Ай-ТИ Фреш

АНАЛИТИЧЕСКИЙ РАЗБОР

Фишинг против сотрудников: почта, мессенджеры, реагирование

Аналитический разбор: как один клик останавливает бизнес и что делать в первый час

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сотрудники получают десятки писем и сообщений в день, а злоумышленники маскируются под банк, поддержку мессенджера или самого руководителя. Один клик — и у атакующего пароль от почты, доступ к банк-клиенту или шифровальщик в сети компании. Обучение не даёт гарантий: под давлением «срочно» кликают даже опытные управленцы. Плана на первый час после клика у большинства нет.

Почему это важно бизнесу

- Поддельный «руководитель» с дипфейком убеждает сотрудника сделать перевод — средний ущерб атаки с дипфейком, по данным МВД, 16 млн рублей
- Один клик останавливает бизнес на дни: СДЭК и «ВинЛаб» — простои от трёх дней, убытки оцениваются до миллиарда рублей
- С 30 мая 2025 за утечку персональных данных — штрафы до 15–20 млн рублей, за повторную — оборотные до 500 млн
- Половина успешных атак на организации строится на социальной инженерии — одни почтовые фильтры не спасают

СТАТИСТИКА

Проблема в цифрах

50%

успешных атак на организации в I полугодии 2025 использовали социальную инженерию

Источник: Positive Technologies, 2025

40%

сотрудников переходят по ссылке из тренировочного фишингового письма, 10% вводят данные

Источник: МегаФон и «Лаборатория Касперского», 2025

16 млн ₽

средний ущерб от одной мошеннической атаки с использованием дипфейка, включая «фейк-босс»

Источник: Ведомости (данные МВД), 2026

26%

атак социнженерии в мессенджерах — имперсонация руководителя, схема «фейк-босс»

Источник: Infosecurity (ГК Softline), III квартал 2025

×6

реже открывают опасные письма сотрудники компаний с регулярным обучением по ИБ

Источник: МегаФон и «Лаборатория Касперского», 2025

до 500 млн

оборотный штраф за повторную утечку персональных данных (1–3% годовой выручки)

Источник: Закон № 420-ФЗ, действует с 30.05.2025

КЕЙС 1 ИЗ 3

СДЭК: шифровальщик остановил доставку по всей стране на три дня

Ситуация

СДЭК — федеральный логистический оператор, тысячи пунктов выдачи по всей России

Как развивались события

1. В ночь на 26 мая 2024 в сеть проник шифровальщик; ответственность взяла группировка Head Mare, известная фишинговыми рассылками с вредоносными вложениями
2. Вредонос зашифровал базы данных и ключевые системы — сайт, приложение, приём и выдача посылок остановились по всей стране
3. Три дня полного простоя; выдача заказов частично возобновилась 29 мая
4. Полное восстановление всех сервисов — только к 6 июня, почти через две недели

ПОСЛЕДСТВИЯ

В пунктах выдачи и на складах застряло, по оценкам, от 1,5 до 3 млн посылок. Ущерб от трёхдневного простоя эксперты оценили минимум в 300–400 млн рублей, а с учётом упущенной выгоды и репутационных потерь — до миллиарда.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Проникнув в сеть, шифровальщик дошёл до критичных систем всей компании: сегментация и резервные копии не обеспечили быстрого восстановления — на него ушло почти две недели.

Источник: Ведомости, РБК, Meduza, май–июнь 2024

КЕЙС 2 ИЗ 3

«ВинЛаб»: 2000 магазинов закрыты, убытки более миллиарда

Ситуация

«ВинЛаб» (Novabev Group) — алкогольная розничная сеть, более 2000 магазинов

Как развивались события

1. 14 июля 2025 — скоординированная атака шифровальщика на ИТ-инфраструктуру Novabev Group; злоумышленники потребовали выкуп
2. Все магазины сети, сайт и мобильное приложение остановились разом — кассы, учёт и логистика завязаны на общую инфраструктуру
3. Компания отказалась платить выкуп; первые ~100 магазинов из 2000+ открылись лишь через неделю
4. Интернет-магазин, приложение и программа лояльности вернулись только к середине августа — более чем через месяц

ПОСЛЕДСТВИЯ

Дневная выручка сети — 200–300 млн рублей; по оценке Forbes, убытки от простоя превысили 1 млрд рублей. Онлайн-продажи и бонусные баллы клиентов были недоступны более месяца.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Единая несегментированная ИТ-инфраструктура превратила взлом в остановку всего бизнеса; отработанного плана быстрого восстановления не оказалось.

Источник: Forbes, РБК, Ведомости, июль–август 2025

КЕЙС 3 ИЗ 3

«Обновите мессенджер»: вредонос на телефоне сотрудника

Ситуация

торговая компания, ~30 сотрудников (обезличенный сценарий)

Как развивались события

1. Вечером менеджеру приходит письмо «обновите мессенджер, иначе аккаунт заблокируют» со ссылкой на установочный файл
2. Приложение ставится в обход официального магазина; вредонос получает доступ к SMS, контактам и экрану
3. В течение часа — входы в корпоративную почту с незнакомых адресов и попытка перевода через банк-клиент
4. Перевод останавливает антифрод банка; устройство изолируют, сессии отзывают, домены атаки блокируют

ПОСЛЕДСТВИЯ

Попытку вывода денег остановил банковский антифрод; утекли контакты и переписка. Расследование, зачистка устройства и внеплановая профилактика заняли несколько рабочих дней.

ГЛАВНАЯ ОШИБКА / ВЫВОД

Личный смартфон с корпоративной почтой и банк-клиентом без MDM и запрета сторонних установок — открытая дверь; спасли двухфакторная защита, антифрод банка и быстрая изоляция устройства.

Источник: типовой сценарий из практики отрасли

КАК ДЕЛАТЬ НЕ НАДО

Типовые ошибки

✕ Ставка только на обучение

Фишинг давит на эмоции: в тренировочных рассылках по ссылке переходят 40% сотрудников. Без технических барьеров обучение не спасает.

✕ MFA нет или второй фактор — SMS

Без MFA украденный пароль означает полный доступ. SMS-коды перехватываются вредоносами на смартфоне — нужен код из приложения или аппаратный ключ.

✕ Личные смартфоны без MDM

Телефон с корпоративной почтой и банк-клиентом ставит приложения из любой ссылки — компания не контролирует свой главный канал доступа.

✕ Паника вместо изоляции

Перезагрузка и сброс к заводским уничтожают следы атаки — не узнать, что утекло. Правильно: режим полёта и звонок в ИТ с другого устройства.

✕ Пароль сменили, сессии не отозвали

Активные сессии и токены переживают смену пароля — атакующий сохраняет доступ к почте и рассылает фишинг контрагентам от имени компании.

✕ Нет плана первого часа

Пока выясняют, кто за что отвечает, вредонос получает команды с сервера управления и рассылает письма по контактам от имени компании.

✕ Домен без SPF/DKIM/DMARC

Письма «от директора» с поддельным отправителем доходят до сотрудников и контрагентов — подделку вашего домена никто не блокирует.

✕ Сотрудник боится признаться

Штрафы за клики приводят к замалчиванию. Час тишины превращает локальный инцидент в шифрование всей сети.

РЕКОМЕНДАЦИИ И ПРАКТИКИ

Как правильно

МИНИМУМ

- MFA через приложение (не SMS) на почте, банке и мессенджерах у всех
- Регламент первого часа: режим полёта, отзыв сессий, звонок в ИТ
- Установка приложений — только из официальных магазинов, не из ссылок
- SPF, DKIM и DMARC с политикой reject на домене компании

НОРМАЛЬНО

- Фишинг-симуляции раз в квартал с разбором для кликнувших
- MDM на всех устройствах с доступом к корпоративной почте
- Почтовый фильтр и блокировка фишинговых доменов на шлюзе
- Письменный план реагирования: роли, контакты, сохранение улик

ХОРОШО

- Ежемесячные симуляции; доля кликов — метрика безопасности
- Аппаратные ключи для админов, бухгалтерии и руководства
- Мониторинг признаков компрометации, автоблокировка адресов атакующих
- Договор на расследование инцидентов с реакцией 24/7

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Знает ли каждый сотрудник, куда звонить в первые 15 минут после клика по подозрительной ссылке?
- [ ] Включена ли MFA через приложение (не SMS) на почте и банк-клиенте у всех сотрудников?
- [ ] Запрещена ли установка приложений из ссылок на телефонах с доступом к корпоративной почте?
- [ ] Перепроверяет ли бухгалтер «срочные поручения руководителя» из чата звонком по известному номеру?
- [ ] Проводили ли вы тестовую фишинговую рассылку и знаете ли свой процент кликнувших?
- [ ] Настроен ли DMARC с политикой reject на домене компании?
- [ ] Сможет ли ваш ИТ отозвать все сессии взломанного аккаунта за 15 минут — ночью и в выходные тоже?
- [ ] Есть ли письменный план реагирования на инцидент — или только устные договорённости?
- [ ] Поблагодарят ли сотрудника за быстрое признание в клике — или накажут, подтолкнув к замалчиванию?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит защиты почты и мессенджеров: SPF/DKIM/DMARC, MFA, права доступа — отчёт с планом устранения
- Внедрение MDM, MFA-приложений и почтовой фильтрации под компанию до 50 рабочих мест
- Регулярные фишинг-симуляции с персональным разбором для кликнувших сотрудников
- Реагирование на инцидент: изоляция, анализ того, что утекло, блокировка инфраструктуры атаки
- Абонентское сопровождение: мониторинг, обновление чёрных списков, дежурный инженер

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

НА ЧЁМ ОСНОВАН РАЗБОР

Источники

01 «Актуальные киберугрозы: I–II кварталы 2025 года», Positive Technologies (ptsecurity.com — 2025)

02 Анализ тренировочных фишинг-рассылок, МегаФон и «Касперский» (cnews.ru — 2025)

03 Infosecurity (ГК Softline): социнженерия в мессенджерах, III кв. 2025 (softline.ru — 2025)

04 «МВД России тестирует ИИ для выявления дипфейков», Ведомости (vedomosti.ru — 2026)

05 «Служба доставки СДЭК три дня не работала. Ущерб — до миллиарда», Meduza (meduza.io — 2024)

06 «Причиной сбоя в работе СДЭК мог стать вирус-шифровальщик», Ведомости (vedomosti.ru — 2024)

07 «Хакеры против „Винлаба“: убытки составят более 1 млрд рублей», Forbes (forbes.ru — 2025)

08 «Novabev Group сообщила о кибератаке с требованием выкупа», РБК (rbc.ru — 2025)

09 КонсультантПлюс: штрафы за нарушения с персональными данными с 30.05.2025 (consultant.ru — 2025)

Все данные пересказаны по открытым источникам; точность на дату публикации разбора.