



Памятка: Как не отдать свои данные мошенникам.

Внутренняя памятка для сотрудников

Контакты: [Айти Вита +7 495 988-1583]

Короткие объяснения терминов, которые встречаются в рабочих сообщениях и настройках аккаунтов.

Фишинг

Это обман по почте, в мессенджере или по телефону. Мошенник притворяется коллегой, банком, ИТ-службой или руководителем и выманивает пароль, код или деньги.

MFA

Почти то же, что 2FA, но проверок может быть больше двух. Например: пароль, код из приложения и отпечаток пальца.

Приложение-аутентификатор

Программа на телефоне, которая каждые 30 секунд создаёт новый одноразовый код. Обычно её один раз привязывают к аккаунту через QR-код.

Фишинговое письмо

Письмо мошенника, которое выглядит как обычное рабочее сообщение. Оно подталкивает перейти по ссылке, открыть файл или ввести пароль.

Фишинговый сайт

Поддельная страница, похожая на настоящий сервис. Введённые логин и пароль сразу попадают к мошеннику.

Вредоносное приложение

Программа, которая крадёт данные, пароли и деньги. Скачивайте приложения только из официальных магазинов.

Дипфейк

Подделка голоса, видео или фото с помощью нейросетей. Мошенник может позвонить голосом руководителя, коллеги или родственника.

Красный флаг

Признак, который должен насторожить: срочность, угроза, просьба о пароле, странный адрес или незнакомый номер. Увидели его — остановитесь и проверьте.

2FA

Это второй замок на аккаунте. При входе нужен не только пароль, но и второй фактор: код из приложения, SMS или аппаратный ключ.

Одноразовый код

Короткий набор цифр или букв, который действует один раз и несколько минут. Никому его не сообщайте — ни банку, ни ИТ-службе, ни руководителю.

Резервные коды

Запасные одноразовые коды на случай, если потеряете телефон. Сохраните их на бумаге в надёжном месте, не в почте и не в чатах.

Фишинговая ссылка

Ссылка на поддельную страницу вместо официального сайта. Наведите курсор и проверьте адрес, прежде чем нажимать.

Вложение

Файл, прикрепленный к письму: документ, архив, картинка или программа. Не открывайте неожиданные вложения, даже если письмо пришло от знакомого.

Удалённый доступ

Другой человек через программу видит ваш экран и управляет устройством. Банк и ИТ-служба никогда не просят включать удалённый доступ.

Социальная инженерия

Обман через эмоции: страх, срочность, любопытство или доверие к руководителю. Главное средство защиты — пауза и проверка.

ИТ-служба и ИБ

ИТ-служба — системные администраторы. ИБ — служба информационной безопасности. При сомнениях обращайтесь к ним по известному каналу.

Главное правило

Остановитесь → проверьте → только потом действуйте.

Что нельзя сообщать

Никогда и никому не сообщайте:



пароль от почты,
корпоративного аккаунта, банка



код из SMS или push-
уведомления



код 2FA и резервные коды



PIN-код, CVV, данные банковской
карты



паспортные данные и сканы
документов



корпоративные документы и
доступы

Важно: настоящая ИТ-служба, банк или руководитель никогда не просят пароль и код 2FA. Если просят — это мошенник.

Признаки фишинга в письме

Остановитесь → проверьте → только потом действуйте.

Если письмо или сообщение вызывает сомнения, лучше потратить 2 минуты на проверку, чем передать мошенникам корпоративные данные.

- Отправитель: смотрите полный адрес, а не только имя.
- Ссылка: наведите курсор и проверьте домен.
- Срочность: «Аккаунт заблокируют через 30 минут».
- Необычные просьбы: пароль, код, деньги, документы.
- Вложения: не открывайте неожиданные файлы.
- Странный стиль: ошибки и нехарактерные формулировки.

Что делать: не отвечать, не кликать, не открывать вложение. Переслать в ИТ или ИБ через кнопку «Сообщить о фишинге».

Правила общения в мессенджерах

Если пишет «руководитель», «коллега», «бухгалтер» или «IT-специалист»:



- не верьте только имени и аватарке;
- позвоните человеку по известному вам номеру;
- задайте личный вопрос, ответ на который знает только реальный коллега;
- не переходите по ссылкам из чатов;
- не сообщайте коды 2FA никому.



Красные флаги

- «Я с нового номера».
- «Не звони, я на встрече».
- «Срочно переведи деньги».
- «Назови код из SMS».

Как включить 2FA: Telegram и WhatsApp

2FA — это второй замок на аккаунте. Даже если мошенник узнает пароль, без второго фактора он не войдёт.

Telegram

1. Откройте «Настройки → Конфиденциальность → Облачный пароль» на iPhone или «Двухэтапная аутентификация».
2. Установите пароль.
3. Добавьте подсказку и резервный email.
4. Проверьте защиту резервной почты.

WhatsApp

1. Откройте «Настройки → Аккаунт → Двухэтапная проверка».
2. Нажмите «Включить».
3. Задайте шестизначный PIN.
4. Добавьте email восстановления.

Если пришёл push-запрос на подтверждение входа, а вы не входили — нажмите «Отклонить» и сообщите в ИТ или ИБ.

Как включить 2FA: MAX, Mail.ru и Яндекс

MAX

1. Откройте «Профиль → Приватность → Пароль для входа».
2. Нажмите «Установить пароль».
3. Создайте надёжный пароль из букв, цифр и символов.
4. Добавьте email восстановления.

Mail.ru

1. Откройте «Почта → Настройки → Все настройки → Безопасность».
2. Выберите «Способы входа с VK ID → Двухфакторная аутентификация».
3. Подключите SMS или приложение.
4. Создайте и сохраните резервные коды.

Яндекс

1. Откройте «Яндекс ID → Безопасность».
2. Выберите способ входа по одноразовому паролю.
3. Установите Яндекс Ключ.
4. Отсканируйте QR-код и создайте PIN-код.

Если вы уже передали данные

Немедленно сообщите в ИТ-службу или службу ИБ.

Смените пароль с чистого устройства.

Включите или обновите 2FA.

Отключите активные сессии и подозрительные устройства.

Расскажите, какие данные и на какой странице вы вводили.

Не скрывайте произошедшее — быстрое сообщение защищает и вас, и коллег.

Чек-лист перед действием

☐ Я проверил полный адрес отправителя?

☐ Ссылка ведёт на официальный домен?

☐ Просят пароль, код, деньги или документы?

☐ Есть срочность или давление?

☐ Я могу проверить это через другой канал?

☐ Я не ввожу данные на странице, которую не проверял?

☐ Меня просят установить программу удалённого доступа?

☐ Меня просят установить приложение не из официального магазина?

**Остановитесь →
проверьте → только
потом действуйте.**



Не давайте удалённый доступ к устройству

Не устанавливайте и не запускайте по просьбе незнакомцев:

- AnyDesk
- TeamViewer
- UltraViewer
- Zoho Assist
- Rudesktop
- Трансляцию экрана своего телефона

1. Прервите разговор.
2. Удалите программу, если уже установили.
3. Сообщите в ИТ или ИБ.



Не устанавливайте неизвестные приложения

Используйте только официальные магазины: Google Play, App Store и RuStore.

- Не устанавливайте APK из мессенджеров, писем и случайных сайтов.
- Проверяйте разработчика и разрешения приложения.
- Не отключайте Play Protect и встроенную защиту системы.



Новая схема обмана

Век ИИ: голос тоже подделывается

Голосовое сообщение или звонок могут быть сгенерированы ИИ и звучать убедительно.

- Перезвоните по известному номеру.
- Не поддавайтесь давлению и срочности.
- Берегите голосовые записи и не публикуйте их без необходимости.
- Задайте личный вопрос, ответ на который знает только реальный собеседник.

Не устанавливайте неизвестные приложения



Используйте только официальные магазины: Google Play, App Store и RuStore.

- Не устанавливайте APK из мессенджеров, писем и случайных сайтов.
- Проверяйте разработчика и разрешения приложения.
- Не отключайте Play Protect и встроенную защиту системы.



Примените на практике

Как не поставить вредоносное приложение

Только официальные магазины. Всегда проверяйте разработчика и разрешения.



Где можно ставить

- Google Play
- App Store
- RuStore
- AppGallery



Где нельзя ставить

Не ставьте APK из писем, чатов, рекламы и случайных сайтов.



Проверяйте разработчика

Сверьте название, логотип, сайт и отзывы с данными компании.

Проверяйте разрешения

- **Камера** — доступ должен быть только у приложений, которые реально снимают фото/видео или сканируют QR.
- **Микрофон** — нужен для звонков, диктофона, голосового поиска. Всё остальное — подозрительно.
- **Контакты** — обычно нужны мессенджерам и почте. Игры, фонарики, калькуляторы — нет.
- **Телефон / журнал вызовов** — для звонков и определителей номера.
- **SMS** — критично: доступ к SMS часто используют для перехвата кодов. Разрешать только банкам и мессенджерам, если без этого нельзя.

Не выключайте защиту

Не отключайте Play Protect и встроенную защиту iOS — они помогают заметить опасное приложение до установки или запуска

Android: Play Protect

iPhone: встроенная защита iOS

Признаки поддельного приложения

- Пришло по ссылке из письма или мессенджера
- Неизвестный или странный разработчик
- Мало отзывов или много однотипных отзывов
- Просит слишком много разрешений
- Просит отключить защиту

Если приложение уже установлено

Действуйте спокойно и по порядку — не продолжайте работу на подозрительном устройстве.



1. Отключите интернет.
2. Удалите приложение.
3. Сообщите в ИТ или ИБ.
4. Смените пароли с чистого устройства.
5. Проверьте активные сессии и уведомления.



Не продолжайте вход

Не вводите логины, пароли и коды, пока устройство не проверено.



Подключите помощь

Передайте ИТ или ИБ название приложения, время установки и скриншоты уведомлений.

Три шага, которые помогают не стать жертвой мошенников.

1

Остановитесь

Не отвечайте сразу. Пауза снижает риск ошибки.

2

Проверьте

Уточните отправителя, ссылку, просьбу и канал связи.

3

Действуйте

Используйте официальный канал и сообщите о подозрении.



Что нельзя делать

- Не сообщать пароли, коды 2FA, PIN и данные карты.
- Не переходить по подозрительным ссылкам и не открывать неожиданные вложения.
- Не переводить деньги под давлением.
- Не устанавливать программы удалённого доступа по просьбе незнакомцев.
- Не устанавливать неизвестные приложения и APK из случайных источников.



Что нужно сделать уже сегодня

- Включить 2FA на важных аккаунтах.
- Сохранить резервные коды в надёжном месте.
- Проверить активные сессии и устройства.
- Сохранить официальные контакты ИТ и ИБ.
- Сообщать о подозрительных письмах, звонках и сообщениях.

Остановитесь → проверьте → только потом действуйте

Если сомневаетесь — спросите. Это не стыдно, это правильно