Кейсы социального инжиниринга Практики и инструменты защиты

Евгений Киров
Cloud Networks

AGENDA

Коротко о докладе

- О современных угрозах бизнесу
- Что такое метод социальной инженерии
- Новейшие инструменты
- Как повысить защищенность бизнеса?

О современных угрозах бизнесу

С защитой все хорошо?

89%

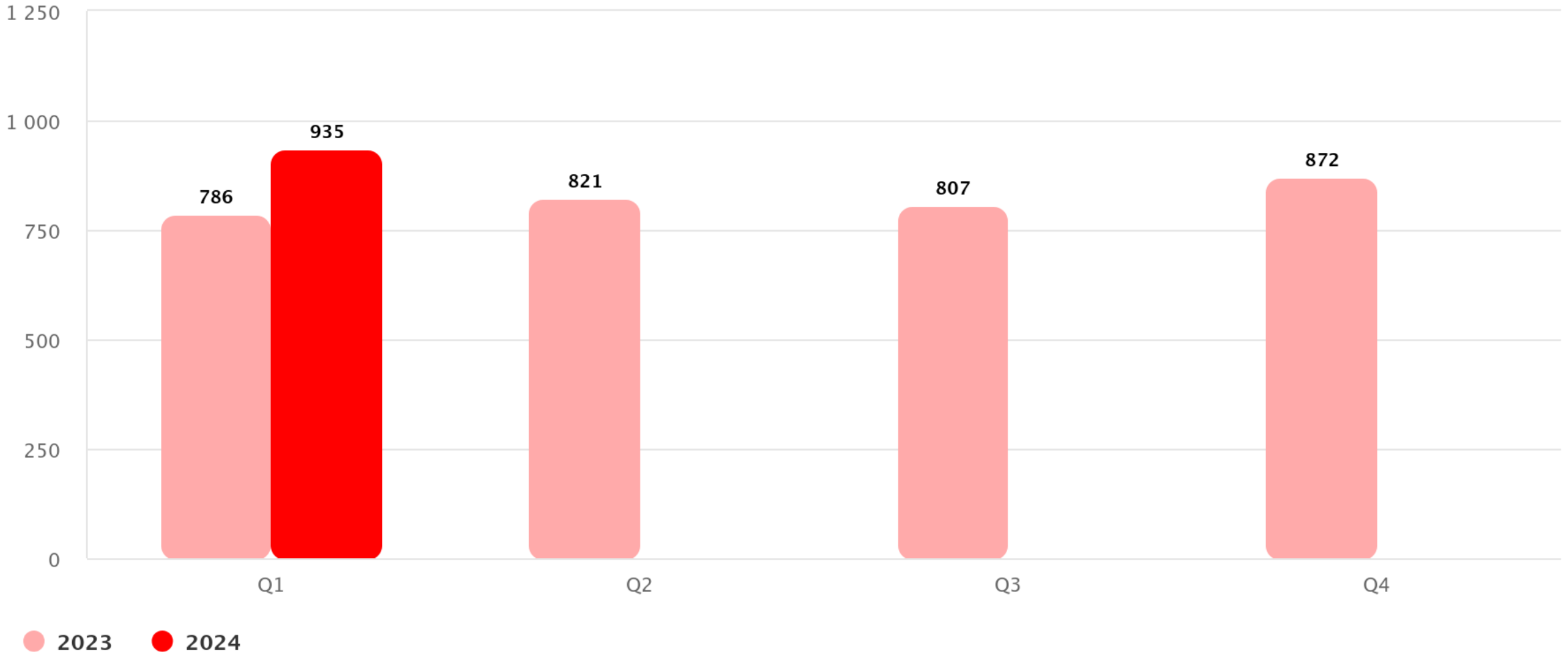
Антивирус

80%

Защита почты

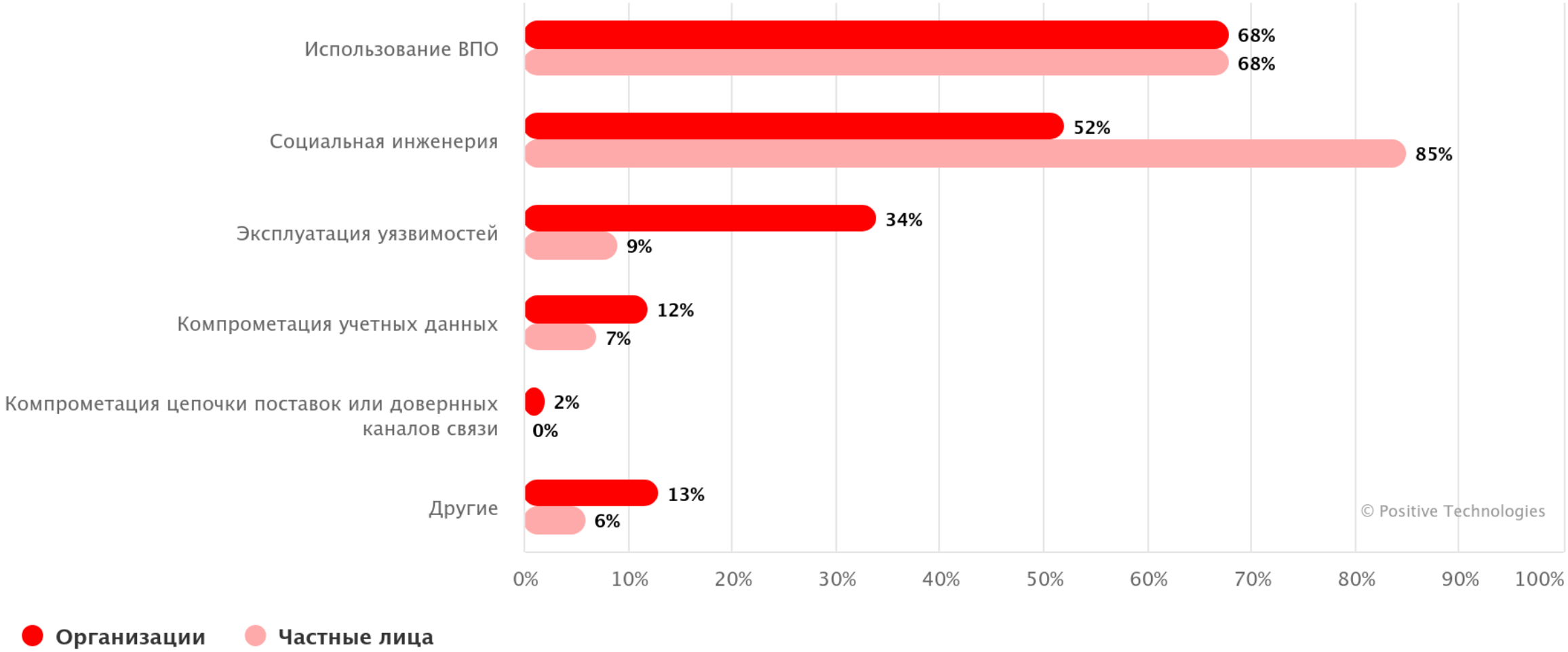
Статистика о защищенности компаний 2024 по решениям (Chat GPT)

Объемы увеличиваются



О современных угрозах бизнесу

Сегодня поговорим

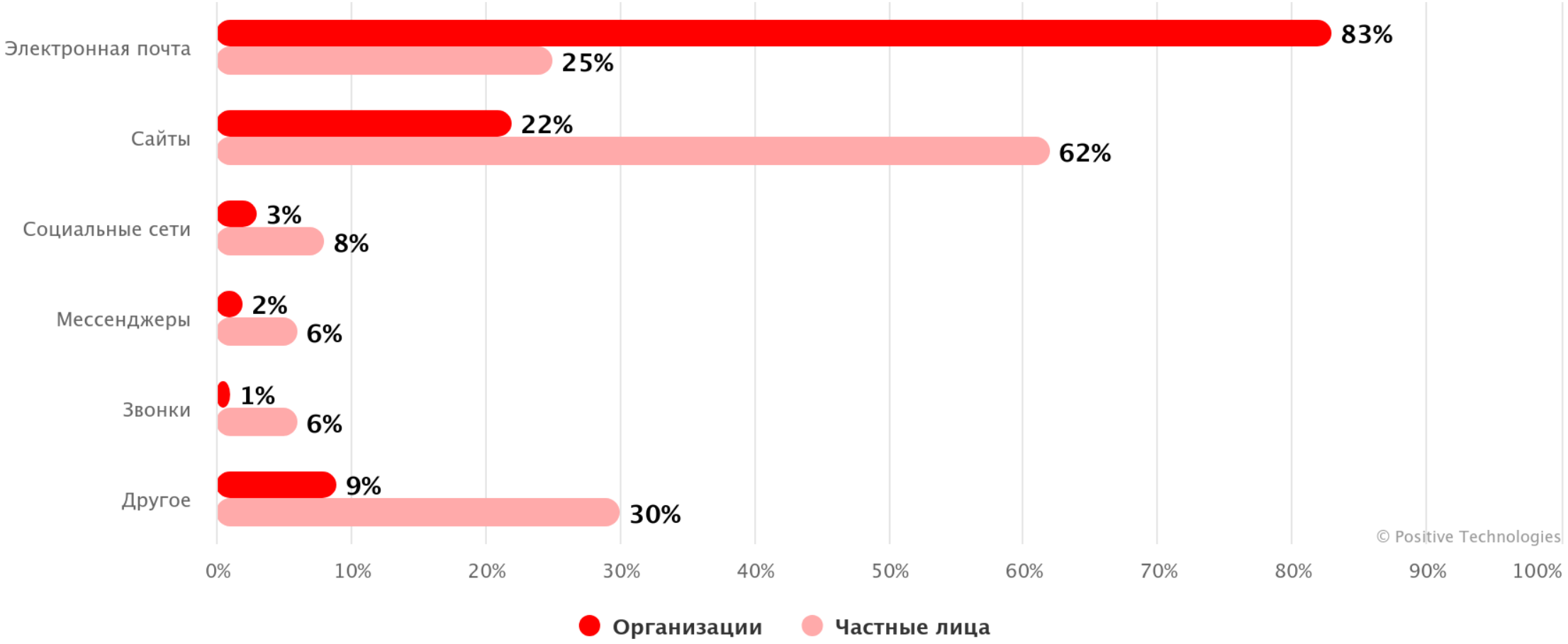


Трендовая угроза

52%

Positive Technologies 2023

Современные угрозы социальной инженерии.



Методы социальной инженерии.

Основные методы

- Фишинг
- Вишинг
- Смишинг
- Обратная социальная инженерия

Методы социальной инженерии.

Более редкие методы

- Бейтинг
- Спуфинг
- Shoulder surfing (серфинг из-за плеча)
- Tailgating, или Piggyback (катание на спине)

Почему она работает?

Исследование, проведенное MIT в 2020 году, показало, что атаки социальной инженерии эффективны, потому что они используют наши естественные когнитивные слабости.

Что такое метод социальной инженерии

Почему она работает?

СТРАХ

Ваш компьютер заражен и заблокирован, Кликните здесь.

НЕВНИМАТЕЛЬ-НОСТЬ

sbernbank.ru
gosyslugi.ru

РАЗДРАЖЕНИЕ

Что бы отписаться «Пройдите по ссылке»

ЛЮБОПЫТСТВО

Смотри как ты отжигаешь на видео

ЖАДНОСТЬ

Скидка при оплате сейчас 50%

ЖЕЛАНИЕ ПОМОЧЬ

Спаси чью-то жизнь

СРОЧНОСТЬ

Отчет прислать сегодня до 15:00

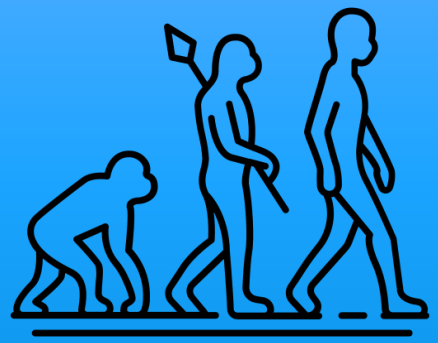
АВТОРИТЕТ

Письмо от руководства с угрозой увольнения или премией

Экспертиза

Новейшие инструменты социальной инженерии

Фишинг



ФИШИНГ

Дипфейк

deepfake от *deep learning* «глубинное обучение» + *fake* «подделка»)
методика синтеза изображения или голоса, основанная на искусственном интеллекте.

Новейшие инструменты

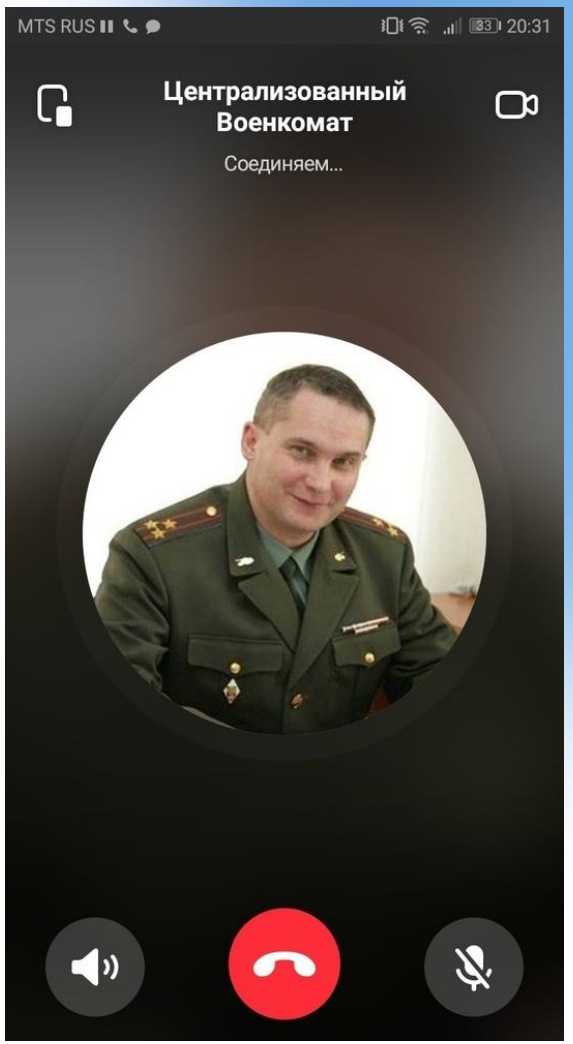
Дипфейк сегодня

Фишинг

Видео дипфейк

Вишинг

Аудио дипфейк



Экспертиза

Кейсы из мировой практики

Arup **25 000 000$**

British Co **220 000 €**

В криптовалютной афере 2022 года дипфейк Илона Маска обещал инвесторам 30 процентов ежедневных дивидендов на всю жизнь.

Воскресший «Сальвадор Дали» приветствовал посетителей музея Флориды. «Дали» мог даже сделать групповые селфи.

В 2019 году в социальных сетях распространилось видео спикера Палаты представителей Нэнси Пелоси. Видео набрало более 2,5 миллионов просмотров на Facebook.

Российские кейсы

Атака через Microsoft Teams на IT-компанию

Убедили сотрудников ввести коды многофакторной аутентификации (MFA)

Атака на энергетическую компанию

Использовали поддельные уведомления от имени служб безопасности и IT-департаментов.

Компрометация через поддельные звонки/почта/SMS.

"fake boss scam» Выдавали себя за руководителей компаний. Крали конфиденциальные данные + переводы

Как защитить компанию?

Как защитить компанию

Люди

Повышение осведомленности пользователей

- Security Awaraness
- Фишинг компании

Повышение культуры безопасности

- Важное только с доверенными лицами
- Мотивация сотрудников – сообщат об инцидентах

Психологическая готовность сотрудников

- Подготовка к давлению и срочности
- Критическое мышление

План реагирования на случай киберинцидента

- Список контактов
- Определить каждый шаг

Как защитить компанию

Инструменты

- Антифишинговые фильтры и почтовые шлюзы
- Мониторинг и контроль привилегий (PAM)
- Многофакторная аутентификация (MFA)
- Анализ поведения пользователей (UBA/UEBA)
- Системы предотвращения вторжений
- Защита от вишинга и смишинга

Как защитить компанию

Инструменты

Контроль доступа на основе ролей и прав (RBAC)

Обнаружение и блокировка вредоносного контента

Шифрование данных

Anti APT
Sandbox

Мониторинг трафика и журналов событий

EDR/XDR

Человек – самое слабое звено

Инновации

Технологии

Отношения

Контакты

Евгений Киров

Руководитель группы пресейл
Cloud Networks

моб. +7 (960) 741 – 58 –
kev@cloudnetworks.ru