Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Антифишинг за одно собрание: наш регламент внедрения

DMARC до p=reject, пометка внешних, кнопка отчёта, FIDO2 и контролируемая симуляция

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

К нам приходят уже после первого клика: сотрудник ввёл пароль на копии банковского портала, и дальше гонка — сбросить пароль и активные сессии, отозвать копии письма из ящиков, снять чужие правила пересылки. Задача проста: одно неверное движение человека не должно превращаться в потерю денег и данных, а обучение должно уложиться в одно собрание, а не в трёхдневный курс.

Почему это важно бизнесу

- Платёж по подменённым реквизитам уходит на чужой счёт; после исполнения поручения вернуть деньги почти невозможно.
- Один украденный почтовый пароль открывает переписку, 1С и банк-клиент — дальше злоумышленник пишет с реального адреса компании.
- Компрометация ящика бьёт по репутации домена: с него уходит рассылка партнёрам, и письма компании начинают уезжать в спам.
- Утечка персональных данных клиентов запускает регуляторные сроки уведомления и риск крупного штрафа для юрлица.
- Разбор инцидента съедает рабочий день бухгалтерии: документы не уходят, отгрузка и сдача отчётности сдвигаются.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

45 мин

Наше собрание: 10 мин разбор, 20 мин практикум, 15 мин регламент и чек-лист

наш регламент проведения

p=reject

Целевая политика DMARC: шаги none → quarantine → reject, ступень через тег t=y

наш регламент внедрения

15 / 8 / 7

Пороги Rspamd reject / add_header / greylist в actions.conf на наших mailcow

наш профиль mailcow

48 ч

Окно ZAP: ретроспективный отзыв доставленного фишинга из ящиков Exchange Online

документация Defender for Office 365

2

PhishThresholdLevel = 2 (Aggressive): high confidence трактуется как very high

документация Set-AntiPhishPolicy

3 / 24 ч

Сроки информирования НКЦКИ: значимые объекты КИИ / прочие объекты КИИ

приказ ФСБ России № 282 от 19.06.2019

РЕАЛИЗАЦИЯ 1 ИЗ 3

Технический контур почты: собираем за один рабочий день

Что настраиваем

Бухгалтерская фирма, 24 рабочих места, собственный mailcow на VPS, домен и DNS под нашим управлением

Как мы это делаем

1. Снимаем базовую линию: DMARC p=none с адресом rua, две недели собираем отчёты и выписываем все легитимные источники отправки — 1С, CRM, рассылки.
2. Закрываем SPF и DKIM по каждому источнику из отчётов, ставим p=quarantine и после двух недель чистых отчётов — p=reject; поддомены закрываем np=reject.
3. Ступень делаем тегом t=y, а не pct: в RFC 9989 тег pct удалён, t=y означает применение политики на уровень мягче заявленной.
4. В Rspamd включаем модуль phishing с фидом OpenPhish (символы PHISHED_URL, PHISHED_OPENPHISH), в actions.conf держим greylist 7, add_header 8, reject 15.
5. Помечаем внешние письма: в Exchange Online Set-ExternalInOutlook -Enabled $true (метка появляется за 24–48 ч), на mailcow — префикс темы через Rspamd.

РЕЗУЛЬТАТ

Подделка нашего домена перестаёт доходить до сотрудников: письмо «от директора» с чужого сервера отбивается по p=reject. Внешняя пометка снимает главный трюк — совпадение отображаемого имени. Пользователь видит карантин mailcow и запрашивает релиз сам, а не пишет в чат «где моё письмо».

КЛЮЧЕВОЙ НЮАНС

Двигать DMARC до p=reject, не разобрав rua-отчёты, — гарантированно уронить рассылку из 1С и CRM. Две недели наблюдения дешевле одного дня, когда документы не уходят контрагентам.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Собрание на 45 минут и кнопка «Сообщить о фишинге»

Что настраиваем

Юрфирма, 18 человек, Microsoft 365 с Defender for Office 365; отдельная короткая сессия для директора и финансиста

Как мы это делаем

1. До собрания включаем кнопку отчёта: Set-ReportSubmissionPolicy -EnableReportToMicrosoft $true -ReportPhishToCustomizedAddress $true плюс ReportPhishAddresses.
2. Тот же адрес ставим в SentTo правила Set-ReportSubmissionRule, иначе письмо уйдёт в Microsoft, но не в наш ящик безопасности.
3. 10 минут — анатомия письма: адрес конверта против отображаемого имени, заголовки Authentication-Results, домен ссылки под текстом.
4. 20 минут — практикум: письма на экране, голосование «фишинг или нет», немедленный разбор без фамилий; 15 минут — регламент и чек-лист.
5. Отдельно с руководителями: их адреса заводим в TargetedUsersToProtect при EnableTargetedUserProtection $true, ставим PhishThresholdLevel 2 и HonorDmarcPolicy $true.

РЕЗУЛЬТАТ

Кнопка превращает «мне тут странное письмо» в событие с меткой времени: сообщение попадает на страницу Submissions, инженер видит его и чистит остальные копии. В окне ZAP 48 часов доставленный экземпляр отзывается из всех ящиков, а не ждёт следующего кликнувшего.

КЛЮЧЕВОЙ НЮАНС

Обучение без кнопки отчёта наполовину бесполезно: человек уже распознал письмо, но у него нет одного очевидного действия. Кнопка плюс телефон дежурного инженера дают половину эффекта собрания.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Контролируемая симуляция: только с письменного согласия

Что настраиваем

Торговая компания, 22 сотрудника; стенд Gophish 0.12.1 (последний релиз проекта, 2022) на отдельном VPS с учебным доменом

Как мы это делаем

1. Сначала бумага: письменное согласие руководства, зафиксированный объём, окно проведения и запрет на публичный разбор персональных результатов.
2. Поднимаем Gophish на изолированном VPS: админка слушает только наш адрес, сохранение введённых паролей выключено — фиксируем сам факт ввода, а не данные.
3. Вносим стенд в advanced delivery policy тенанта — учебный домен плюс SenderIpRanges, иначе фильтр съест письмо и исказит статистику прогона.
4. Прогон, затем собрание в течение двух суток: показываем агрегат «открыли / перешли / ввели данные», без фамилий и без выговоров.
5. Повтор раз в квартал, между прогонами — одно короткое напоминание в месяц на пять минут чтения.

РЕЗУЛЬТАТ

Мы получаем не мнение, а числа: сколько людей дошло до формы ввода. Разговор с руководителем переходит из «надо бы обучить» в конкретный план работ, а команда видит масштаб на собственном примере — и после такого вступления слушает совсем иначе.

КЛЮЧЕВОЙ НЮАНС

Симуляция без письменного согласия и без правила обезличенных результатов рушит доверие: следующий реальный инцидент от вас просто скроют. Мы не запускаем прогон, пока согласие не подписано.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- **DMARC сразу в p=reject**
  Политика ужесточается без разбора rua-отчётов — и рассылки из 1С, CRM и сервисных систем начинают отбиваться у получателей в тот же день.

- **Ступень через тег pct**
  В RFC 9989 тег pct удалён и обработчиками не учитывается; смягчение политики на время внедрения задаётся тегом t=y, а не долей писем.

- **Две пометки внешнего письма**
  Старое транспортное правило с текстом в теме плюс включённый Set-ExternalInOutlook дают дубль: пользователь привыкает и перестаёт замечать обе.

- **Кнопка есть, ящика нет**
  ReportPhishAddresses указывает на мёртвый ящик, ответа никто не даёт — и через месяц кнопкой перестают пользоваться совсем.

- **Симуляция как ловушка**
  Прогон без письменного согласия руководства и с публичным разбором фамилий даёт обратный эффект: о реальных инцидентах сообщать перестают.

- **Обучение без техконтура**
  Собрание без DMARC, MFA и карантина перекладывает всю защиту на внимание человека, а внимание предсказуемо проседает через три месяца.

- **SMS вместо второго фактора**
  Код пересказывают по телефону или вводят на поддельной странице; устойчив к этому только привязанный к домену FIDO2-ключ или passkey.

- **Живые legacy-протоколы**
  Пока открыты POP, IMAP и SMTP AUTH с базовой аутентификацией, украденный пароль обходит любые политики многофакторного входа.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- SPF и DKIM по всем источникам, DMARC p=none с rua на наш разбор
- MFA на почту, VPN и банк-клиент; закрыты POP, IMAP и SMTP AUTH
- Пометка внешних писем и собрание на 45 минут с чек-листом
- Один дежурный номер: кликнул — звонишь сразу, без разбирательств

НОРМАЛЬНО

- DMARC p=quarantine, затем p=reject после двух недель чистых отчётов
- Карантин с уведомлениями и кнопка «Сообщить о фишинге» в Outlook
- Антифишинг-политика: PhishThresholdLevel 2, HonorDmarcPolicy $true
- Модуль phishing в Rspamd с фидом OpenPhish и порогами 7 / 8 / 15

ХОРОШО

- FIDO2 и условный доступ со strength «Phishing-resistant MFA»
- Квартальные симуляции Gophish по письменному согласию руководства
- Регламент реакции: отзыв в окне ZAP 48 ч, сброс сессий и паролей
- Ежемесячная пятиминутка и метрика: сколько писем прислали по кнопке

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Проверить SPF, DKIM и DMARC домена и собрать rua-отчёты минимум за две недели до ужесточения политики
- [ ] Довести DMARC до p=reject, убедившись, что каждый легитимный источник отправки подписан DKIM
- [ ] Закрыть несуществующие поддомены тегом np=reject, а смягчение на время внедрения задавать тегом t=y
- [ ] Включить пометку внешних отправителей и убрать дублирующее транспортное правило с текстом в теме
- [ ] Развернуть кнопку «Сообщить о фишинге» и назначить ящик, который читают каждый рабочий день
- [ ] Включить MFA на всех внешних входах, директору и бухгалтеру выдать аппаратный FIDO2-ключ
- [ ] Отключить базовую аутентификацию и неиспользуемые протоколы POP, IMAP и SMTP AUTH
- [ ] Настроить карантин с уведомлениями и проверить, что пользователь умеет запросить релиз письма
- [ ] Зафиксировать регламент реакции: отзыв письма, сброс паролей и сессий, доклад руководству
- [ ] Поставить в календарь квартальную симуляцию и ежемесячное пятиминутное напоминание

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).

- Настраиваем SPF, DKIM и DMARC и доводим домен до p=reject без потери легитимных рассылок
- Разворачиваем антифишинг-контур в Microsoft 365 или mailcow: политики, карантин, кнопка отчёта
- Проводим собрание на 45 минут для всей команды и отдельную сессию для руководителей
- Готовим и проводим контролируемую симуляцию на Gophish по письменному согласию руководства
- Пишем регламент реакции и держим дежурный канал: звонок после клика разбираем в тот же час

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

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Set-AntiPhishPolicy: PhishThresholdLevel, HonorDmarcPolicy, защита адресов (learn.microsoft.com — 2026)

02 Zero-hour auto purge (ZAP): поиск в пределах последних 48 часов (learn.microsoft.com — 2026)

03 Set-ReportSubmissionPolicy и Set-ReportSubmissionRule: кнопка отчёта (learn.microsoft.com — 2026)

04 Set-ExternalInOutlook: нативная пометка внешнего отправителя (learn.microsoft.com — 2026)

05 Phishing module: PHISHED_URL, PHISHED_OPENPHISH, openphish_map (docs.rspamd.com — 3.x)

06 Rspamd tweaks: actions.conf — reject 15, add_header 8, greylist 7 (docs.mailcow.email — 2026)

07 RFC 9989 DMARC: отмена тега pct, теги t и np (заменил RFC 7489) (rfc-editor.org — 2026)

08 Приказ ФСБ России № 282: информирование НКЦКИ, сроки 3 и 24 часа (cert.gov.ru — 2019)

Основано на официальной документации продуктов и нашей практике внедрения.