



Основы безопасного поведения в сети

Инструкция специалиста



Почему безопасность в сети важна?

Киберпреступность стремительно растет.

В 2024 году количество преступлений с применением IT-технологий достигло **765,4 тыс. случаев**, что на **13,1%** больше, чем в 2023 году.

Доля IT-преступлений среди всех преступлений также увеличилась: **с 25% в 2020 году до 40% в 2024 году**. И по прогнозу экспертов она увеличится до 50% в течение двух следующих лет.

Что вы узнаете сегодня

1. Основные угрозы в сети
2. Технологические методы защиты
3. Практические рекомендации

Основные понятия

- 1. Кибербезопасность** — это защита данных, устройств и сетей от кибератак.
- 2. Киберпреступность** — это преступления, совершаемые с использованием цифровых технологий: интернет, сотовый телефон, нейросети и тому подобное.
- 3. Цифровая гигиена** — это набор правил и привычек, которые помогают минимизировать риски в сети.

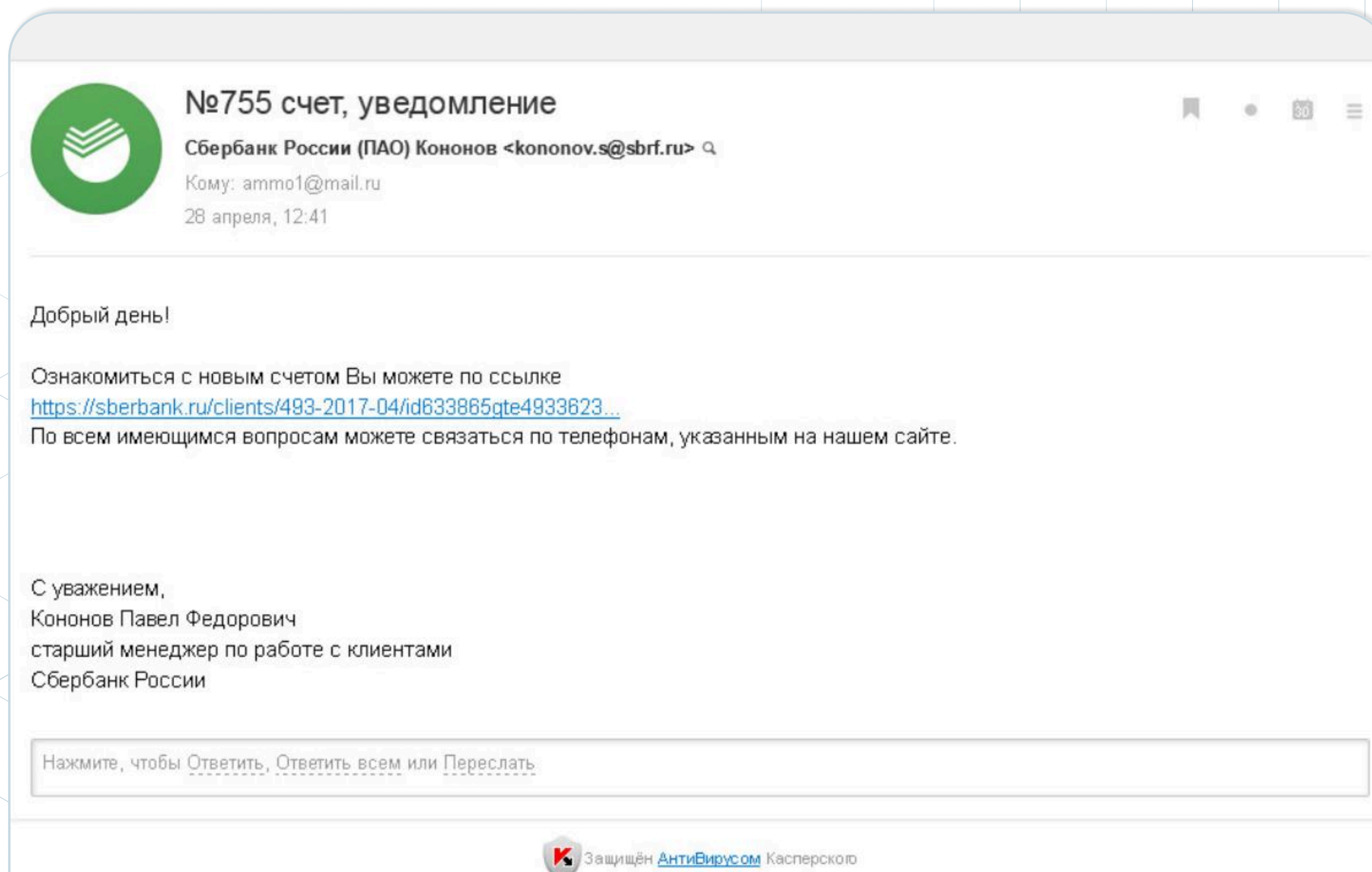
Основные угрозы в сети

Что угрожает вам и как это работает?



Фишинг: что это и как работает?

Фишинг — это метод, при котором мошенники пытаются получить ваши данные, выдавая себя за доверенный источник



Фишинговый сайт

 СберБанк

×

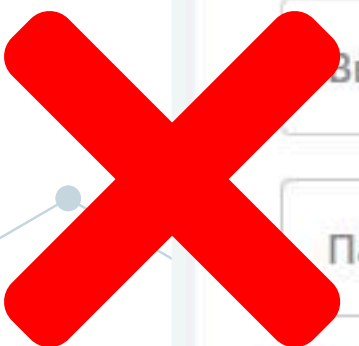
+

←

→

↻

 http://online.sberblank.ru



Вход в СберБанк Онлайн

Логин Телефон Номер карты

Введите логин

Пароль

☒ Запомнить меня

Забыли логин или пароль?

Войти

Нет карты Сбербанка

 СберБанк

×

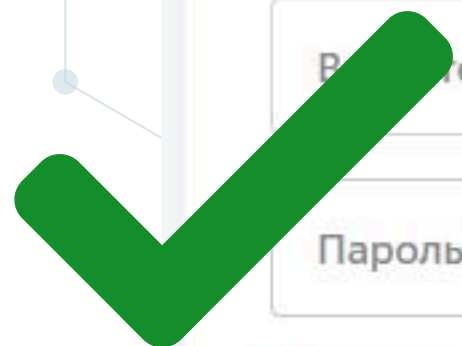
+

←

→

↻

 SberBank of Russia OJSC [RU] https://online.sberbank.ru



Вход в СберБанк Онлайн

Логин Телефон Номер карты

Введите логин

Пароль

☒ Запомнить меня

Забыли логин или пароль?

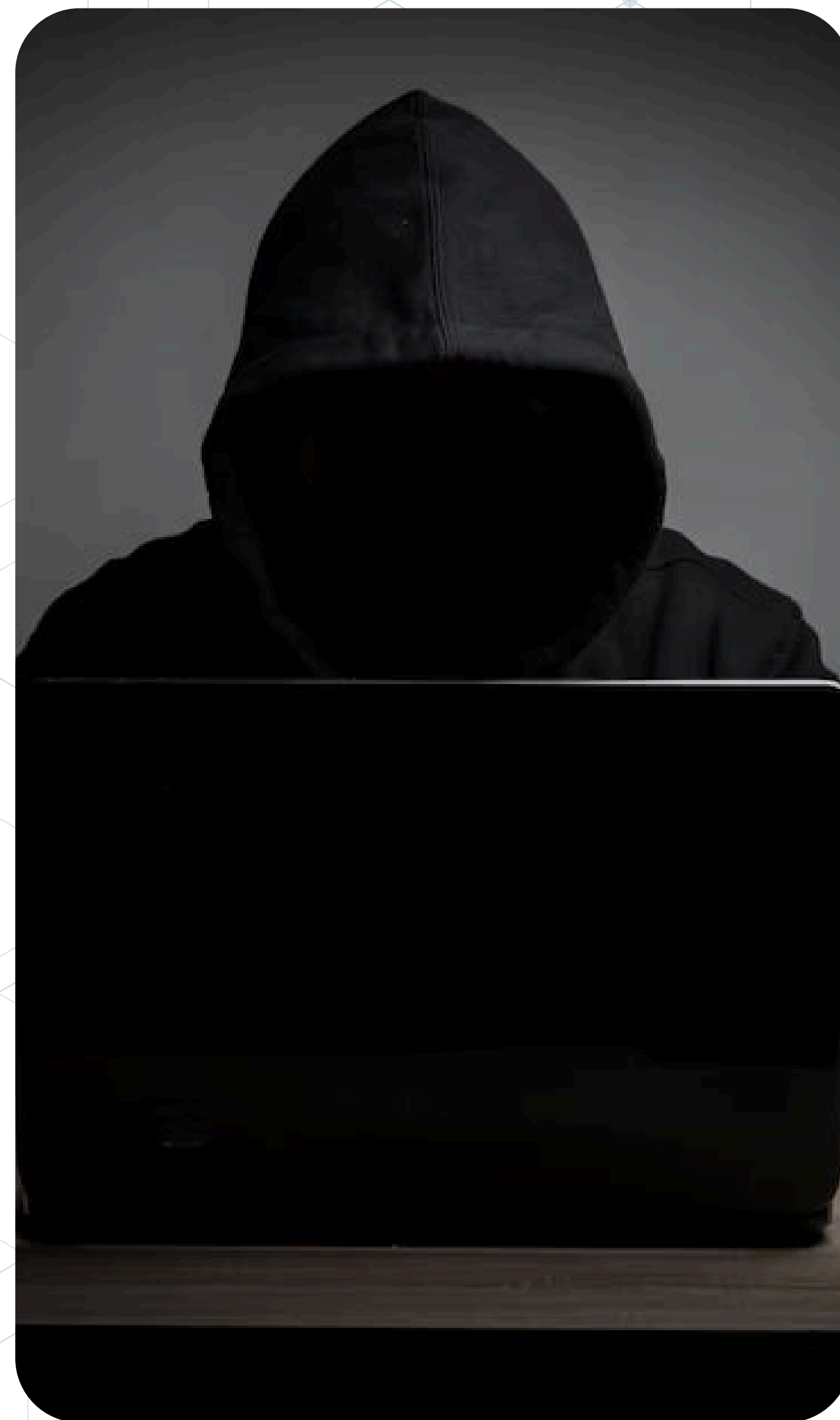
Войти

Нет карты Сбербанка

Профайлинг

— это процесс сбора и анализа информации о человеке или группе людей, чтобы составить подробный профиль их поведения, предпочтений и привычек. Этот подход позволяет создавать психологические, социальные или коммерческие портреты.

С помощью профайлинга мошенники могут создавать индивидуализированные сообщения или письма, которые выглядят так, будто они отправлены от знакомых или доверенных организаций.



Как распознать, что это фишинговое письмо?

1. Вы не ждали это письмо. Вы не знаете отправителя лично

**2. В письме — проблема или срочный вопрос.
Вы узнали о проблеме из этого письма**

От вас требуется срочное действие

3. Вас просят перейти по ссылке

Всегда проверяйте информацию. Не спешите.

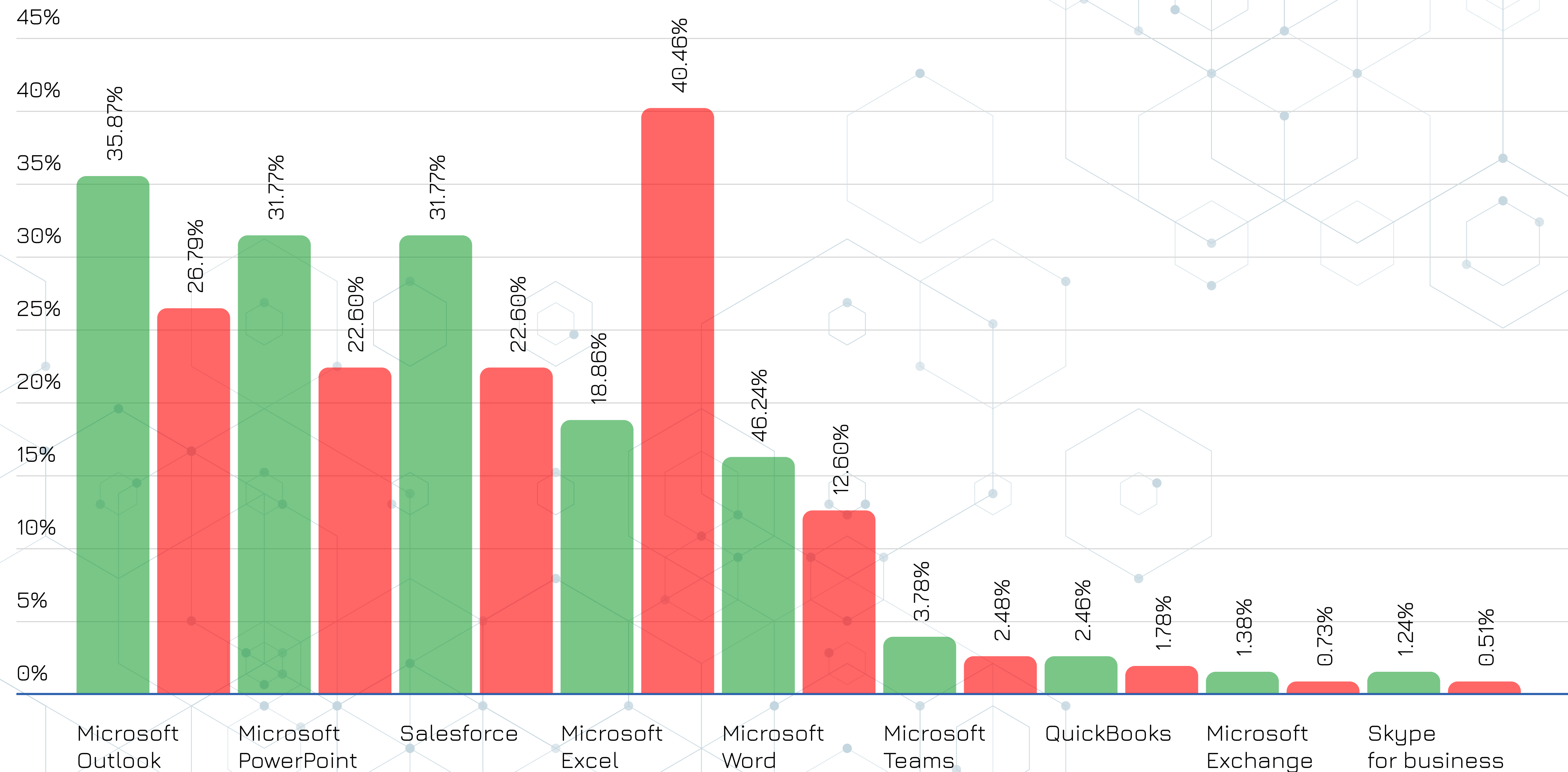
Последствия фишинга

Levitas capital - австралийский хедж-фонд закрылся
всего из-за одной ссылки.

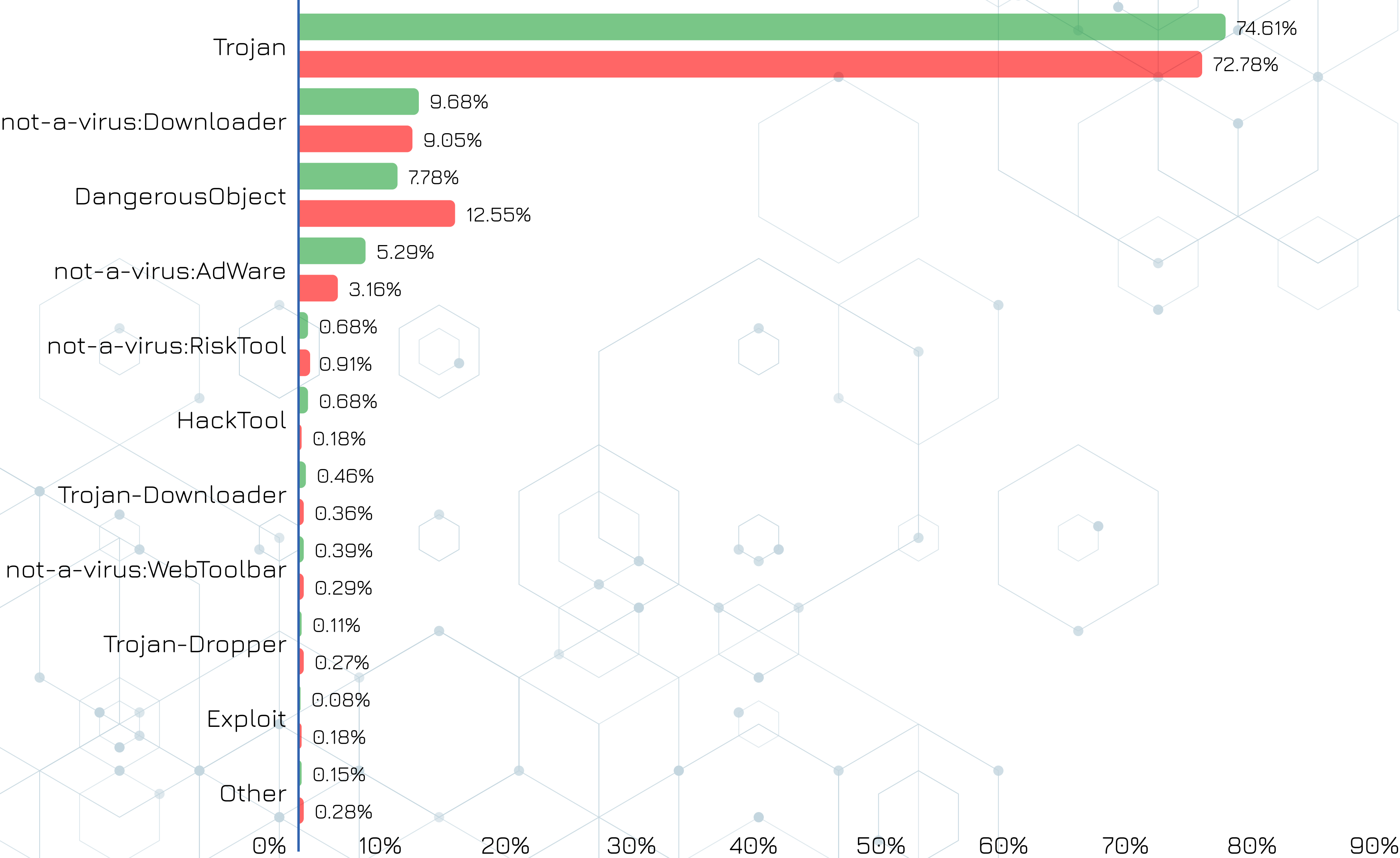
Это был **Whaling**.



Вредоносное ПО



Немного цифр



Ущерб от NotPetya

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7 [REDACTED] BWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

NjjH [REDACTED] P5

If you already purchased your key, please enter it below.

Key:

Вишинг и Смишинг:

Телефонные и угрозы в мессенджерах

Вишинг: Звонок «из банка» с просьбой сообщить код

Смишинг: SMS или сообщение в мессенджере с подозрительной ссылкой

Вишинг (Vishing – Voice Phishing)

◆ Что это?

Мошенники используют телефонные звонки, чтобы обманом заставить жертву выдать конфиденциальные данные (пароли, данные карт, коды из SMS)

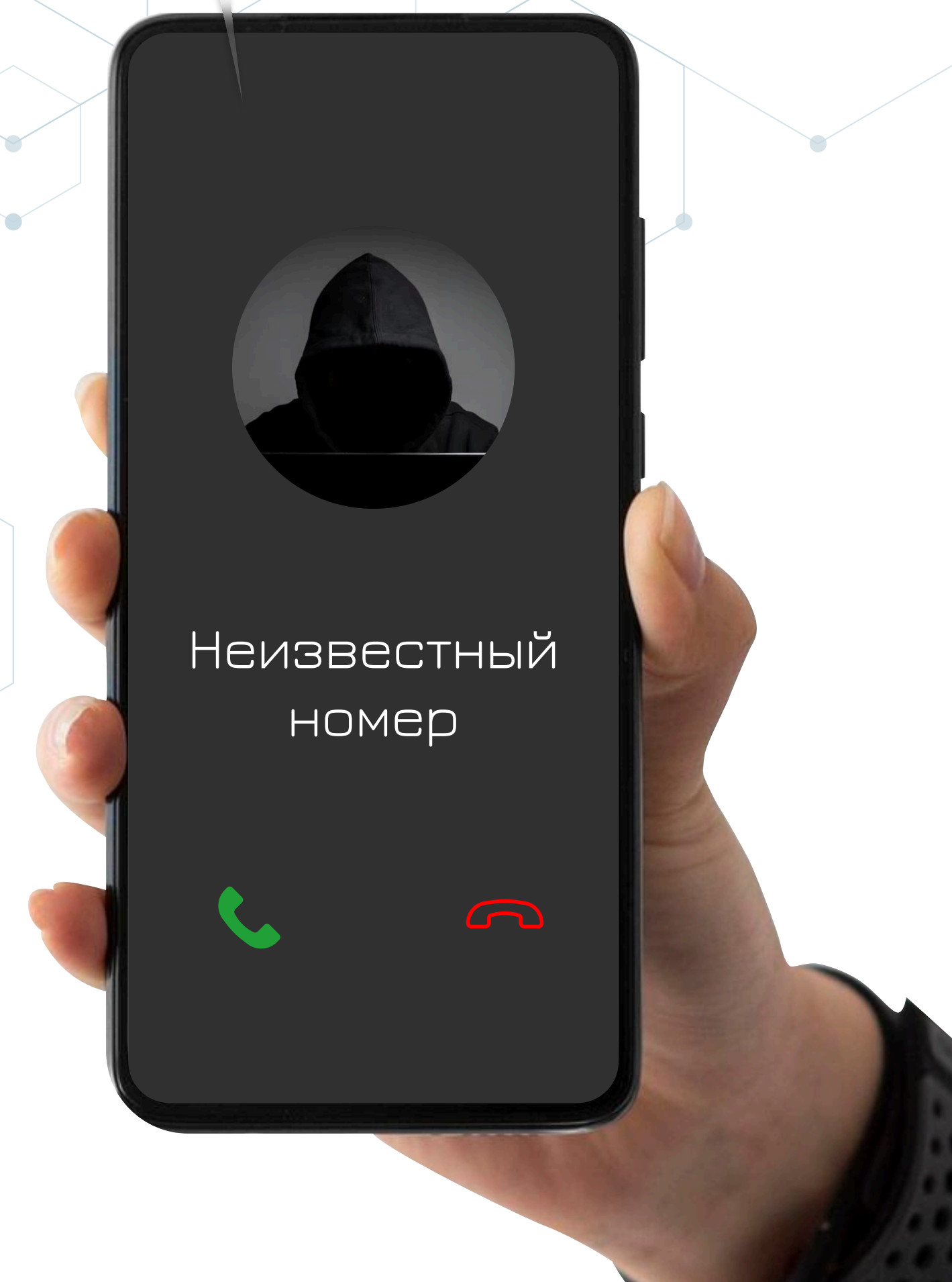
◆ Как работает?

- Представляются сотрудниками банка, техподдержки, правоохранительных органов
- Сообщают о «проблеме» (мошеннические операции, блокировка карты)
- Убеждают назвать личные данные или перевести деньги

◆ Пример:

**«Здравствуйте, это служба безопасности банка!
На вашем счете подозрительная операция.
Подтвердите данные карты!»**

Здравствуйте,
это служба безопасности...



Вот еще пример

Звонок с номера, похожего на ведомственный

– Здравствуйте, майор [Фамилия], говорит капитан Сидоров из Главного управления. У нас срочная ситуация, связанная с выполнением задач в зоне СВО. Ваше подразделение включено в список для экстренного развертывания

– **Согласно новым распоряжениям, необходимо пройти обязательную проверку безопасности.**

Нам нужно подтвердить вашу личность и доступ к закрытым каналам связи

– В целях идентификации продиктуйте последние 4 цифры вашего служебного удостоверения и пароль от рабочего аккаунта. Также направьте SMS с кодом, который вам сейчас придет, для активации защищенного доступа. Это необходимо для оформления приказа в системе

Дополнительные сценарии вишинга:

- ◆ «Ваши коллеги уже подтвердили данные, не задерживайте процесс!»
- ◆ «У вас выявлены подозрительные транзакции, срочно продиктуйте код из SMS для проверки.»
- ◆ «На ваше имя поступил приказ о командировке в зону СВО, подтвердите готовность и укажите данные банковской карты для начисления выплат.»

Смишинг (Smishing – SMS Phishing)



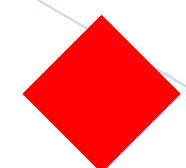
Что это?

Мошенничество через SMS или мессенджеры, направленное на получение персональных данных или установку вредоносного ПО



Как работает?

- Жертве приходит SMS с просьбой перейти по ссылке или отправить ответное сообщение
- Ложные сообщения о доставке, штрафах, блокировке аккаунта
- Ссылка ведет на фейковый сайт или заражает устройство вирусом



Пример:

«Ваша посылка задержана. Подтвердите данные по ссылке: [вредоносная ссылка]»

iMessage
Сегодня 07:57

Новый логин [usdt[REDACTED].com] новая
учетная запись: maddie, пароль:
[REDACTED], баланс: 4 440
582.73U.SDT, пожалуйста, никому
не сообщайте эту информацию.
Ответьте R, чтобы отменить.

← +79 [REDACTED]
В сети: сегодня в 9:43

Сегодня

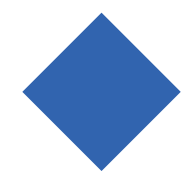
ВТБ
ЕСМС 20/09/2018 12:25:59
Оплата покупки с Вашей
банковской карты на сумму
13390 RUB выполнена успешно/
OZON.RU Платёж будет
выполнен в течение суток.
Если Вы не совершали
данный платеж, просьба
обратиться в отдел финансовой
безопасности банка по
телефону: +7 (499) [REDACTED]

13:26

Другие возможные сценарии Смишинга



«[Фамилия Имя], ваш военный билет требует срочного обновления в цифровой системе МО РФ. Перейдите по ссылке для загрузки данных.»



«Система безопасности зафиксировала подозрительный вход в ваш личный кабинет МО РФ. Подтвердите личность, перейдя по ссылке: [link].»



«На ваше имя поступил приказ о награждении. Подробности и форма подтверждения: [link].»

Масштаб проблемы

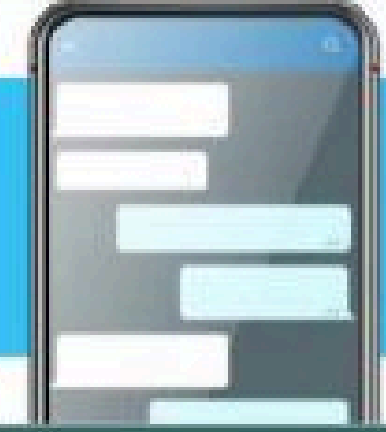
НЕЖЕЛАТЕЛЬНЫЕ ЗВОНКИ И СМС: **МАСШТАБ ПРОБЛЕМЫ**



Скажите, в последние полгода-год Вам лично звонили или поступали СМС-сообщения от телефонных мошенников? Вы можете дать один или два ответа (закрытый вопрос, до двух ответов, в % от всех опрошенных)



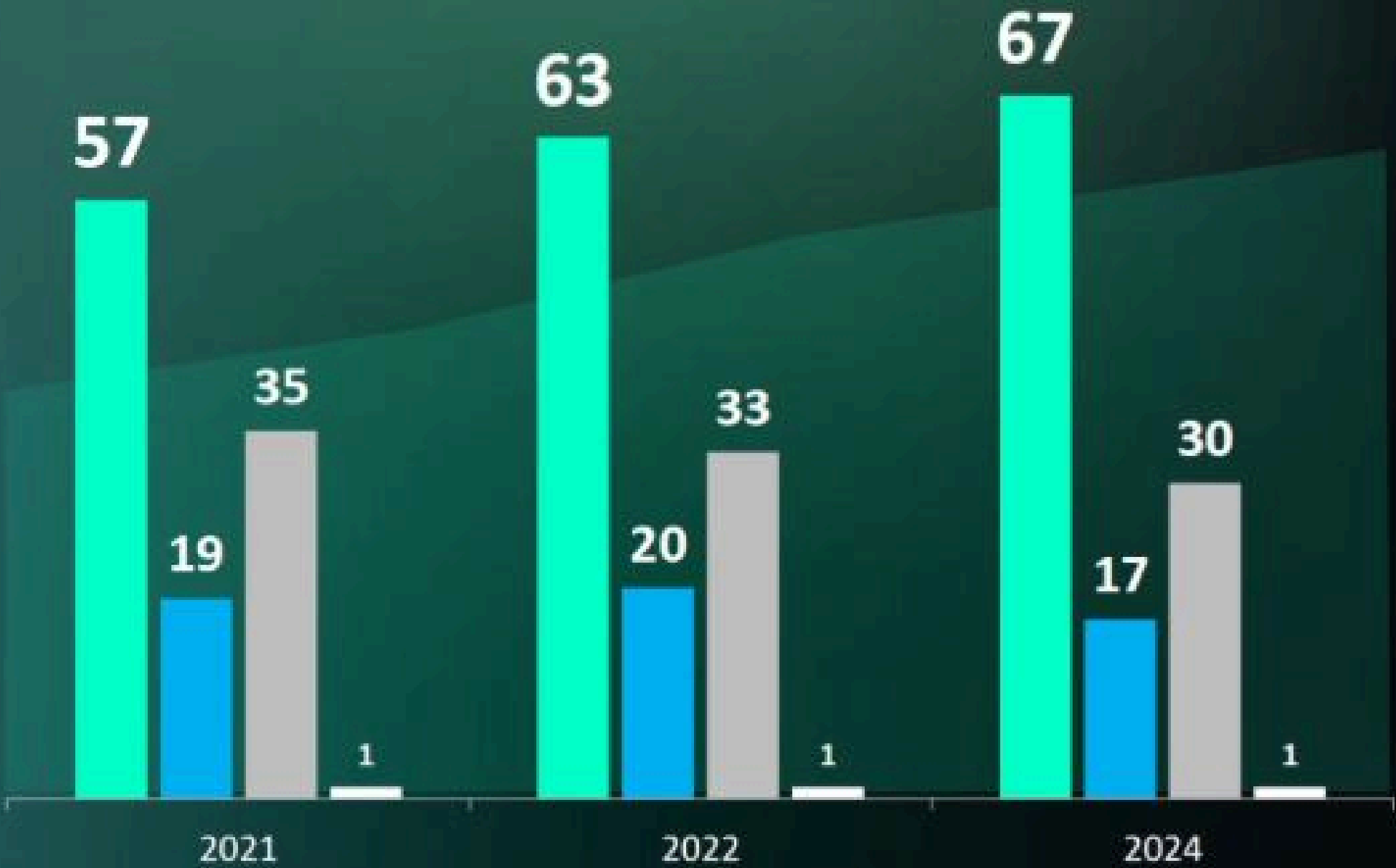
Были звонки



СМС-сообщения

Ничего такого не было

Затруднились ответить



Всероссийский телефонный опрос «ВЦИОМ-Спутник» проведен 2 февраля 2024 г.

Наиболее частые сценарии

◆ **Схема 1. Операторы сотовой связи**

«действие вашей сим карты заканчивается, какой у вас оператор связи? Продиктуйте код из СМС»

◆ **Схема 2. Общение с работодателем**

«Заполните анкету в ходе нашего общения. Укажите данные банковской карты для перечисления будущей зарплаты.

«Предоставьте персональные данные для бухгалтерии/кадровика»

◆ **Схема 3. Звонки или сообщения от знакомых**

«Я в беде, связи нет, говорить не могу, нужны деньги»

«Проголосуйте за мою племянку вот по этой ссылке»

Наиболее частые сценарии

◆ **Схема 4. Оплата услуги по фейковому QR коду**

Человеку предоставляют QR код с неофициального сайта и предлагают оплатить услугу «через камеру гаджета»

◆ **Схема 5. Звонки и сообщения из банка**

«Сейчас у вас списываются деньги. Замечаем в последние Дни странные операции по вашей карте, вам надо опередить мошенников и спрятать свои средства на безопасном счету»

◆ **Схема 6. Звонки и сообщения от государственных ведомств**

Вам звонит следователь/дознаватель/судебный пристав/ оперативник ФСБ. «На вас заведено уголовное дело «продиктуйте ваши данные, я все проверю»

Последствия вишинга и смишинга

Санкт-Петербург, 7 июня, 2024, 11:31 — ИА Регнум. Потери денежных средств россиян от телефонного мошенничества могут достигать 250 млрд рублей в год. Об этом заявил на собственной сессии Сбера в рамках Петербургского международного экономического форума заместитель председателя правления Сбербанка **Станислав Кузнецов**.

Немного цифр

1. Бизнес и государство теряют в среднем 5,5 миллиона рублей на одном инциденте утечки (Данные Касперски)

С утечками информации чаще всего сталкиваются компании из следующих сфер:

- продажи (37%)
- финансовый сектор (20%)
- игровая индустрия (10%)

2. В марте прошлого года В.В. Путин сообщил:

“Совокупный ущерб от кибермошенничества в России в 2023 составил более 200 млрд рублей, тогда как раскрываемость таких преступлений снизилась до 23%”

3. 1. До 100 дней составляет сейчас среднее время обнаружения проникновения в корпоративные информационные системы с момента взлома, утверждают инженеры Microsoft. При этом лишь:

- 25% жертв хакеров-злоумышленников предпринимали какие-либо меры безопасности
- 75% даже не обновляли операционную систему и не ставили апдейты с «лечением» потенциальных уязвимостей

Как защититься?

- ◆ **Не отвечать** на подозрительные звонки/SMS
- ◆ **Не переходить** по ссылкам из непроверенных источников
- ◆ **Внимательно проверяйте** ссылки на ошибки
- ◆ **Не сообщать** персональные данные по телефону
- ◆ **Проверять информацию** через официальные контакты (банк, госуслуги и т. д.)

Фейковые аккаунты

◆ Создание фейкового аккаунта с нуля

◆ Клонирование профиля

◆ Взлом аккаунта

Как Илон Маск, Apple и Билл Гейтс обманули людей



Как защититься от этого?

1. Вообще никогда не открывайте ни подарки в соц.сетях, ни ссылки, ни переходите на сайты
!Особенно в рабочем профиле!
2. Совершайте видеозвонок, когда у вас просят деньги, и у вас есть желание их отправить
3. Если вам показалось, скорее всего вам не показалось
4. Используйте сложные пароли и двухфакторную аутентификацию, чтобы защититься от взлома
5. Отключите автозагрузку медиа в мессенджерах

Приложения для хранения паролей



Bitwarden



RoboForm



Dashlane

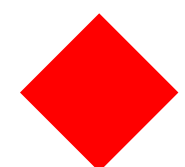


KeePass

Целевой фишинг: атака на вас лично

Как работает атака?

- ◆ В отличие от массового фишинга, где мошенники рассылают одинаковые сообщения многим пользователям, **spear phishing** — это персонализированная атака
- ◆ Злоумышленники собирают информацию о жертве (работа, друзья, интересы) и создают доверительное сообщение
- ◆ Обычно такие атаки направлены на сотрудников компаний, госслужащих, военных



Пример:

«Здравствуйте, [Имя]! Мы обновляем систему безопасности вашего личного кабинета МО РФ. Для подтверждения личности пройдите авторизацию: [ссылка]»

Как защититься?

- ◆ Всегда проверяйте адрес отправителя сообщения
- ◆ Никогда не переходите по подозрительным ссылкам, даже если они выглядят официально
- ◆ Подтверждайте важную информацию через официальные каналы связи
- ◆ Используйте корпоративные email-адреса только по работе, не привязывайте их к соцсетям

Почему вас это может коснуться?

Telegram-канал Baza сообщает, что телефонные мошенники обманули 65-летнего генерал-лейтенанта ФСБ в отставке Героя России Николая Гаврилова. Ссылаясь на собственные источники, авторы канала уточнили, что злоумышленники представились генералу членами Российской ассоциации героев и обманули офицера на 1,5 млн рублей, Гаврилов обратился с заявлением в полицию, по факту случившегося проводится проверка.

Мошенники развели на 19,5 млн генерал-лейтенанта в отставке

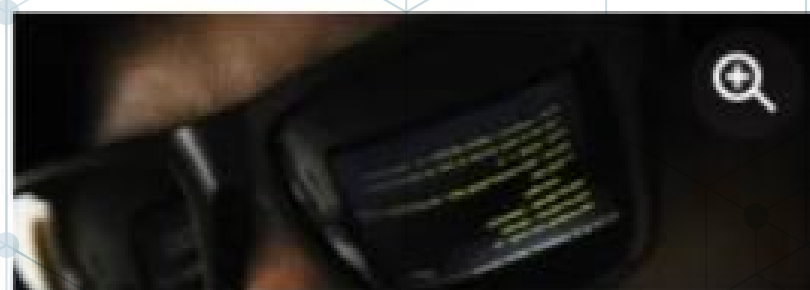


Константин Чуйкин

06 февраля 2025 в 14:46



Размер текста 18



Генерал-лейтенант в отставке Герман Гриднев отдал телефонным мошенникам около 19,5 млн рублей. Об этом сообщили в правоохранительных органах.

Генерала обманули на 50 миллионов рублей, назначая встречи прямо у прокуратуры и посольства Мадагаскара

Начальник финансовой службы Центрального аппарата Министерства обороны СССР Миренков и его жена оказались жертвами мошенников. Генералу объяснили, что в России орудуют аферисты, которые похищают деньги граждан и отправляют их на Украину, а для убедительности ему позвонил «сотрудник ФСБ».

Мошенники прислали Миренкову документы якобы от ЦБ, где было указано, что генерал стал жертвой преступников, и теперь его сбережения под угрозой. Генералу вызывали такси, за несколько дней он передал мошенникам десятки миллионов рублей: отставной военный снимал деньги в разных банках и отдавал сумки, набитые наличкой, из рук в руки.

Одну из встреч мошенники назначили у Генпрокуратуры на Большой Дмитровке, другую — у посольства Мадагаскара. Также звучал и пароль, который курьер назвал Миренкову. Лишь через неделю генерал с женой догадались, что их обманули.

👍 Лайк 97 🔄 171

7 фев 2024

Анонимность в сети: кто вас слушает, как вас отслеживают и как защититься

Мы живем в эпоху тотальной цифровой слежки,
где **каждое** наше слово, **каждое** действие
в интернете может быть **зафиксировано**,
проанализировано и **использовано**



Кто прослушивает?

1. Государственные структуры

- Разведывательные службы (ФСБ, АНБ, ЦРУ) анализируют коммуникации в целях национальной безопасности
- В ряде стран включая РФ, операторы связи обязаны хранить данные звонков и сообщений пользователей

Кто прослушивает?

1. Государственные структуры

- Разведывательные службы (ФСБ, АНБ, ЦРУ) анализируют коммуникации в целях национальной безопасности
- В ряде стран включая РФ, операторы связи обязаны хранить данные звонков и сообщений пользователей

2. Корпорации

- Google, Facebook, Apple и другие собирают данные о ваших действиях и предпочтениях для рекламы
- Смарт-колонки (Алиса, Siri, Google Assistant) могут включаться без вашего ведома и отправлять данные

Кто прослушивает?

1. Государственные структуры

- Разведывательные службы (ФСБ, АНБ, ЦРУ) анализируют коммуникации в целях национальной безопасности
- В ряде стран включая РФ, операторы связи обязаны хранить данные звонков и сообщений пользователей

2. Корпорации

- Google, Facebook, Apple и другие собирают данные о ваших действиях и предпочтениях для рекламы
- Смарт-колонки (Алиса, Siri, Google Assistant) могут включаться без вашего ведома и отправлять данные

3. Киберпреступники

Используют поддельные мобильные приложения для доступа к микрофону и камере.
Перехватывают звонки через уязвимости в сетях связи

Кто прослушивает?

1. Государственные структуры

- Разведывательные службы (ФСБ, АНБ, ЦРУ) анализируют коммуникации в целях национальной безопасности
- В ряде стран включая РФ, операторы связи обязаны хранить данные звонков и сообщений пользователей

2. Корпорации

- Google, Facebook, Apple и другие собирают данные о ваших действиях и предпочтениях для рекламы
- Смарт-колонки (Алиса, Siri, Google Assistant) могут включаться без вашего ведома и отправлять данные

3. Киберпреступники

Используют поддельные мобильные приложения для доступа к микрофону и камере.
Перехватывают звонки через уязвимости в сетях связи

4. Конкуренты

В бизнесе могут использоваться методы промышленного шпионажа для сбора информации о переговорах

Как вы оставляете “цифровой след”?

1. Социальные сети

- Лайки, комментарии, геолокация, подписки — все это создает ваш цифровой профиль
- Даже удаленные сообщения и публикации могут сохраняться в базе данных платформ

2. Гаджеты

- Смартфоны с Android и iOS ведут постоянный мониторинг геолокации
- Камеры ноутбуков и телефонов могут быть взломаны и использоваться для наблюдения

3. Поисковые запросы

- Запросы в Google и Яндекс помогают составить ваш психологический портрет
- Спецслужбы могут запросить доступ к истории браузера

4. Банковские транзакции

- Системы скоринга отслеживают, как и где вы тратите деньги
- Цифровые кошельки (Apple Pay, Google Pay) собирают данные о покупках

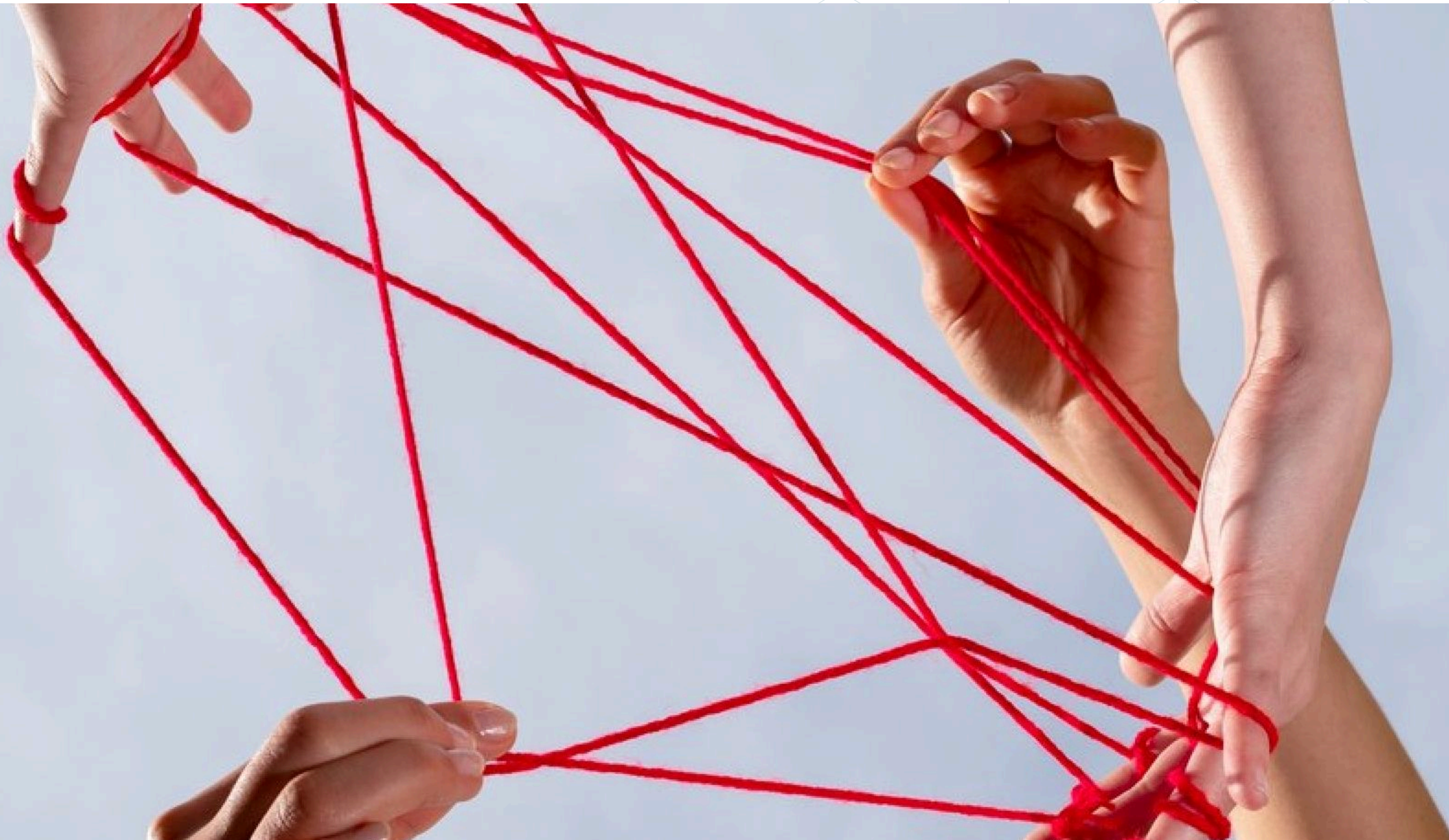
Как это может быть использовано против вас?

Кража личности и подделка документов



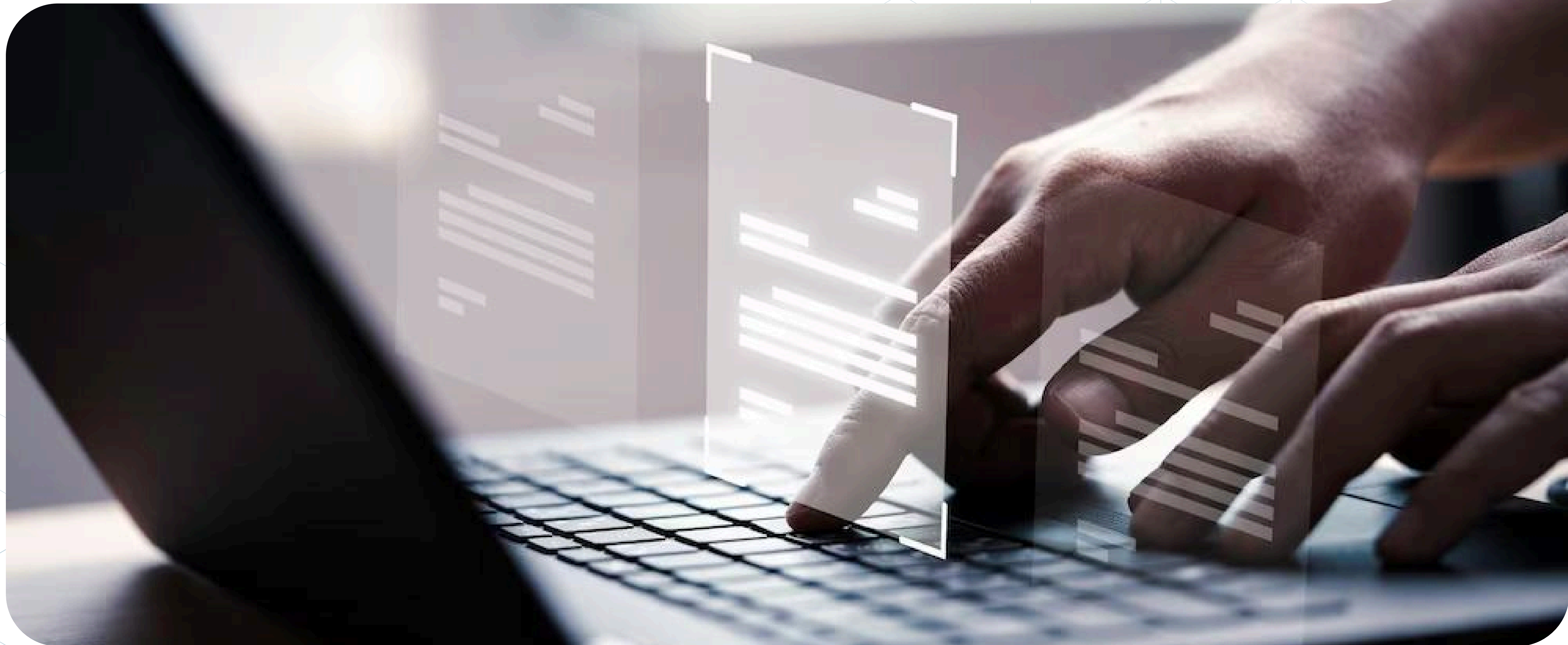
Как это может быть использовано против вас?

Манипуляция вашим мнением (социальная инженерия, политическая пропаганда)



Как это может быть использовано против вас?

Вымогательство, шантаж и утечка личной информации



Как это может быть использовано против вас?

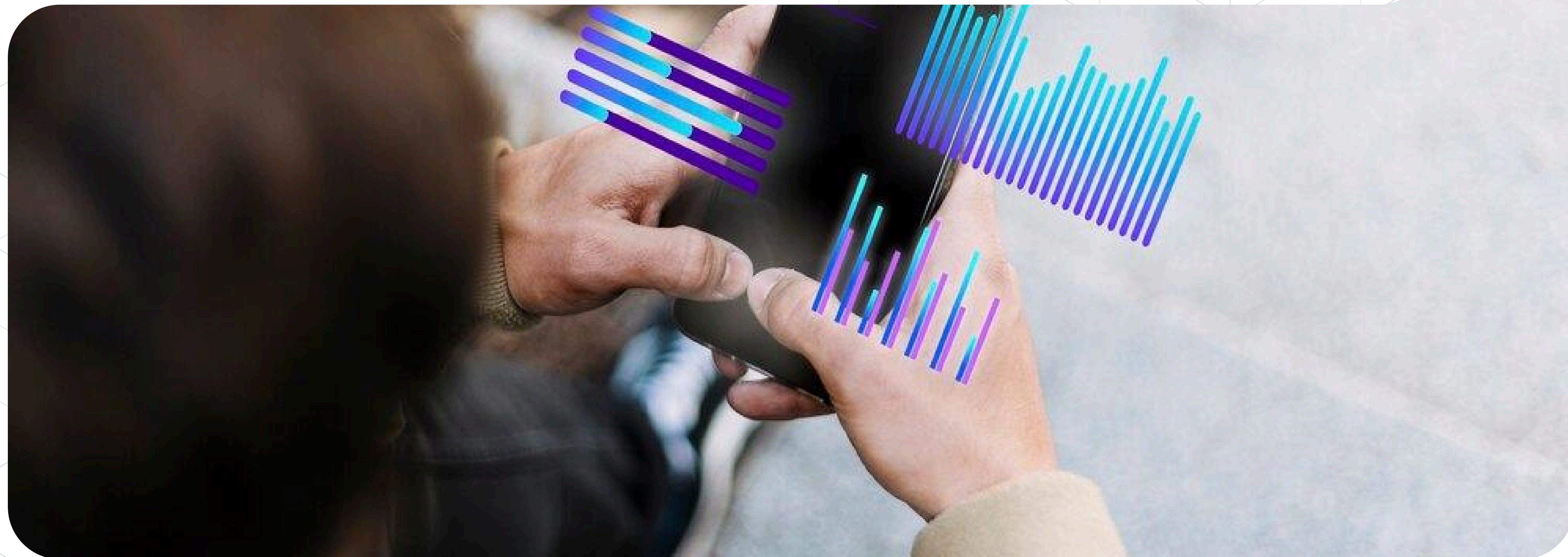
Подделка личности и кража аккаунтов



Как это может быть использовано против вас?

Утечка геолокации и слежка за передвижениями

Прослушка смартфона и сбор данных через микрофон



Мини-квест на цифровую безопасность

1. Проверьте, к каким приложениям у вас включен доступ к микрофону?

Мини-квест на цифровую безопасность

1. Проверьте, к каким приложениям у вас включен доступ к микрофону?

**2. Теперь к фото
Что значит полный доступ?**

Мини-квест на цифровую безопасность

1. Проверьте, к каким приложениям у вас включен доступ к микрофону?

**2. Теперь к фото
Что значит полный доступ?**

3. У кого один и тот же пароль более чем к 2-3 сайтам или ЛК?

Проверьте свои почты и логины на этом сайте

https://haveibeenpwned.com

';--have i been pwned?

Check if your email address is in a data breach

email address

pwned?

Using Have I Been Pwned is subject to [the terms of use](#)

877
pwned websites

14,949,300,875
pwned accounts

115,799
pastes

229,165,825
paste accounts

Largest breaches

-  772,904,991 [Collection #1 accounts](#)
-  763,117,241 [Verifications.io accounts](#)
-  711,477,622 [Onliner Spambot accounts](#)
-  623,161,853 [B... ..](#)

Recently added breaches

-  1,977,011 [SpyX accounts](#)
-  672,546 [Lexipol accounts](#)
-  220,503 [Color Dating accounts](#)
-  22,204 [Flat Earth Sun, Moon and Zodiac](#)

Что делать, чтобы стать “невидимкой” в сети?



Использовать VPN(iVPN, FoxRay) — скрывает ваш IP-адрес и шифрует интернет-трафик



Анонимные браузеры (Tor/Dolphin) — позволяет анонимно выходить в сеть, маршрутизируя трафик через несколько



Анонимные поисковики:

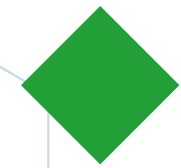
- DuckDuckGo — не отслеживает запросы.
- Startpage — анонимизирует запросы через Google

Что делать, чтобы стать “невидимкой” в сети?



Обход трекеров и куки:

- Используйте браузеры с блокировкой трекинга (Brave, Dolphin, Firefox с расширениями типа uBlock Origin)
- Очищайте cookies и кэш после посещения сети



Шифрование данных:

- Используйте зашифрованные мессенджеры (Signal, Telegram с секретными чатами)
- Храните пароли в менеджерах (Bitwarden, KeePass)



Использование временных e-mail и номеров:

- Сервисы типа TempMail, ProtonMail для одноразовой регистрации
- Виртуальные SIM-карты или номера для анонимных звонков

Основные аспекты анонимности в интернете:

- ◆ **Скрытие IP-адреса** — предотвращает идентификацию пользователя по его сетевому адресу
- ◆ **Минимизация цифрового следа** — снижение количества собираемой информации (куки, поисковые запросы, история посещений)
- ◆ **Шифрование данных** — защита информации от перехвата третьими лицами (VPN, Tor, HTTPS)
- ◆ **Использование анонимных сервисов** — почта, мессенджеры, поисковики, работающие без отслеживания
- ◆ **Отказ от личной идентификации** — работа с псевдонимами, временными номерами почтовыми ящиками

Что делать прямо сейчас?

- ◆ Удалите старые, слабые пароли (и поставьте парольный менеджер)
- ◆ Включите двухфакторную аутентификацию на всех сервисах
- ◆ Проверьте, какие приложения используют камеру и микрофон
- ◆ Зайдите в Telegram и **проверьте активные сессии** (многие обнаружат вход с неизвестных устройств)
- ◆ Установите **VPN** и **безопасный браузер (Brave/Tor)**

Что будет, если вы это не сделаете?

- ◆ **Оформление кредитов, снятие денег с банковских счетов, подделка SIM-карты (SIM-свопинг)**
- ◆ **Продажа данных на черном рынке**
- ◆ **Обман ваших знакомых через соц.сети**
- ◆ **Создание подставных аккаунтов в соц.сетях**
- ◆ **Уголовные дела о мошенничестве**

Как нейросети помогают злоумышленникам

Фишинг и социальная инженерия

- ◆ **Генерация убедительных писем** — нейросети могут создавать безупречно оформленные фишинговые письма, адаптированные под стиль компании
- ◆ **Автоматический анализ жертвы** — ИИ может собирать информацию из соцсетей, подстраивая сообщения под жертву (spear phishing)
- ◆ **Голосовые фейки** — с помощью **нейросетей для синтеза речи** можно подделывать голос реального человека (например, руководителя компании) и звонить сотрудникам для проведения мошеннических транзакций (вишинг)

Как нейросети помогают злоумышленникам

Подделка документов и мошенничество с личными данными

- ◆ **Генерация поддельных паспортов и удостоверений** — некоторые нейросети позволяют создавать фотореалистичные изображения людей, которых не существует, что затрудняет обнаружение подделки
- ◆ **Подмена лиц в видеозвонках** — deepfake-технологии помогают мошенникам выдавать себя за реальных людей во время видеозвонков в банках и госорганах
- ◆ **Создание фальшивых аккаунтов** — нейросети автоматически создают и ведут тысячи ботов в соцсетях, делая их похожими на настоящих людей

Как нейросети помогают злоумышленникам

Взлом паролей и атаки на банковские системы

- ◆ **ИИ-ускорение перебора паролей** — алгоритмы могут анализировать стиль создания паролей и предсказывать вероятные комбинации, обходя простые защиты
- ◆ **Автоматизация атак на банковские системы** — ИИ-боты могут вести себя как реальные пользователи, проходя стандартные системы защиты (например, распознавание аномального поведения)
- ◆ **Распознавание капчи** — нейросети могут быстро разгадывать капчи, обходя защиту сайтов

Что мы не успели разобрать

1. **«Отказ в обслуживании» (DDoS-атака)** — имитация непрерывного потока пользователей.
Сайт “ложится”
2. **Внедрение SQL-кода** (Structured Query Language — структурированный язык запросов)
— код обрабатывает такие запросы, которые ведут к структурированным базам данных
3. **Уязвимость нулевого дня (0-day)** — уязвимость, которую еще не обнаружили разработчики
4. **Туннелирование DNS** — кибератака с применением протокола DNS для передачи постороннего трафика HTTP и других протоколов через порт 53. Таким образом воруются личные данные
5. **Кибератака через посредника (MITM - man in the middle)** — злоумышленники перехватывают данные и переписку между двумя людьми или устройствами.
Это делают при помощи публичной Wi-Fi-сети или вредоносного ПО

Рекомендации по защите активов бизнеса и гос.учреждений

Реализация комплексных решений по кибербезопасности

Спам-фильтры, протоколы проверки подлинности, процедуры верификации

Регулярное обновление механизмов безопасности

Использование современных технологий для предотвращения атак

Обучение сотрудников

Повышение уровня знаний сотрудников о цифровой безопасности

Формирование культуры внимательного отношения к цифровым угрозам

Проведение регулярных тренингов по кибербезопасности

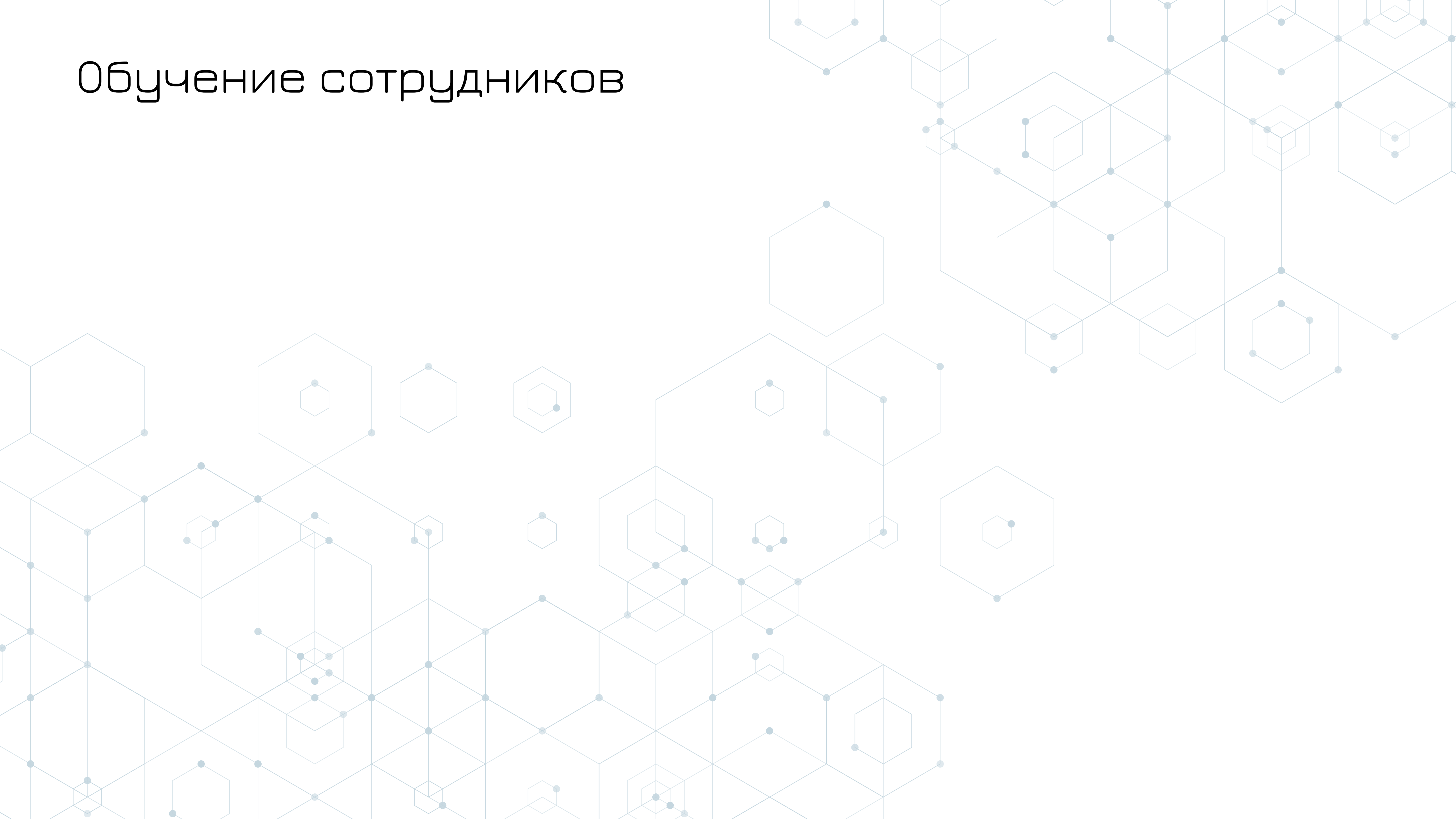
Внедрение классических инструментов

Использование надежных паролей и их регулярное обновление

Применение многофакторной аутентификации

Четкие регламенты работы с конфиденциальными данными

Обучение сотрудников

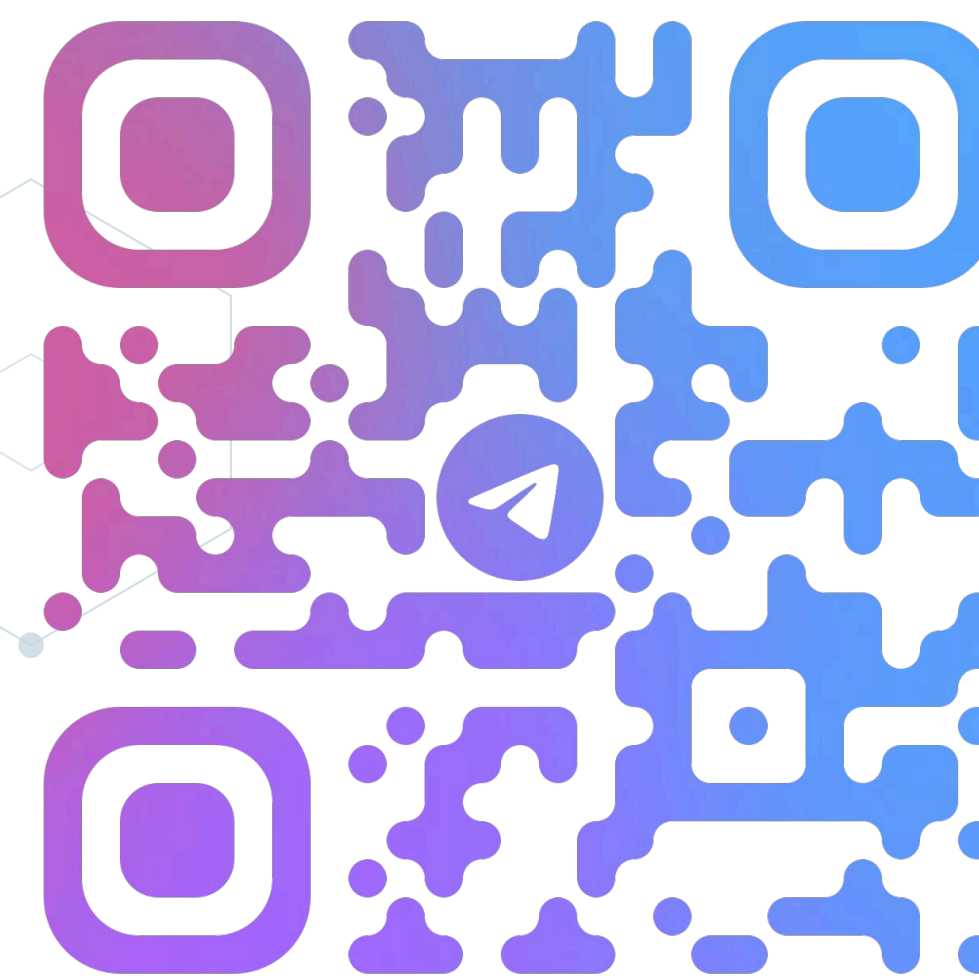


Ярошевич Егор Сергеевич



- ◆ Генеральный директор ООО "НАДА"
- ◆ Директор компании NeuroXpert
- ◆ Эксперт аналитического центра минобрнауки

<https://neuroxpert.pro>



@EGOR_NIKONOV