secure-help.net
Кому: you@mail.com

Dear Customer,

Dear User,

Dear Valued Member,

Hello Sir/Madam,

✓ НАСТОЯЩАЯ КОМПАНИЯ

От: support@nimbus.com
Кому: alex.petrov@mail.com

Hi Alex,

По вашей карте, заканчивающейся на **4417**

Ваш заказ **#48213**

С уважением,
Команда Nimbus Bank

ВАЖНО ПОНИМАТЬ

Одно лишь упоминание вашего имени не доказывает подлинность письма.

Злоумышленники могут взять его из соцсетей или утечек данных и использовать в фишинговых атаках. Обращайте внимание на другие признаки.

КАК ПРОВЕРИТЬ

Есть ли в письме детали, которые знает только настоящая компания?

Если такое письмо могло прийти кому угодно — считайте его подозрительным.

- Последние 4 цифры карты
- Номер заказа
- Реальная дата операции

@lionsoulbatyshchikov

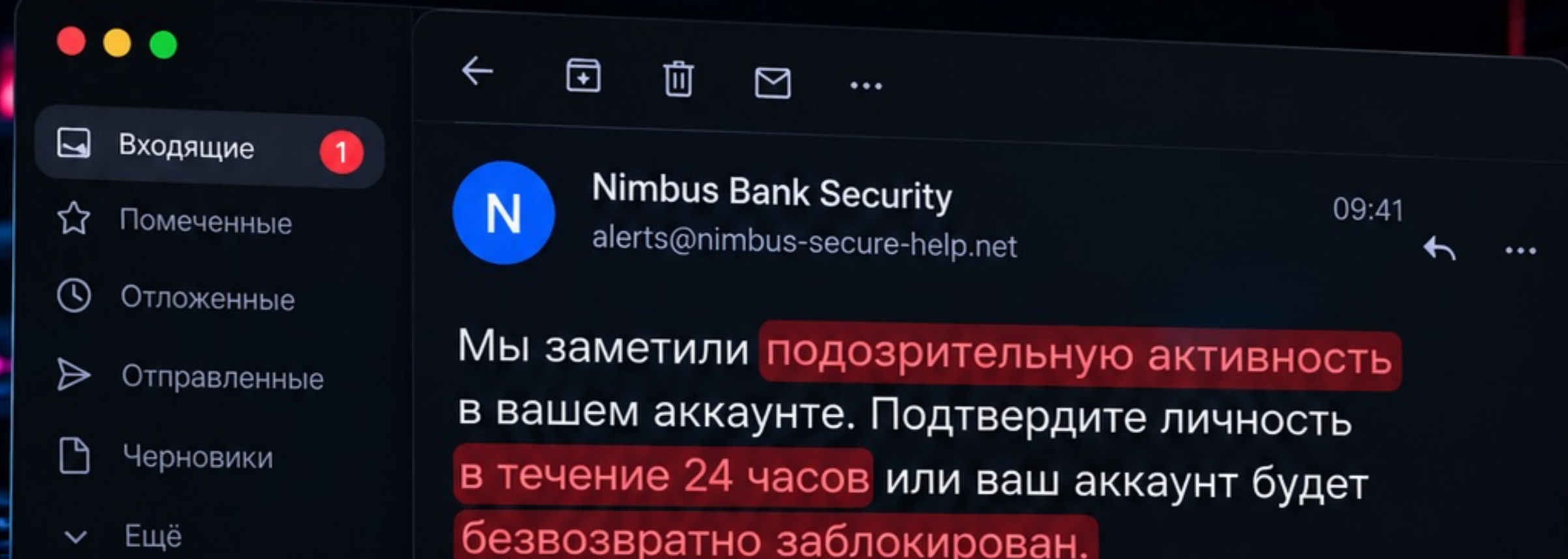
КИБЕРБЕЗОПАСНОСТЬ

09/20

Давление и срочность

Эти фразы заставляют вас нервничать, чтобы вы перестали думать и кликнули.





УРОВЕНЬ ДАВЛЕНИЯ



ТАКИЕ ФРАЗЫ — ТИПИЧНЫЙ ПРИЗНАК

- Final notice
- Act now
- Last warning
- Legal action
- Unauthorized payment
- Account locked
- Within 24 hours
- Confirm or lose access

КАК ПРОВЕРИТЬ

Сам факт давления — это уже красный флаг.

Закройте письмо и свяжитесь с компанией через официальное приложение или номер с их сайта.

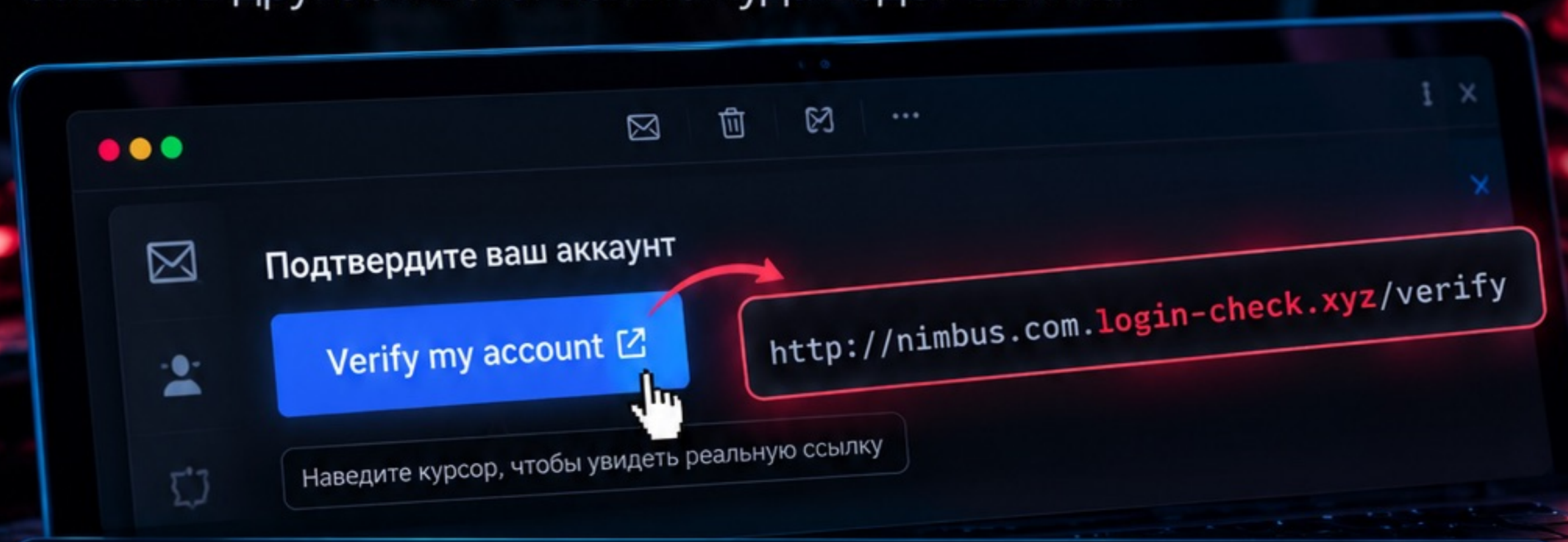
@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

10/20

Несовпадение ссылки

Кнопка может говорить одно, а перейти вы можете совсем в другое место. Важно куда ведёт ссылка.



Разбираем настоящую ссылку

http://nimbus.com.login-check.xyz/verify

http://
нет шифрования (не HTTPS)

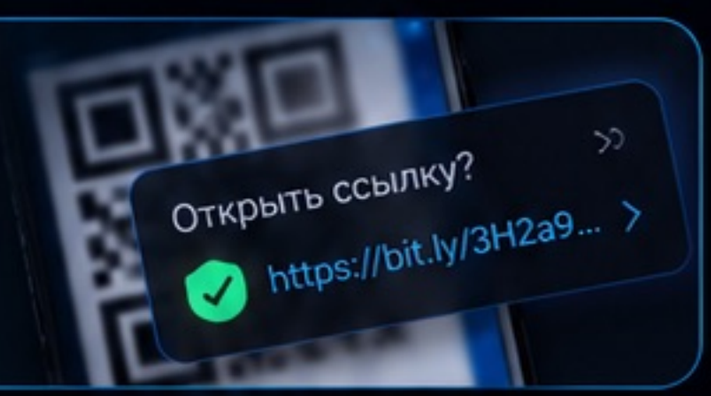
Похоже на банк (это обманка)

Реальный домен принадлежит злоумышленникам

Страница

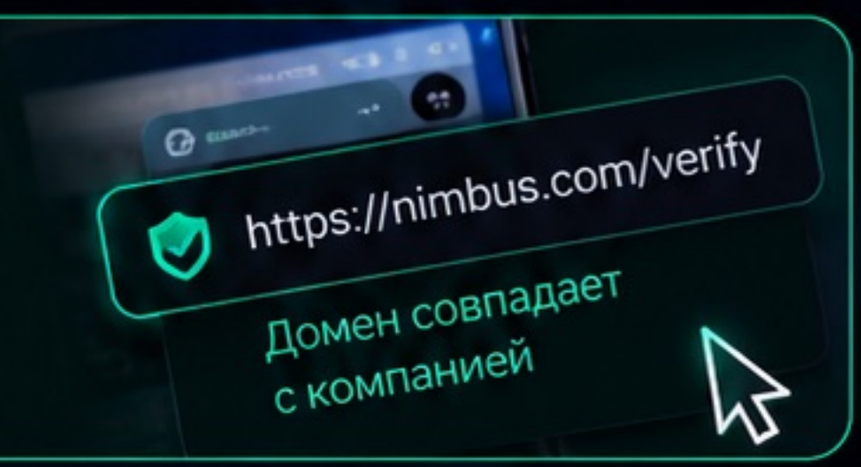
Короткие ссылки и QR-коды скрывают реальный адрес

Используйте предпросмотр ссылки или всплывающее окно с URL вашей камеры, прежде чем открывать.



Как проверить?

Наведите курсор (или нажмите и удерживайте на телефоне) перед тем, как кликнуть.
Если реальный домен не принадлежит компании — не открывайте ссылку.



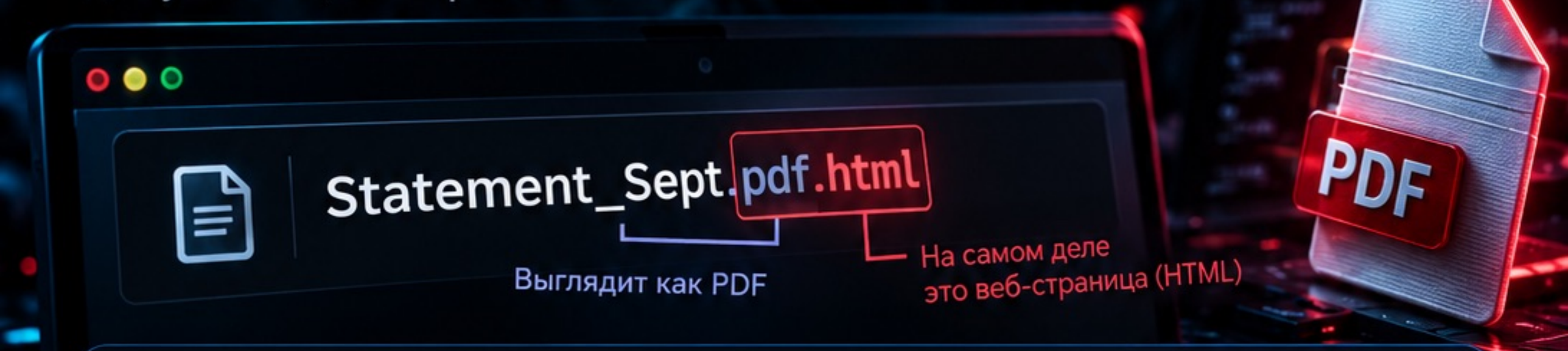
@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

11/20

Файл в маске

Файлы могут скрывать свою настоящую природу. Часто опасные файлы выглядят как обычные документы, изображения или PDF.



Расширение	Что может делать	Уровень риска
.exe .scr .bat	Запускает программу на вашем устройстве	■■■
.html .htm	Открывает поддельную страницу для кражи данных (даже офлайн)	■■■
.zip .iso .img	Может содержать другие файлы и скрывать вредоносное содержимое	■■■
.docm .xlsm	Запускает макросы, если вы нажмёте «Включить контент» (Enable)	■■■
.pdf	Может содержать ссылки, QR-коды и встроенные скрипты	■■□
.jpg .png	Обычно безопасны, но могут использоваться в атаках (например, со скрытыми данными)	■□□

КАК ПРОВЕРИТЬ

Включайте отображение расширений файлов и никогда не нажимайте «Enable» на неожиданных файлах.

@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

Поддельная страница входа

На вид обе страницы одинаковые.
О правде говорит только адрес в строке браузера.

Настоящий сайт

nimbus.com/login

N

Nimbus Bank

Войдите в аккаунт

Email

Password

Sign in

Фишинговый сайт

nimbus.com.login-check.xyz

N

Nimbus Bank

Войдите в аккаунт

Email

Password

Sign in

Замок в браузере — не гарантия безопасности

Он означает только, что соединение зашифровано (HTTPS).
Злоумышленники тоже могут получить SSL-сертификат бесплатно.

Как проверить?

Используйте **password manager** — он не будет автозаполнять данные на поддельном домене. Если поля остались пустыми — остановитесь и проверьте URL.

Сохранённые данные

nimbus.com

nimbus.com.login-check.xyz

КИБЕРБЕЗОПАСНОСТЬ

13/20

SPF, DKIM, DMARC

Почтовый сервер проверяет каждое письмо по трём признакам. На скриншоте — пример, как это выглядит у атакующих.

SPF

Список разрешённых отправителей

Проверяет, разрешён ли сервер, с которого отправлено письмо, отправлять почту от домена.

Если домен используется злоумышленниками — SPF не проходит.

DKIM

Цифровая подпись письма

Проверяет, было ли письмо подписано доменом и не изменилось ли оно в пути.

Поддельные письма часто либо не имеют DKIM, либо подпись некорректна.

DMARC

Политика обработки

Говорит, что делать, если SPF или DKIM не прошли: отклонить, отправить в спам или принять.

DMARC помогает защитить ваш домен от подделки.

Результаты проверки (пример фишингового письма)

```
spf=fail   dkim=none   dmarc=fail
```

Проверка не пройдена

Прохождение проверок не гарантирует безопасность

Злоумышленники могут настроить SPF, DKIM и DMARC для своего поддельного домена. Всегда проверяйте и другие признаки.

КАК ПРОВЕРИТЬ?

Откройте заголовки письма (Show original / View source)

в почтовом клиенте и найдите строки с SPF, DKIM и DMARC. Если вы видите fail — это серьёзный признак подделки.

```
Authentication-Results: mx.google.com
spf=fail (sender IP is not authoriz
dkim=none (no signature)
dmarc=fail (p=none)
```

КИБЕРБЕЗОПАСНОСТЬ

Формы фишинга

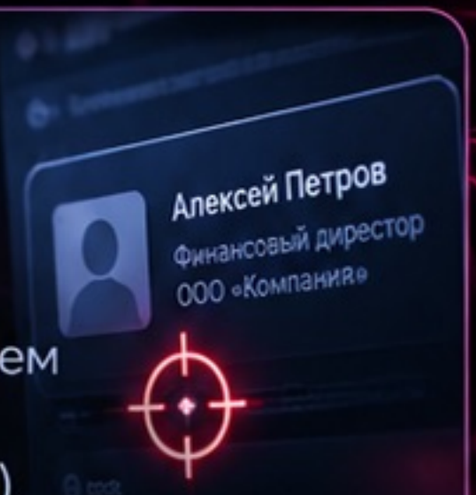
Фишинг — это не один приём, а целый набор методов. Он встречается везде.

Фишинг по email

Массовые письма, которые рассылаются тысячам получателей одновременно.

Целевой фишинг

Направленное письмо именно вам с использованием ваших реальных данных (имя, должность, компания).

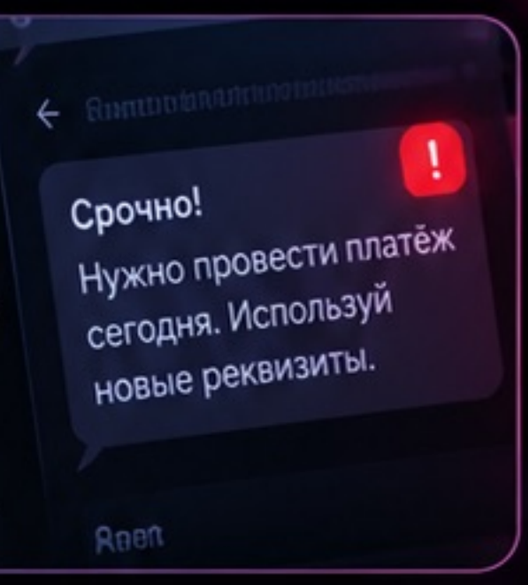


Whaling

Атаки на топ-менеджеров и руководителей с упором на их полномочия и крупные бюджеты.

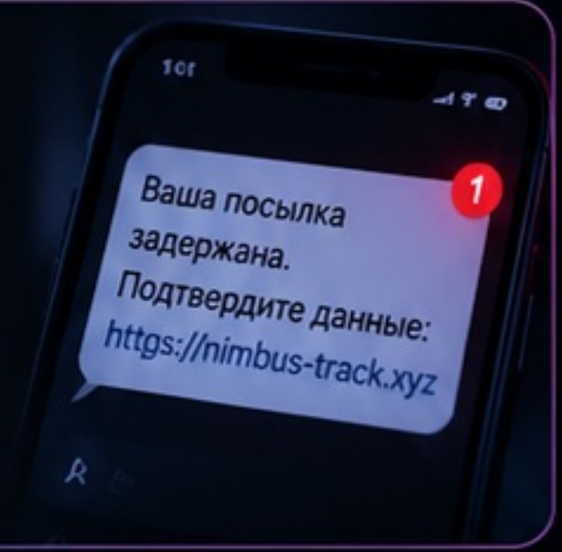
BEC

Поддельный руководитель или поставщик просит совершить платёж или изменить реквизиты.



Smishing

Фишинг через SMS и мессенджеры (например, WhatsApp, Telegram).



Vishing

Телефонные звонки с попыткой обмана, иногда с использованием клонированного голоса.



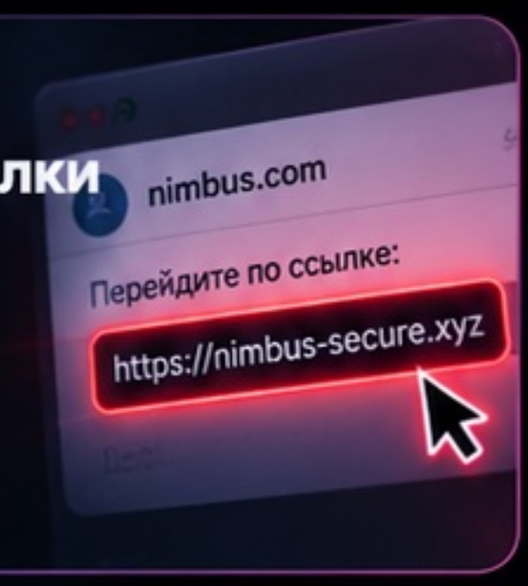
Quishing

QR-код, который ведёт на поддельный сайт.



Фишинг с заменой ссылки

Настоящее письмо копируется, но ссылка внутри подменяется на вредоносную.



КИБЕРБЕЗОПАСНОСТЬ

15/20

Апгрейд ИИ для фишинга

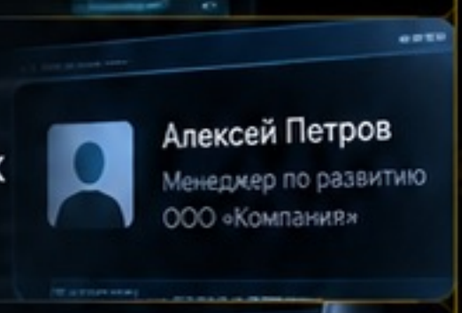
ИИ убрал старые шаблоны. Исчезли не ошибки — исчезла сама ловушка.

Раньше

- ~~Ошибки и странная грамматика~~
- ~~Одно и то же письмо для всех~~
- ~~Подозрительные голосовые сообщения~~
- ~~Несколько копий, которые легко блокировать~~

Сейчас

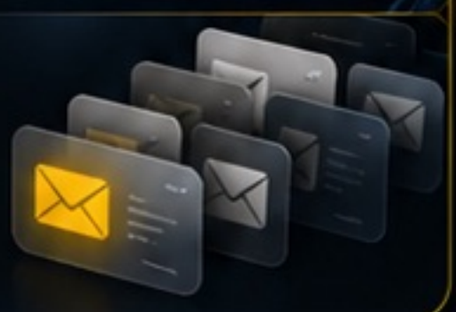
- Грамотный и естественный текст на любом языке благодаря AI
- Персонализированные письма на основе ваших публичных данных



- Клонированные голоса руководителей



- Тысячи уникальных вариантов, которые трудно отследить



ГЛАВНЫЙ ПРИЗНАК ОСТАЁТСЯ ПРЕЖНИМ

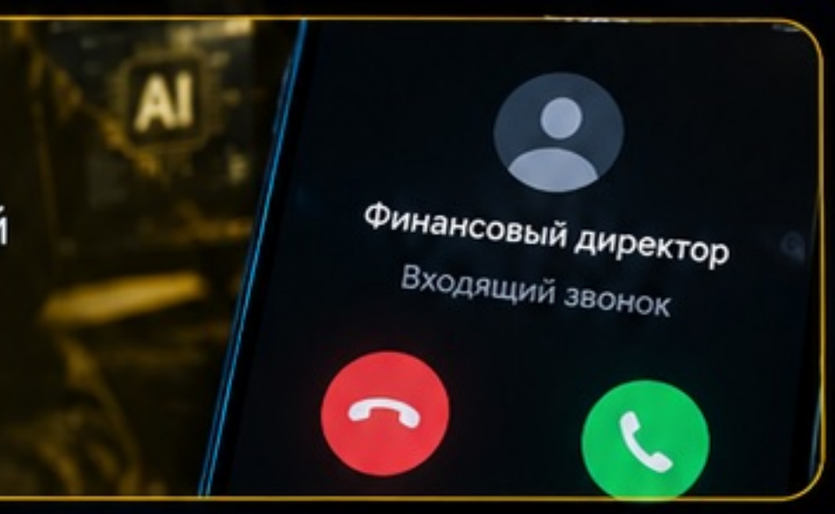
Просьба не меняется.

Проверь запрос

кликнуть · оплатить · войти · поделиться кодом

Как проверить?

Если вам звонят или пишут с срочной просьбой о деньгах — положите трубку и перезвоните по известному номеру.



@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

16/20

Найдите фишинг

Один из этих писем настоящий, другое — фишинговое.
Решите, прежде чем листать дальше.

Настоящее письмо?

Ваш заказ #48213 отправлен

10:12

ParcelNow
<updates@parcelnow.com>

Здравствуйте, Алексей!

Ваша посылка в пути и должна прибыть в четверг.
Вы можете отслеживать её в приложении ParcelNow.



Фишинговое письмо?

Доставка не удалась: требуется действие

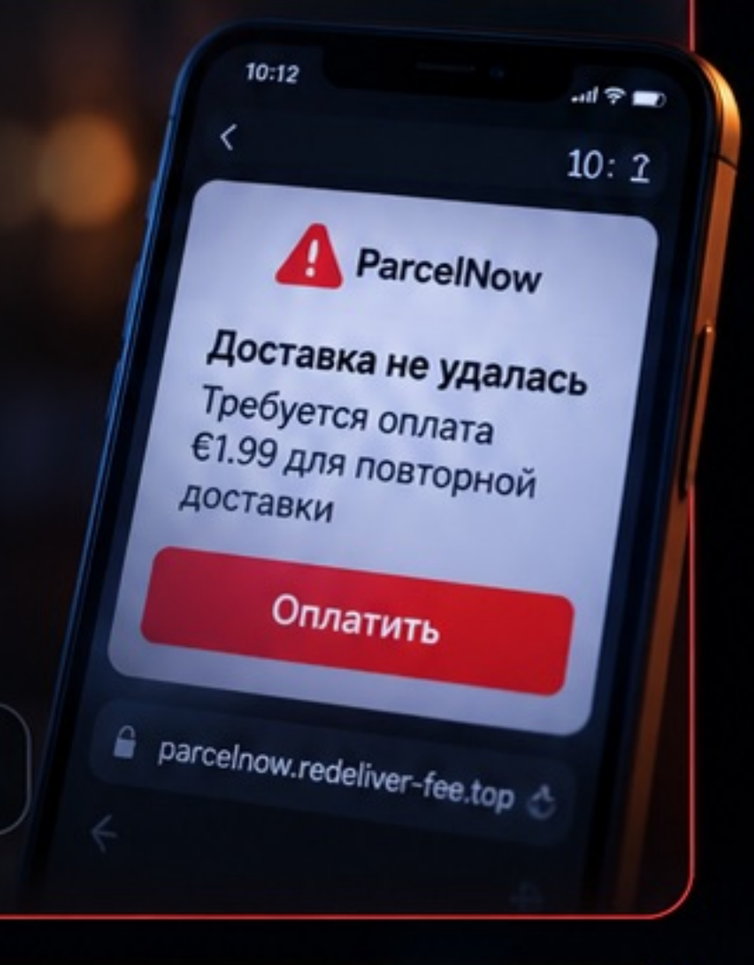
ParcelNow
<support@parcelnow-delivery.info>

Уважаемый клиент!

Мы не смогли доставить вашу посылку. Оплатите €1.99 за повторную доставку в течение 12 часов, иначе она будет возвращена.

Оплатить €1.99 сейчас

parcelnow.redeliver-fee.top/pay



Как проверять?

Смотрите на адрес отправителя, содержание письма и ссылки. Если просят срочно оплатить, перейти по ссылке или что-то ввести — это почти всегда фишинг.

КИБЕРБЕЗОПАСНОСТЬ

17/20

В — это фишинг

Оба письма выглядят похоже, но только одно настоящее. Разберём, как это определить.

✕ Фишинговое письмо

10:12

Доставка не удалась: требуется действие 2

ParcelNow 1
<support@parcelnow-delivery.info>

Уважаемый клиент, 3

Мы не смогли доставить вашу посылку. Оплатите €1.99 за повторную доставку в течение 12 часов, иначе она будет возвращена. 4

Оплатить €1.99 сейчас

parcelnow.redeliver-fee.top/pay 5



1 **Похожий домен**
Адрес выглядит как legit, но домен другой.

2 **Срочная тема**
Создаёт давление, чтобы вы действовали не думая.

3 **Общая приветственная фраза**
Не используется ваше имя.

4 **Жёсткий дедлайн**
Типичный приём для фишинга.

5 **Ссылка на сомнительный домен**
Ведёт на сторонний сайт, а не в приложение.

✓ Настоящее письмо

10:12

Ваш заказ #48213 отправлен

ParcelNow
<updates@parcelnow.com>

Здравствуйте, Алексей!

Ваша посылка в пути и должна прибыть в четверг.
Вы можете отслеживать её в приложении ParcelNow.



✓ Признаки настоящего письма

Официальный домен компании	parcelnow.com
Использует ваше имя и номер заказа	Здравствуйте, Алексей! #48213
Нет подозрительных ссылок и давления	Ведёт в приложение

@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

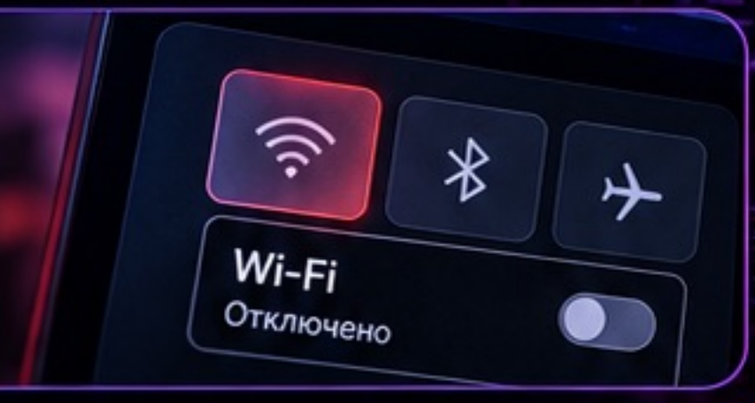
18/20

Уже перешли по ссылке? Действуйте

Ошибаются все. Главное — быстро минимизировать риски и не дать инциденту развиться.

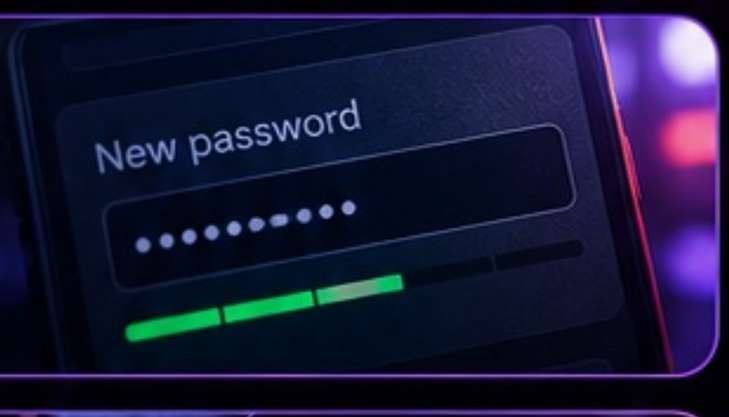
01 Отключитесь от сети

Сразу отключите Wi-Fi или мобильный интернет, чтобы остановить возможную загрузку вредоносного ПО и его распространение.



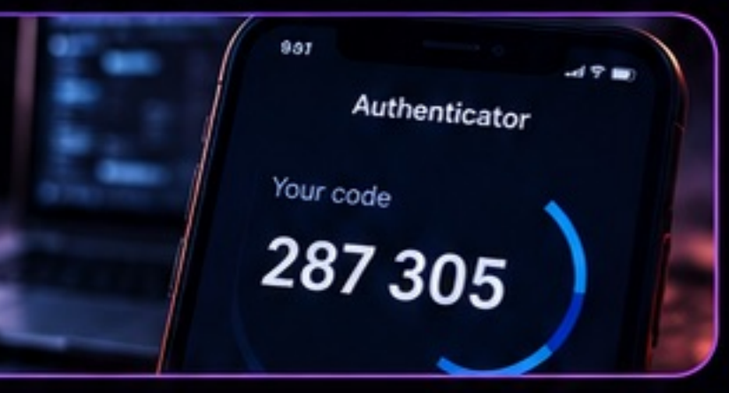
02 Смените пароль

На реальном сайте и везде, где вы его использовали. Начните с самых важных аккаунтов (почта, банк, рабочие сервисы).



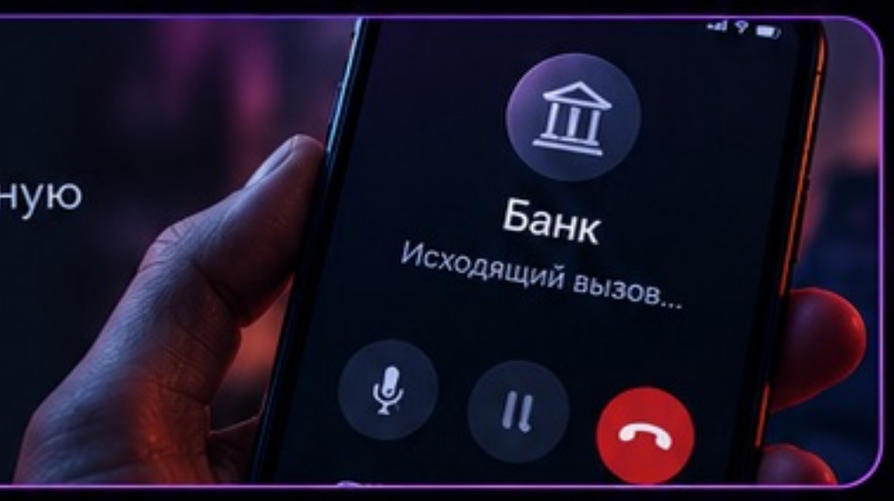
03 Включите MFA

Используйте authenticator app — это сильно снижает риск несанкционированного доступа даже при утечке пароля.



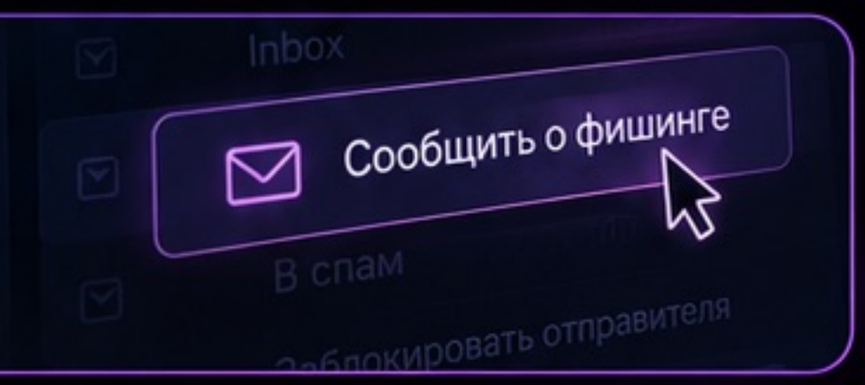
04 Свяжитесь с банком или IT

Если вводили платёжные данные или доверительную информацию — сразу позвоните в банк или внутренний IT-отдел. Используйте номер с карты, сайта или корпоративного intranet, а не из письма.



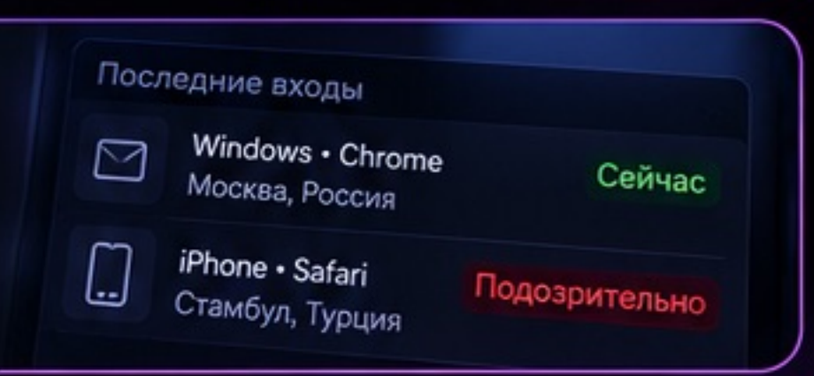
05 Сообщите о письме

Отправьте письмо в Report phishing. Это поможет заблокировать рассылку и защитить других.



06 Проверьте свои аккаунты

В ближайшие недели следите за входами и транзакциями. Убедитесь, что нет подозрительной активности.



@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

19/20

Проверка за 10 секунд

Всего четыре буквы. Прогоняйте их в каждом неожиданном письме.

S Отправитель

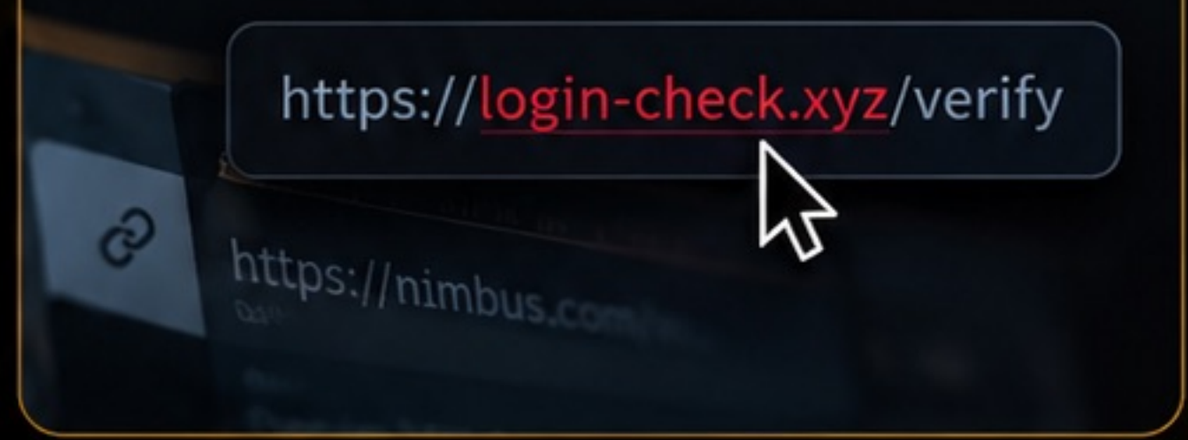
Похож ли адрес на настоящий домен компании?

P ParcelNow
<updates@parcelnow.com>

secure-help.net ≠ nimbus.com

L Ссылки

Куда на самом деле ведёт ссылка? Наведи курсор перед кликом.



A Вложения

Вы ожидали этот файл? Какая у него последняя расширение (extension)?

Statement_Sept.pdf.html
248 KB

M Сообщение

Вызывает ли сообщение срочность, давление или просит деньги/коды?

Срочно!
Нужно оплатить €1.99
в течение 12 часов,
иначе посылка будет возвращена.
10:12

Если есть сомнения — идите напрямую.

Откройте официальное приложение или вручную введите адрес в браузере.



@lionsoulbatyshchikov

КИБЕРБЕЗОПАСНОСТЬ

20/20

Теперь вы читаете email как аналитик.

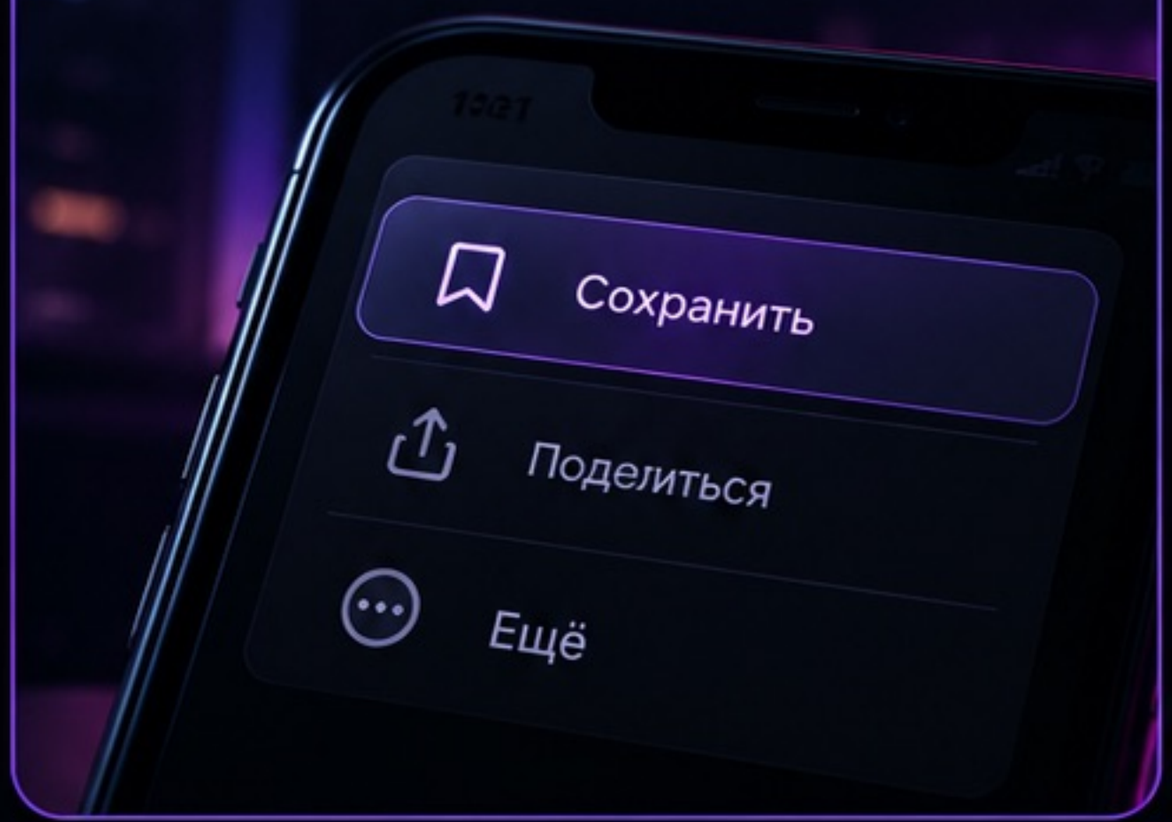
Вы уже умеете замечать ключевые признаки фишинга. Давайте закрепим:

1 2 3 4 5 6 7 8

8 признаков — все найдены

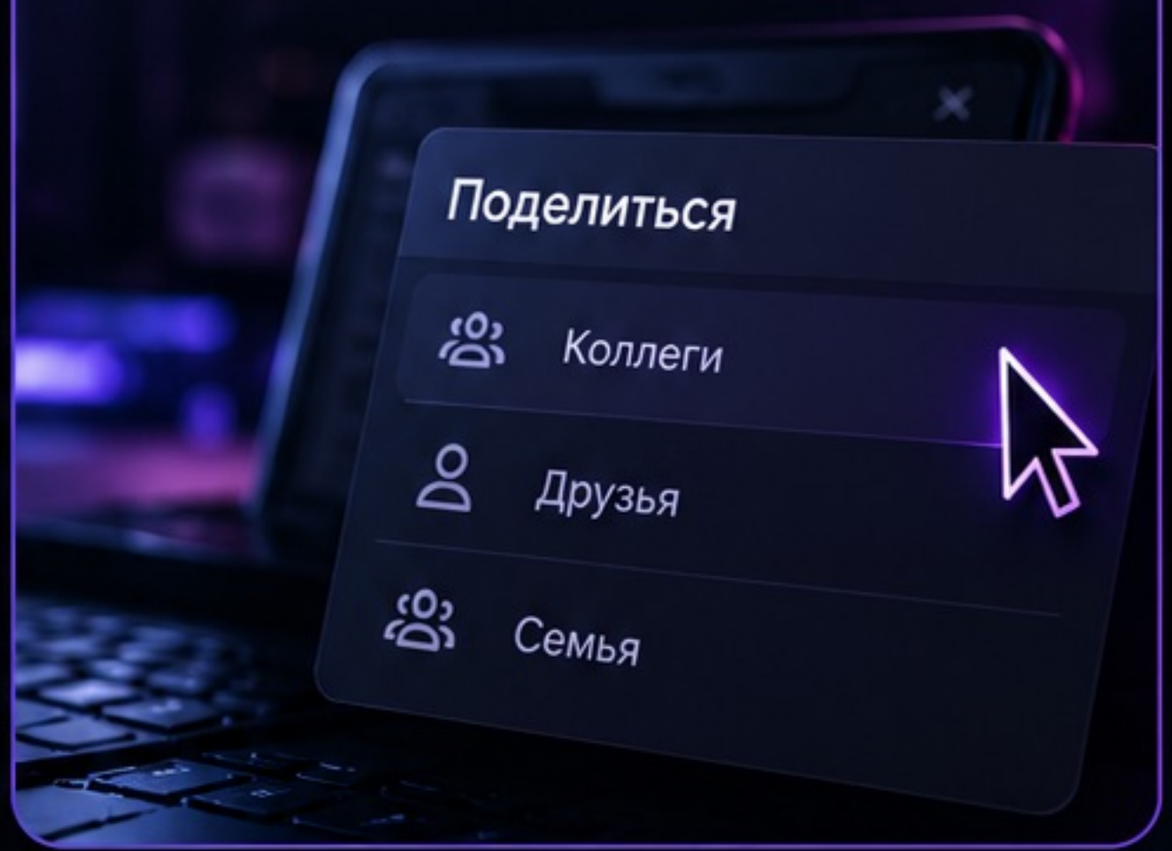
Сохраните

чтобы быстро проверить в следующий раз



Поделитесь

с тем, кто кликает на всё подряд



СЛЕДИТЕ ЗА НОВЫМИ РАЗБОРАМИ

Практические советы, реальные примеры и свежие техники от кибербезопасников.

@lionsoulbatyshchikov