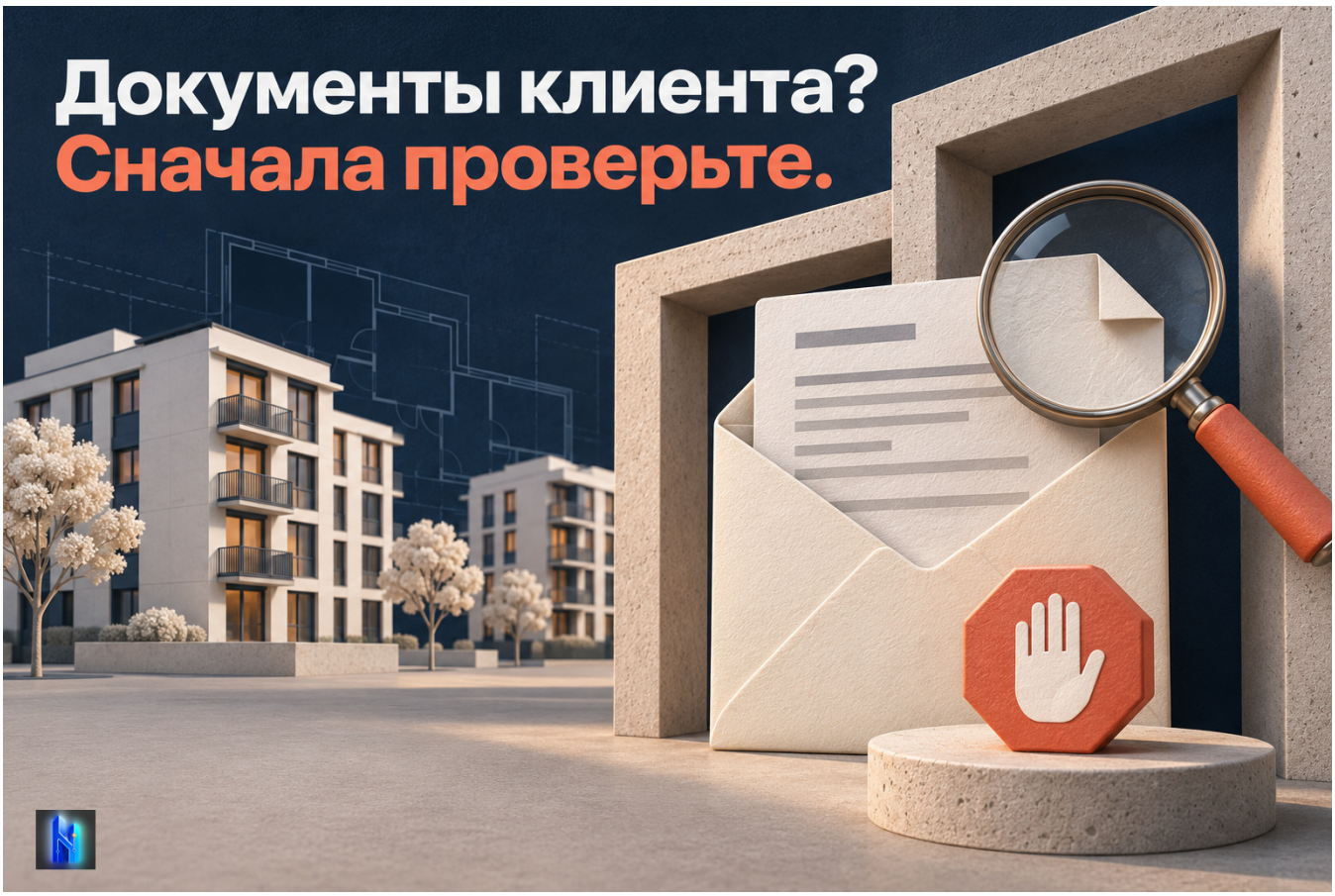
Разбор подозрительного письма

Три учебные ситуации, независимая проверка отправки и план действий после ошибочного перехода.



Практический гайд с заполненным учебным примером и чистыми рабочими листами. Подготовлено редакцией Нейросистемы риелтора.

Учебные цифры не являются данными о текущем рынке. Обложка представляет концептуальную иллюстрацию.

1. Карточка первичного разбора

Карточка помогает выбрать действие по подозрительному письму. Она не доказывает безопасность файла и не заменяет техническую проверку устройства. Не открывайте сомнительную ссылку только ради заполнения полей.

Поле	Что фиксировать
Ожидание	Какой документ и от кого ожидали
Отправитель	Видимое имя и полный адрес
Просьба	Что предлагают сделать
Необычное изменение	Новый вход, код, программа или реквизиты
Независимый контакт	Уже известный способ связи
Следующий шаг	Продолжить обычный порядок или остановиться

Учебные ситуации
А, Б и В вымышлены. Подозрительные сайты не открывались, тестовые фишинговые письма никому не отправлялись. Примеры предназначены для защитного разбора.

Письмо / время / ожидаемое действие	Наблюдение / что проверяю

2. Три вопроса до действия

Три вопроса перед действием

ОЖИДАНИЕ	ПРОИСХОЖДЕНИЕ	ПРОСЬБА
Какой документ вы ждали?	Откуда пришло это сообщение?	Что предлагают сделать сейчас?

Проверка проходит без открытия сомнительной ссылки.

Ожидание, адрес и требуемое действие проверяются вместе.

Вопрос	Что настораживает
Ждали ли такой файл?	Неожиданное предложение под видом документа
Понятно ли происхождение?	Изменённый адрес или неподтверждённый контакт
Что требуется сделать?	Пароль, код, установка программы, новые условия

Имя над письмом и отсутствие предупреждения не дают гарантии. Сохраняйте точное наблюдение: «не подтвердили изменение», «не узнаю адрес», «требуется пароль». Не объявляйте человека мошенником по одному несовпадению.

Необычный признак	Как проверю его без выполнения просьбы

3. Адрес без перехода на сайт

Учебная строка	К какому домену относится
documents.example.com	example.com
example.com.files.example.net	example.net

Строки приведены для объяснения структуры и не предназначены для входа. Знакомое слово в начале адреса не подтверждает нужный сервис. Если адрес назначения непонятен, откройте известный сервис самостоятельно и проверьте ожидаемый материал там.

HTTPS не решает всё
Защищённое соединение не подтверждает, что вы открыли нужный сайт. Предупреждение браузера не обходите ради срочного документа.

Ожидаемый сервис	Что вижу / с чем сверю официально

4. Случай А: ожидаемый план

Наблюдение	Основание
План действительно ожидался	Есть предварительная договорённость
Контакт известен	Совпадает с прежней связью
Отправка подтверждена отдельно	Клиент назвал файл и согласованный сервис
Сервис открыт самостоятельно	Переход не зависит от сомнительного письма

Следующее действие: продолжить обычную проверку материала с принятыми средствами защиты. Независимое подтверждение отправки не превращает любое вложение в гарантированно безопасное. Не отключайте защиту ради просмотра.

Какой факт подтвердил клиент?	Как получаю файл обычным способом?

5. Случай Б: пароль ради предложения

Наблюдение
Неожиданное письмо требует за пять минут ввести пароль почты и одноразовый код для просмотра «секретного предложения». Действие останавливается.

Не делать	Следующее действие
Не вводить пароль и код	Проверить аккаунт через привычный вход
Не переходить по сомнительной ссылке	Использовать официальный сервис
Не отвечать секретами	Сообщить о подозрении штатным способом почты
Не отключать защиту	При необходимости обратиться к ответственному

Не проверяйте подозрение пробным вводом настоящего пароля. Если уже передали данные, переходите к порядку разбора инцидента и фиксируйте только факт передачи, без самого секрета.

Что просили / что уже сделано	Кому сообщил / следующий шаг

6. Случай B: изменились реквизиты

Наблюдение
Письмо пришло со знакомым именем, но предлагает новые реквизиты. Независимого подтверждения изменения нет. Статус: изменение не подтверждено.

Проверка	Рабочая реакция
Есть прежний согласованный канал	Связаться по нему
Новый номер только в этом письме	Не считать его независимым доказательством
Изменение не подтверждено	Не передавать его как согласованную инструкцию
Изменение подтверждено по принятому порядку	Зафиксировать основание и продолжить процедуру

Реплика
Получил сообщение об изменении условий. Уточню по нашему обычному каналу, прежде чем передавать их дальше. Подтвердите, пожалуйста, что именно изменилось и кто согласовал изменение.

Что изменилось / независимый контакт	Подтверждение / что пока остановлено

7. Итог трёх ситуаций

Три учебных ситуации, разные действия

А

ОБЫЧНЫЙ ПОРЯДОК

План подтверждён

Б

ОСТАНОВИТЬ

Просьба пароля и кода

В

ПОДТВЕРДИТЬ

Изменение реквизитов

Это выбор следующего шага, а не статистика реальных атак.

Один путь возвращается к обычной проверке, два останавливают предлагаемое действие.

Случай	Следующий шаг
А	Продолжить обычную проверку
Б	Остановить действие, сообщить о подозрении
В	Проверить изменение независимо

Это три учебных решения, а не статистика мошенничества и не процент обнаружения атак. Ситуация В пока требует уточнения, а не публичного обвинения. Для А продолжается обычная защита при работе с файлами.

Мой случай / наблюдение	Решение / основание / кто проверит

8. Если уже взаимодействовали

Что произошло	Что записать
Открыли страницу	Время, устройство, адрес без повторного перехода
Скачали или запустили файл	Имя, действие, известные сообщения защиты
Ввели пароль или код	Какой аккаунт, время; сам секрет не записывать
Потеряли доступ	Какое официальное восстановление начато
Ушли неизвестные сообщения	Кого затронуло, что подтверждено

Остановите взаимодействие с подозрительным источником. Сообщите ответственному за рабочий аккаунт. Для Яндекс ID используйте официальный порядок проверки устройств, сессий, настроек безопасности и пароля; при потере доступа предусмотрено восстановление. Если устройство вызывает сомнения, нужна помощь специалиста и проверенное устройство.

Фактически выполненное действие	Ответственный / время / дальнейший контроль

9. Не расширяйте распространение данных

Рискованная привычка	Рабочая замена
Переслать вложение всей команде	Описать признаки и передать специалисту по установленному порядку
Загрузить клиентский файл в случайный проверщик	Использовать утверждённые средства защиты
Попросить клиента прислать код для сверки	Уточнить факт отправки без секретов
Объявить всё исправленным после одного действия	Проверить активность, настройки и последствия

Кому сообщаем о подозрении	Как передаём сведения без лишних данных

Сообщая о подозрительном письме через функции почты, учитывайте порядок передачи сообщения и вложений сервису. Не публикуйте клиентскую переписку для коллективного обсуждения.

10. Правило команды на каждый день

Правило	Как проверить применение
Известный независимый канал	Сотрудник не использовал номер только из подозрительного письма
Секреты не пересылаются	Пароли и коды отсутствуют в переписке разбора
Необычные просьбы останавливаются	Назначена конкретная проверка
Инцидент не скрывается	Ответственный знает фактические действия
Закрытие подтверждено	Есть результат проверки, а не предположение

Что внедряем в команде	Кто отвечает / когда проверим

Подготовлено редакцией Нейросистемы риелтора. Источники проверены 15.11.2026. Материал содержит защитные организационные рекомендации; реальные аккаунты и подозрительные файлы не исследовались.

Источники и проверка

Google Gmail: как распознать фишинг

Яндекс Почта: сообщить о нарушении

Яндекс ID: безопасность аккаунта

Google Chrome: защищённое соединение