



Полномочный представитель Президента России
в Центральном федеральном округе

ДИАЛОГ

Центр
Управления
Регионом
Калужская область

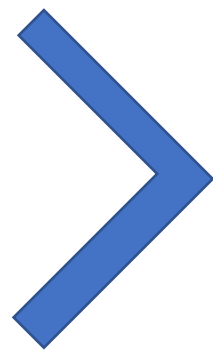


ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЦИФРОВАЯ ГИГИЕНА:

Как не стать жертвой мошенников
в 2025 году?

МАСШТАБ ПРОБЛЕМЫ

**>295 млрд
рублей**



₽

Годовой бюджет
Калужской области

Украл мошенники у россиян в 2024 году
по данным «Сбербанка»

КТО СТАНОВИТСЯ ЖЕРТВАМИ

**Сотрудники
судов**

[Источник](#)

Студенты

[Источник](#)

Домохозяйки

[Источник](#)

Пенсионеры

[Источник](#)

Дети

[Источник](#)

Госслужащие

[Источник](#)

Раньше

Уязвимые категории
граждан: в основном,
пожилые люди

Сейчас

Большинство
социальных слоев

ПОЧЕМУ ЖЕРТВ МОШЕННИКОВ СТАЛО БОЛЬШЕ?

Ежедневные действия в интернете

Регистрируемся в социальных сетях

Делаем покупки на маркетплейсах

Смотрим видео, слушаем музыку

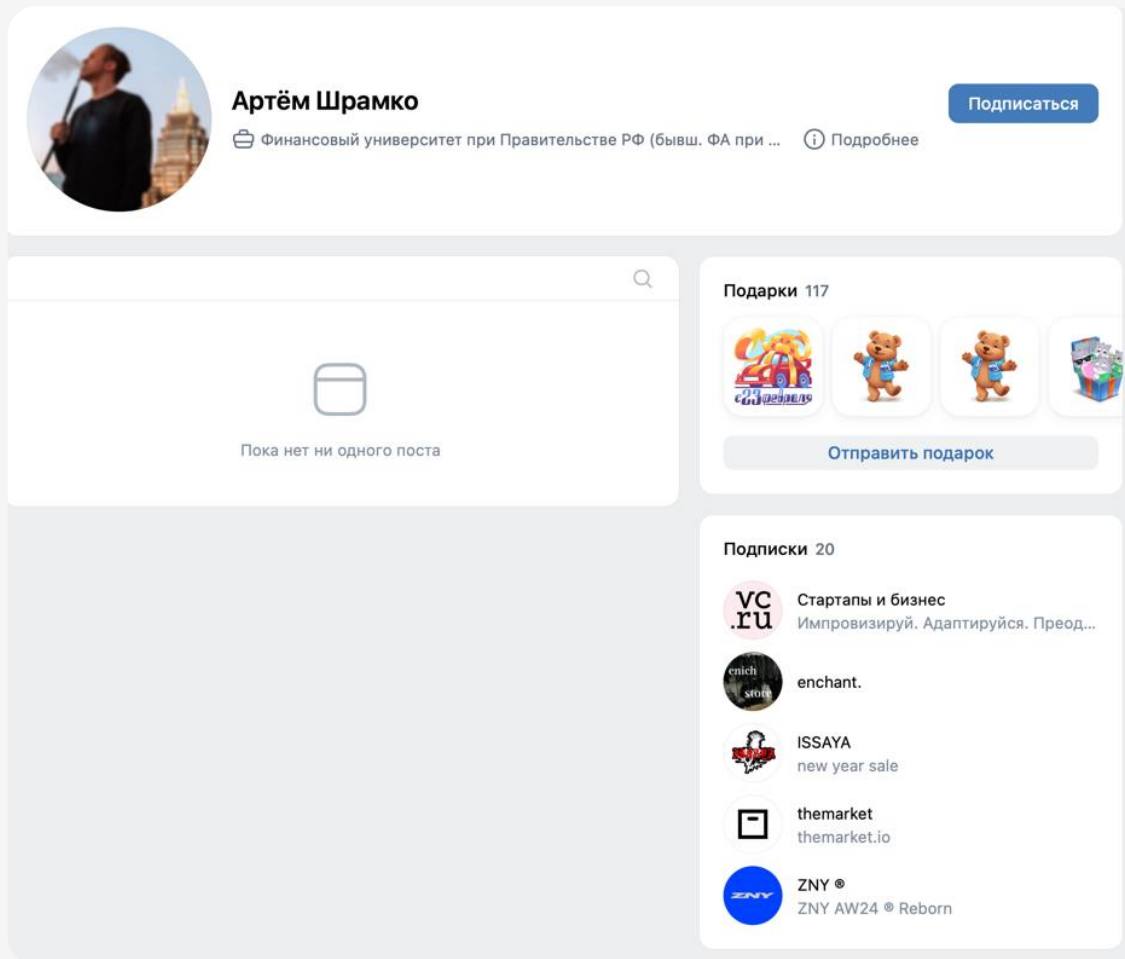
Пользуемся поисковиками

**«Цифровой след»
из персональных данных**



Желание его обезопасить

ПРИМЕР ЦИФРОВОГО СЛЕДА: СОЦСЕТИ



Страница открытая:

- › ФИ + дата рождения
- › Интересы

Страница закрытая:

- › Местоположение
- › Устройство
- › Просмотренный контент
- › Контакты

Социальная сеть + Партнеры = цифровая «витрина данных»

ПОЧЕМУ ЭТИ ДАННЫЕ ВАЖНЫ
И КАК ОНИ ПРИМЕНЯЮТСЯ

ЛЕГАЛЬНОЕ ИСПОЛЬЗОВАНИЕ

- › Целевая реклама
- › «Умная» лента в соцсети
- › Социологические исследования
- › Поведенческая аналитика со стороны госструктур
- › Предотвращение или расследование преступлений

НЕЛЕГАЛЬНОЕ ИСПОЛЬЗОВАНИЕ

- › Продажа данных на черном рынке
- › Мошенничество с помощью социального инжиниринга
- › Шантаж
- › Угрозы

— ОТ ЧЕГО МЫ ЗАЩИЩАЕМСЯ?



Информационная безопасность —

практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации

Информационная безопасность —

правильная защита «цифровых следов»

Злоумышленник может украсть вашу жизнь!

УРОВНИ ЦИФРОВЫХ УГРОЗ В СЕТИ

I уровень (низкая)

Мошенник получает общедоступные данные

Данные: ФИО, электронная почта

Виды мошенничества: телефонные звонки, фишинг, социальная инженерия

II уровень (средняя)

Мошенник получает критически важные персональные данные

Данные: дата рождения, паспорт, прописка

Виды мошенничества: сталкеринг, регистрация фиктивных компаний

III уровень (высокая)

Мошенник получает доступ к финансовым данным

Данные: банковская карта, доступ к ЛК в банках

Виды мошенничества: кража денег, оформление кредитов

IV уровень (наивысшая)

Мошенник получает полный контроль над личностью

Данные: биометрия, секретные ключи и кодовые слова, логины и пароли

Виды мошенничества: оформление документов, использование личности в преступных схемах

ОТКУДА МОШЕННИКИ ПОЛУЧАЮТ ДАННЫЕ

Социальная инженерия

Утечки

Фишинг

Взлом

УГРОЗА №1: СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Социальная инженерия – это набор методов и практик, которые заставляют человека выполнить какие-либо действия

Социальная инженерия применяется мошенниками для манипуляций с целью отъема денег, совершения жертвой преступлений и т. д.



ЖЕРТВЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ



Калуга, внимание



● Калужанка спасала дочь, а попала на мошенников

21-летний мужчина из Чеченской республики выманил у калужанки 700 тысяч рублей в мае 2024 года. Как? Схема простая:

- Сообщник преступника позвонил женщине и представился полицейским
- Он сказал, что её дочь виновата в ДТП. Чтобы девушка избежала уголовного наказания, мошенник убедил мать отдать накопления
- Преступник пришёл к женщине и забрал деньги

Злоумышленника поймали. Суд приговорил его к 5 годам лишения свободы в колонии строгого режима.

Подписаться! | Поддержать канал

t.me/klg_alarm/12619

4.2K 👁 May 31 at 10:49

ШКАЛА ОПАСНОСТИ



ЖЕРТВЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

МОШЕННИЧЕСТВО ПОЖАРЫ И ЗАДЫМЛЕНИЯ ПОЛИЦИЯ САНКТ-ПЕТЕРБУРГ

В Санкт-Петербурге задержана 37-летняя женщина, которая подожгла здание полиции на Васильевском острове, поверив телефонным мошенникам.

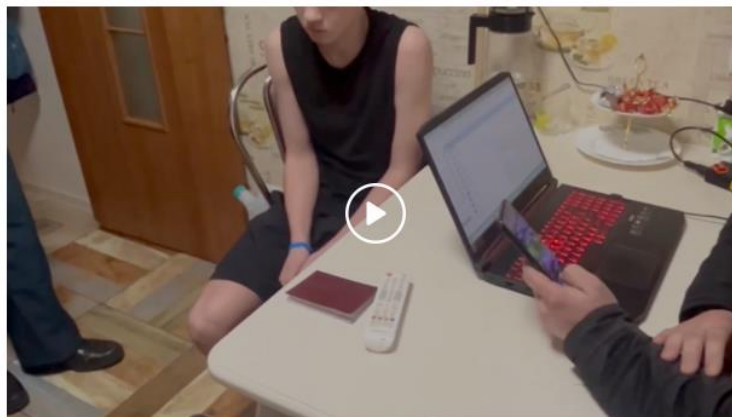
Жительница Санкт-Петербурга пошла на преступление, поверив телефонному мошеннику, который сообщил, что ее аккаунт на «Госуслугах» взломан, с помощью него оформлены кредиты, а деньги отправлены на Украину для помощи ВСУ.

ШКАЛА ОПАСНОСТИ



ЖЕРТВЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Один из задержанных за поджог по заданию мошенников признался содеянном



© ЦОС ФСБ России/ТАСС

По словам задержанного, он осознавал, что его действия могли привести к сходу с рельсов вагонов и гибели людей

МОСКВА, 30 мая. /ТАСС/. Один из молодых людей, который по заданию телефонных мошенников с Украины совершил поджог на железной дороге, признался в содеянном и сказал, что осознавал, что такие действия могут привести к жертвам

ШКАЛА ОПАСНОСТИ



ГЛАВНАЯ ОПАСНОСТЬ –

СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ (ВПЛОТЬ ДО ТЕРАКТОВ)
ЖЕРТВОЙ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

КАК РАБОТАЕТ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Глава Козельского района в своем телеграм-канале предупредила, что от её имени коллегам пишет клон — это мошенники

1 шаг: сбор информации

Мошенники изучают структуру организации: кто за что отвечает, кто подчиняется кому, кто занимается финансами.

2 шаг: подделка контакта руководителя

Создают e-mail или аккаунт в мессенджере, визуально похожий на адрес директора (например: `ivan.petrov@company.ru`).

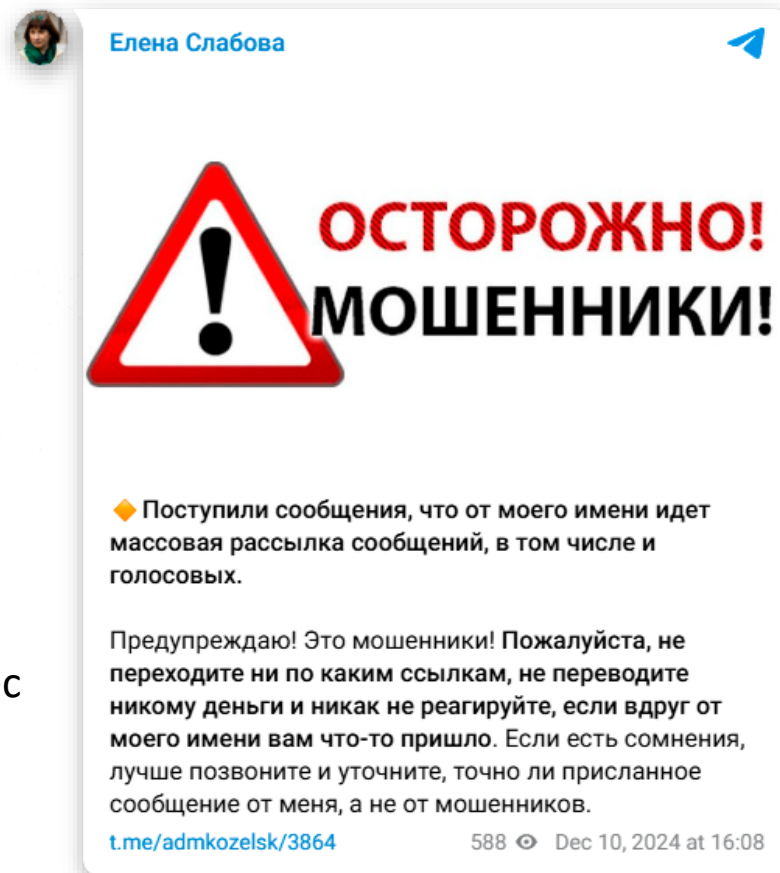
Выдают себя за начальника — через почту, WhatsApp, Telegram и т. д.

3 шаг: контакт с сотрудником и давление

Пишут бухгалтеру или менеджеру от имени "шефа", используя формулировки:

- «Это срочно»
- «Не обсуждай с коллегами»
- «Я на встрече, просто сделай»

Задача — вызвать стресс и вынудить действовать без проверок.



КАК РАБОТАЕТ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Телефонные мошенники похитили у бывшего первого замглавы аппарата Госдумы Безверхова более 44 млн рублей

1 шаг: получили номер телефона жертвы

Вероятно, номер Юрия Безверхова был найден в одной из баз данных, попавших в утечку

2 шаг: установили контакт через мессенджер

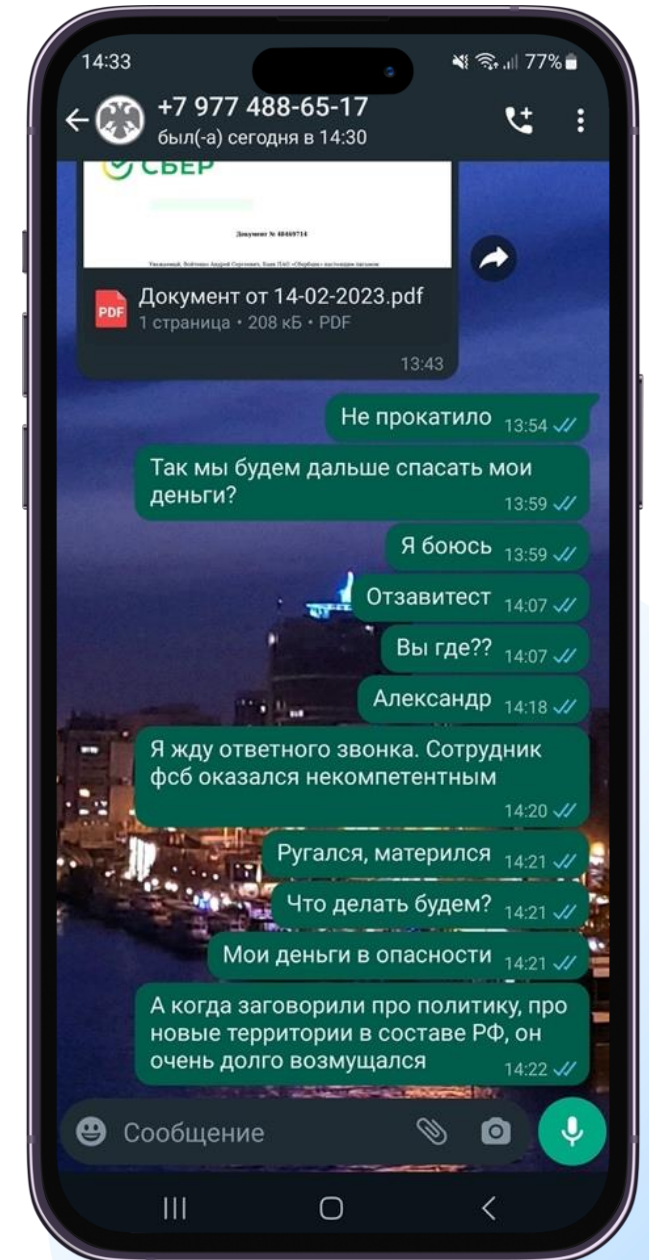
По статистике пользователи больше доверяют «неизвестным» контактам WhatsApp, чем «неизвестным» номерам телефона

3 шаг: получили личные данные и коды подтверждения

Под предлогом «возврата средств» или «проверки безопасности» выманили у жертвы чувствительную информацию: паспортные данные, логины, СМС-коды, возможно, данные карты и CVV-код.

4 шаг: перевели деньги с его счета на счета сообщников

5 шаг: исчезли, заблокировав контакт



КЕМ ПРЕДСТАВЛЯЮТСЯ МОШЕННИКИ?

БАНКИ

МВД

ФСБ

РАБОТОДАТЕЛИ

КОЛЛЕГИ

**ГОСУДАРСТВЕННЫЕ
ОРГАНЫ**

**НАЛОГОВАЯ
ИНСПЕКЦИЯ**

**СУДЕБНЫЕ
ПРИСТАВЫ**

РОДСТВЕННИКИ

**ПРЕДСТАВИТЕЛИ
«ГОСУСЛУГ»**

КЕМ ПРЕДСТАВЛЯЮТСЯ МОШЕННИКИ?

Закрытая структура, мало
публичной информации о
методах работы, сфере
полномочий

ФСБ

Репутация силового органа,
занимающегося особо важными
и опасными преступлениями

Страх перед неизвестностью



ОБЩИЕ ПРАВИЛА

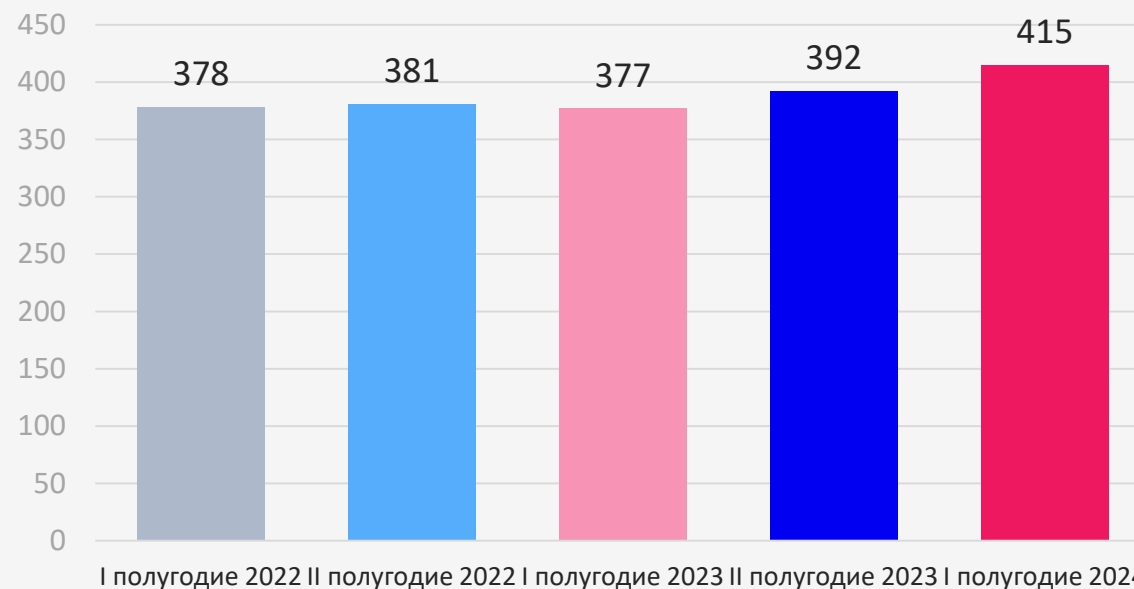
- › Установить определитель номера от оператора связи или банка
- › Никогда не выполнять требования звонящего сразу. Взять паузу, рассказать о ситуации родственникам и друзьям
- › Не переводить свои деньги на чужие счета
- › Не доверять обещаниям высокой доходности
- › НИКОМУ и НИКОГДА не сообщать свои данные:
 - коды из СМС и пуш-уведомлений
 - данные банковской карты: номер, срок действия и трехзначный код с обратной стороны
 - ПИН-код
 - кодовое слово
 - номер договора
 - контрольные вопросы
 - паспортные данные

УГРОЗА №2: УТЕЧКИ ДАННЫХ

ЧТО ВОРУЮТ?

- › ФИО
- › Телефоны
- › Адреса
- › Почта
- › Паспорт (редко)
- › Платежные данные (редко)

Утечки данных в России, тыс. случаев



КРУПНЕЙШИЕ УТЕЧКИ ДАННЫХ В РОССИИ

Организация	Утечка	Содержание
СДЭК	822 млн записей	ФИО, телефоны, адреса
Яндекс.Еда	50 млн	ФИО, телефоны, адреса
СберСпасибо	52 млн записей	ФИО, телефоны, платежные данные
Спортмастер	46 млн записей	ФИО, телефоны, почта, дата рождения

УТЕЧКИ ДАННЫХ В ГОСУДАРСТВЕННЫХ СТРУКТУРАХ РОССИИ

Организация	Утечка	Содержание
Силловые ведомства	20 тысяч записей	ФИО, телефоны, адреса
Росреестр	82 млн записей	ФИО, телефоны, адреса
Межведомственный оборот	500 тысяч записей	ФИО, телефоны, контакты
Региональные МФЦ	300 тысяч записей	ФИО, телефоны, почта, дата рождения

КАК ИСПОЛЬЗУЮТ УТЕЧКИ?

Интернет-расследования

Выслеживание человека через социальные сети и в реальном мире. Угрозы и запугивания.

Взлом цифровых ресурсов

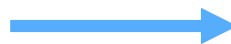
Клонирование цифровой личности.
Репутационные риски.

Финансовое мошенничество

УТЕЧКИ ДАННЫХ: ЗАЩИТА

Проблема

Взлом цифровых ресурсов
в результате утечки данных

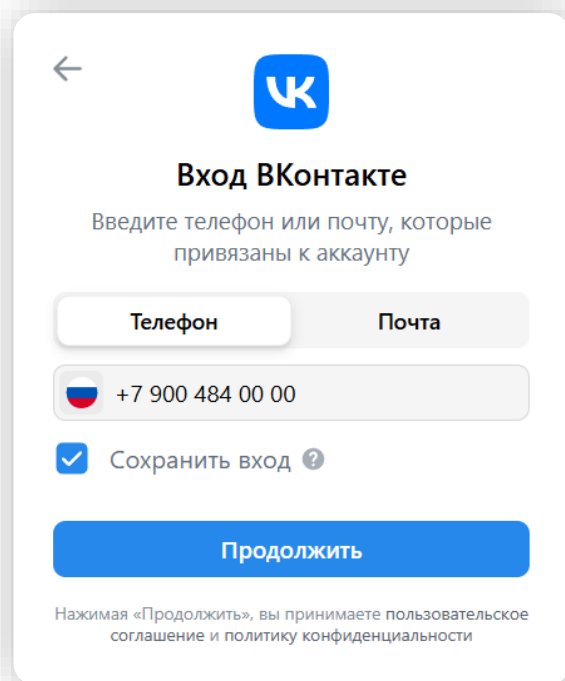


Решение

2FA аутентификация

УТЕЧКИ ДАННЫХ: ЗАЩИТА

2FA аутентификация – это подтверждение авторизации с помощью дополнительного одноразового кода или пароля



← 

Вход ВКонтакте

Введите телефон или почту, которые привязаны к аккаунту

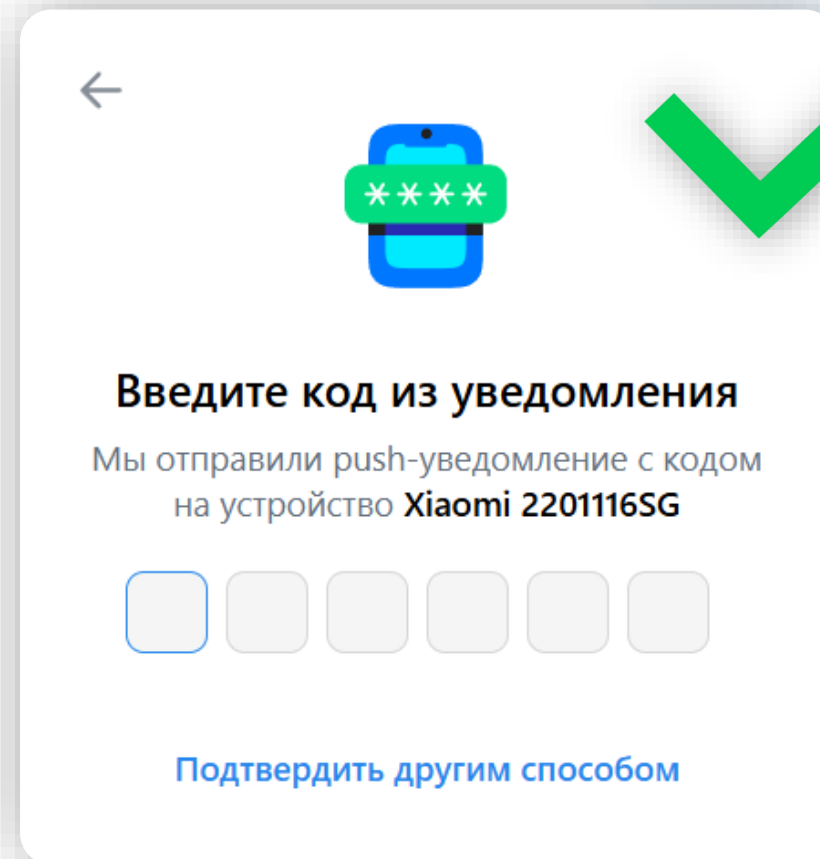
Телефон Почта

 +7 900 484 00 00

☒ Сохранить вход ?

Продолжить

Нажимая «Продолжить», вы принимаете пользовательское соглашение и политику конфиденциальности



← 

Введите код из уведомления

Мы отправили push-уведомление с кодом на устройство **Xiaomi 2201116SG**

[Подтвердить другим способом](#)

Не зависят от нас

Инсайдер, кража информации,
взлом

Зависят от нас

Отсутствие цифровой гигиены

УТЕЧКИ ДАННЫХ: ФИШИНГ

Фишинг* — это утечка данных вследствие отсутствия цифровой гигиены

Фишинг — основной вид интернет-мошенничества и основной способ для злоумышленников проникнуть в конфиденциальные системы

Используется для кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации

*от англ. fishing – рыбалка



АТАКИ ПО КОЛИЧЕСТВУ ЖЕРТВ

Массовые —

злоумышленники берут за основу несколько самых популярных интернет-сервисов, формируют легенду и рассылают тысячи писем через различные адреса

Добрый день!

Вчера мы пытались до вас дозвониться: Писали на почту и звонили на телефон.

Вы зарегистрировались у нас на сайте и получили подарок.

Новый iPhone 16 Pro практически ваш!

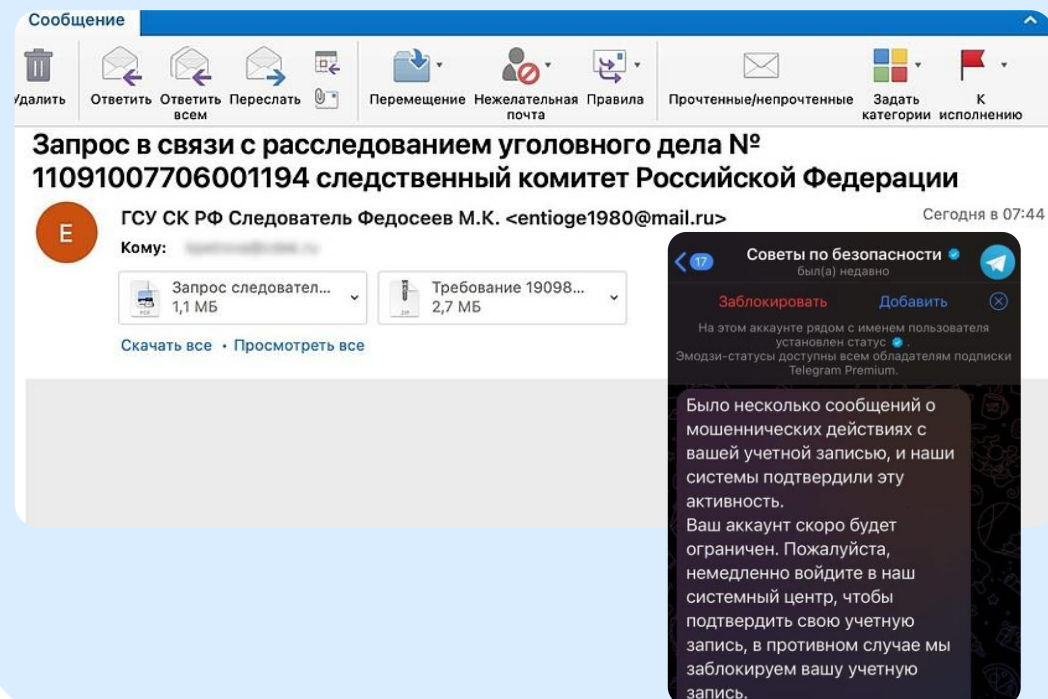
У вас остался последний день, для того чтобы воспользоваться всеми привилегиями

[Перейти на сайт и попробовать](#)

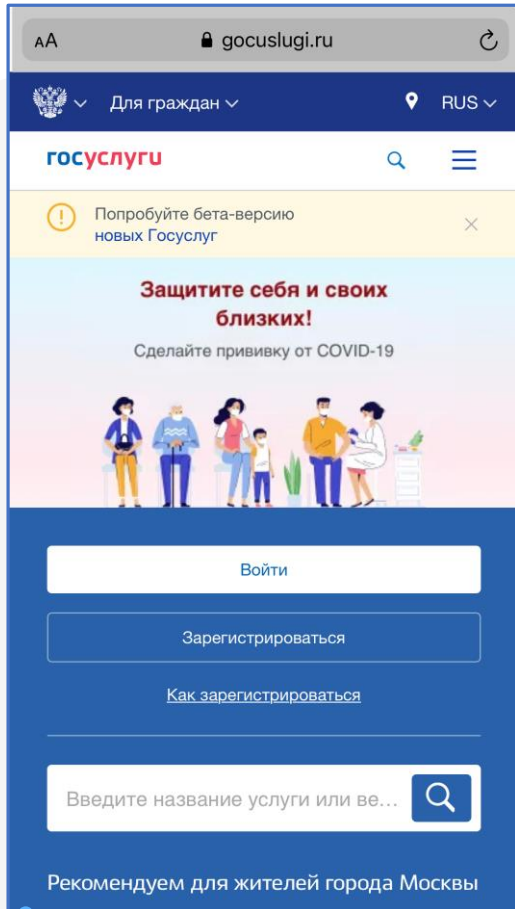
Поддержка **WILDBERRIES**

Таргетированные —

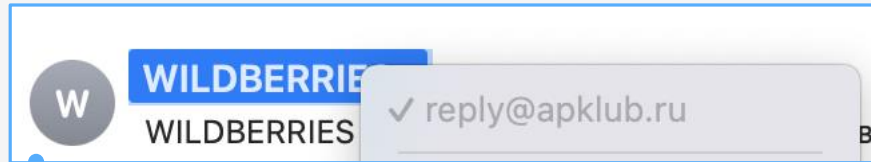
персонализированные и целенаправленные атаки. Сбор и систематизация данных на жертву



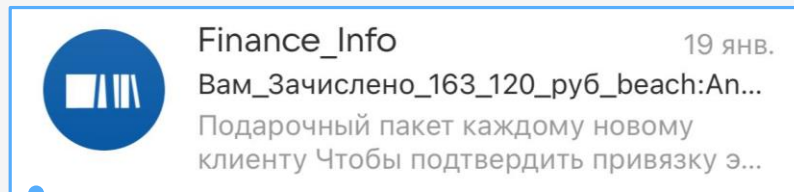
ПРИЕМЫ ЗЛОУМЫШЛЕННИКОВ



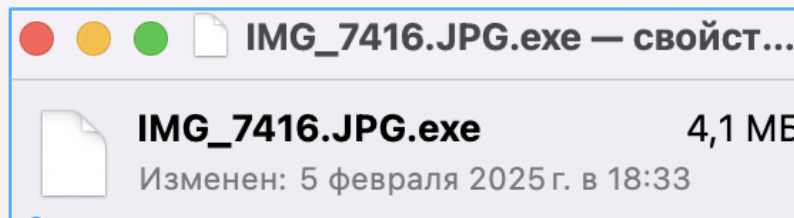
манипуляции со ссылками



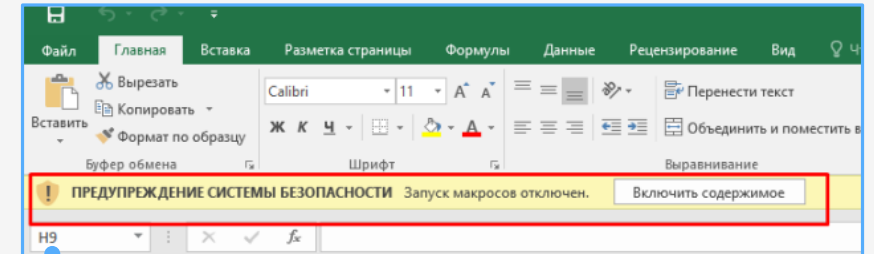
подмена отправителя (спуфинг)



брендирование



манипуляции с типом файла



запуск вредоносного ПО



использование QR-кодов

КАК РАБОТАЕТ ФИШИНГ

На электронную почту поступает сообщение якобы от Федеральной службы судебных приставов (ФССП) с «предсудебным уведомлением».

1 шаг: отправка письма с поддельного адреса

Жертве на электронную почту приходит письмо якобы от ФССП (или другого госоргана), но с обычного адреса на mail.ru, а с неофициального домена.

2 шаг: приложение PDF-документа с «электронной подписью»

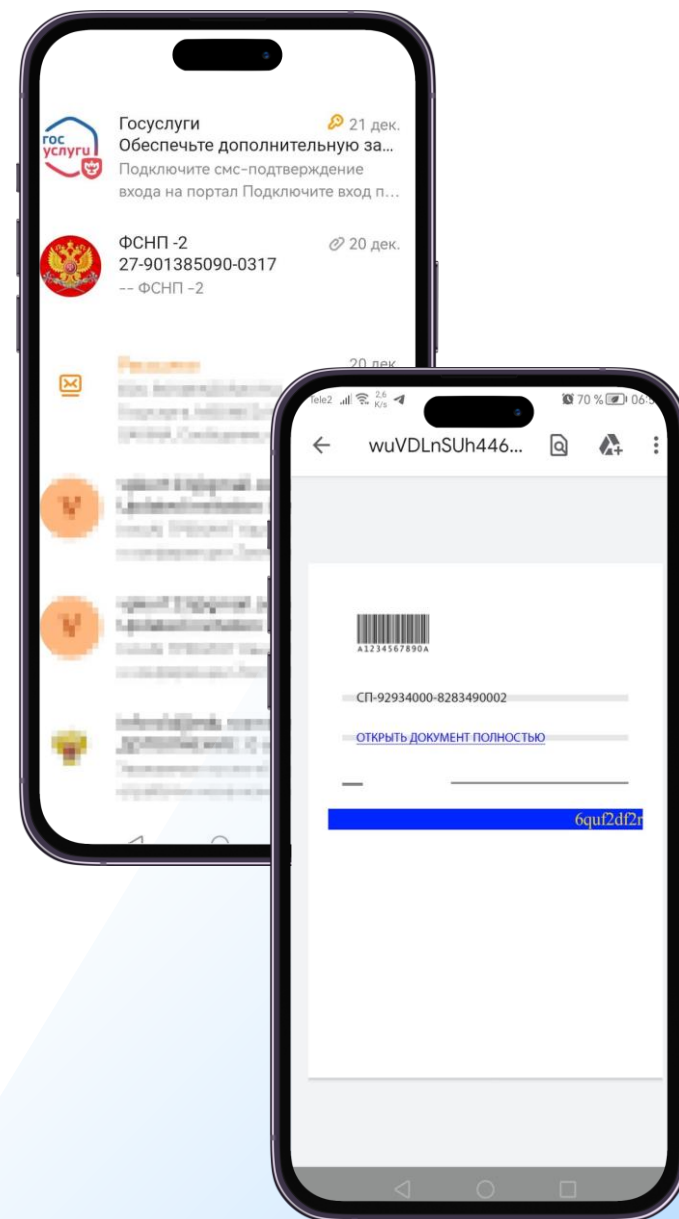
Во вложении — формально оформленный PDF-файл, якобы подписанный ЭЦП. Это придает письму видимость официальности.

3 шаг: создание чувства срочности и давления

Пользователю сообщают о «долге» в 300 рублей и пугают последствиями: блокировка банковских карт, запрет на выезд и т. п.

4 шаг: ввод данных и подтверждение оплаты

5 шаг: настоящее списание — уже на другую сумму и другому получателю



ПОПУЛЯРНЫЕ УЛОВКИ МОШЕННИКОВ

Ваша учетная запись была или будет заблокирована/отключена

В вашей учетной записи были обнаружены подозрительные или мошеннические действия. Требуется обновления настроек безопасности

Вы получили важное сообщение. Перейдите в личный кабинет, чтобы ознакомиться

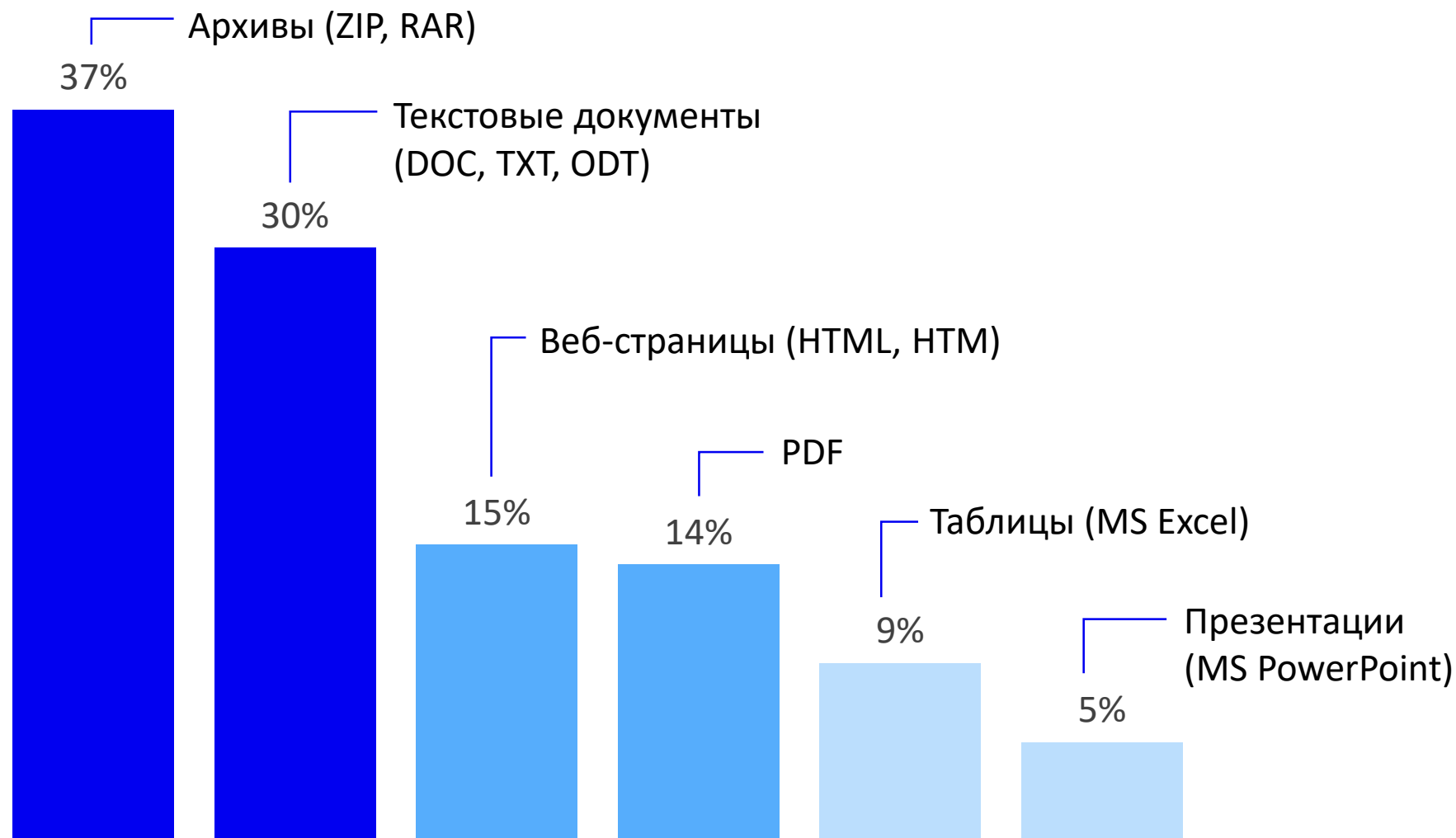
Вам пишет МВД и прочие государственные органы в момент, когда истекает срок у ваших документов



КАК РАСПОЗНАТЬ ФИШИНГ

- Критическое мышление и здравый смысл
- Анализ получаемой информации от приложения, средства защиты информации (антивируса) или операционной системы
- Анализ предлагаемой гиперссылки
- Структура URL
- Анализ почтовых заголовков

НА КАКИЕ ВЛОЖЕНИЯ ОБРАТИТЬ ВНИМАНИЕ



КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА?

90%

психология

10%

методы

ПСИХОЛОГИЧЕСКИЕ ВЕКТОРЫ АТАК

Страх

Ваш компьютер заражен и заблокирован. Кликните здесь.

Невнимательность

www.sberbank.ru
www.gmall.com

Раздражение

Чтобы отписаться, перейдите по ссылке.

Любопытство

Смотри как ты отжигашь на видео!

Жадность

Скидка 50% при оплате прямо сейчас!

Желание помочь

Ваш коллега потерял свои вещи. Дайте его номер.

93% атак

Усилители реакции

Срочность

Отчет прислать сегодня до 15:00

Авторитет

Письмо от руководства с угрозой увольнения или наоборот премией.

— Не поддаваться на эмоциональным триггерам – **ЖАДНОСТИ, СТРАХУ, СРОЧНОСТИ, АВТОРИТЕТУ, ГНЕВУ**

Вопросы для самопроверки

Ожидаю ли я это сообщение?

Есть ли смысл в том, что от меня требуют?

Знаю ли я автора?

Если я это сделаю, какие могут быть последствия?

Похоже ли это поведение на автора письма?

УГРОЗА №3: ДИПФЕЙК

Дипфейк* – это подмена изображения или голоса с помощью программного обеспечения, чаще всего – нейросети

1



2

*от англ. deepfake – глубокий, проработанный фейк (обман)

УГРОЗА №3: ДИПФЕЙК

Актер Том Круз



Сгенерированный

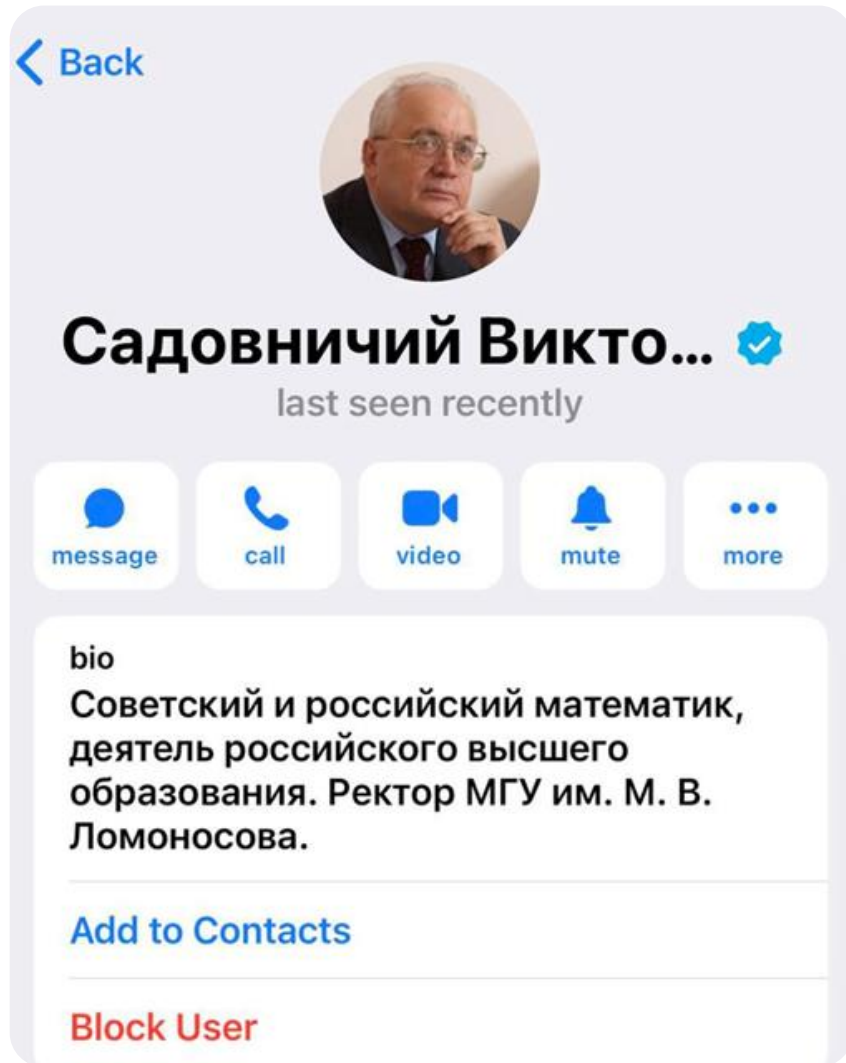
Настоящий

УГРОЗА №3: ДИПФЕЙК

Дипфейки чаще всего используются для мошенничества методом социальной инженерии. Также могут применяться для фишинга

В начале 2024 года мошенники с помощью **дипфейков** заставили финансиста гонконгского филиала транснациональной компании перевести им с корпоративного счета **более 25 млн долларов**

ДИПФЕЙКИ В СОЦИАЛЬНЫХ СЕТЯХ



- › Дипфейки в голосовых сообщениях
- › Дипфейки в «кружочках»
- › Цифровой двойник (полная копия профиля)

Не существует единого и абсолютно надежного технического или методологического способа обнаружения дипфейков

— ДИПФЕЙКИ: ЗАЩИТА

1. Комплексный анализ ситуации

Этот человек ранее общался со мной?

Уместен ли наш диалог в текущий момент?

Является ли просьба или указание странным?

2. Анализ изображения

Есть ли искажения изображения?

Не кажется ли изображение неестественно гладким?

Не «плывет» ли изображение при движении, поворотах головы?

Есть ли в речи неправильные ударения?

Есть ли в речи металлический звон, «эффект робота»?

3. Проверка по альтернативным каналам связи

Звонок по телефону (не в мессенджере)

Просьба друзей, родственников или коллег подтвердить факт коммуникации

ИИ И ЕГО ИСПОЛЬЗОВАНИЕ

Генеративный искусственный интеллект —

это тип ИИ, который может создавать новый контент и идеи, включая диалоги, истории, изображения, видео и музыку. Как и любой ИИ, он основан на моделях машинного обучения, предварительно обученных на огромных объемах данных



БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ ИИ

Использовать для
повседневных задач –

ДА

Использовать для решения
конфиденциальных
запросов –

НЕТ

ChatGPT

УТЕЧКА ДАННЫХ

В марте 2023 года разработчик ChatGPT компания OpenAI обнаружила проблему и в течение нескольких часов чат-бот не работал.

В это время некоторым пользователям неожиданно оказалась **доступна история чужой переписки**.

Сообщалось также, что в открытый доступ могла попасть **платежная информация подписчиков** улучшенной платной версии приложения ChatGPT-Plus.

Message ChatGPT



Search



Сколько случаев остановки чат-бота было с тех пор?

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

ПО и устройства:

01

Устанавливать
только официальное
ПО, своевременно
обновлять

02

Использовать
антивирусы

03

Работать из
непривилегированных
учеток, не «взламывать»
устройства

04

Устанавливать
пароли на вход
в устройство

05

Подключить удаленное
уничтожение
информации при
пропаже устройства

06

Не оставлять
устройства
без присмотра,
блокировать экран

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

Социальные сети и мессенджеры:

01

Парольная политика

02

Изучить вкладку
«безопасность»
во всех сервисах,
подключить 2FA

03

Не выкладывать
документы в открытый
доступ

04

Не выкладывать то, что
может (и будет!)
использовано
против вас (в том числе
семейные аккаунты)

05

Постараться
максимально почистить
историю о себе

06

Помнить про фишинг
через любые каналы
доставки

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

Деанонимизация:

01

Чистить метаданные в документах при необходимости их пересылки или размещения в открытые источники информации (убирать автора у документа word, геолокацию с фотографий)

02

Не использовать онлайн-редакторы документов и файлов

03

не использовать облачные хранилища

04

не использовать персональные данные при регистрации (если это строго не требуется сервисом)

05

не использовать общедоступные VPN

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

Чат-боты и ИИ:

01

Не вводите
конфиденциальные
данные

02

Читайте политику
конфиденциальности

03

Используйте
корпоративные версии
(по возможности)

04

Минимизируйте
интеграции с базами
данных на ПК

05

Проверяйте
сгенерированные
ответы

06

Внедрите политику
использования и
внутренний регламент
по работе с ИИ

ПОЛЕЗНЫЕ РЕСУРСЫ И ССЫЛКИ

Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

Реестры лицензионного ПО, банки данных угроз

fstec.ru

Национальный координационный центр по компьютерным инцидентам (НКЦКИ)

Проверка утечки данных по логину, почте или телефону, базы уязвимостей, информационные материалы

safe-surf.ru

Центр правовой помощи гражданам в цифровой среде Главного радиочастотного центра

Бесплатная правовая помощь жертвам дистанционного мошенничества

4people.grfc.ru

СЕКЦИЯ ВОПРОСОВ/ОТВЕТОВ