

Индивидуальные рекомендации по защите финансовых данных для клиентов и сотрудников

Посоветуйте своим сотрудникам и клиентам следовать приведенным ниже рекомендациям по кибербезопасности в их личном поведении, чтобы повысить их готовность и защитить финансовые данные от киберугроз.

1. Обеспечьте внедрение основных практик в области кибергигиены на всех устройствах.

- ⇒ Используйте надежные пароли на всех личных и профессиональных устройствах и рассмотрите возможность использования диспетчера паролей.
- ⇒ Регулярно обновляйте операционные системы, другое ПО и приложения на своих компьютерах и мобильных устройствах.
- ⇒ Установите антивирусное, антивредоносное ПО и защиту от программ-вымогателей для предотвращения, обнаружения и удаления вредоносных программ.
- ⇒ Используйте брандмауэр для предотвращения несанкционированного доступа к компьютеру.
- ⇒ Используйте продукты безопасности только от надежных компаний. Ознакомьтесь с отзывами о компьютерах и потребительскими изданиями, а также рассмотрите возможность консультации с производителем вашего компьютера или операционной системы.

2. Соблюдайте осторожность при работе с конфиденциальной информацией.

- ⇒ Не отправляйте пароли от банковского счета или другие конфиденциальные данные финансового счета по незашифрованной электронной почте.
- ⇒ Соблюдайте осторожность в отношении того, где и как вы подключаетесь к Интернету для связи с банком или другого обмена конфиденциальной личной информацией. Общедоступные сети Wi-Fi и компьютеры в таких местах, как библиотеки или бизнес-центры отеля, могут представлять опасность.

3. Противодействуйте фишингу.

- ⇒ Не открывайте вложения из электронных писем сразу после получения и не переходите по ссылкам в незапрошенных или подозрительных электронных письмах. Остановитесь. Подумайте. Нажмите на кнопку.
- ⇒ С подозрением относитесь к ситуациям, когда кто-то неожиданно обращается к вам через Интернет или по телефону и запрашивает личную информацию. Даже при общении с известными адресатами сведите к минимуму обмен личной информацией по электронной почте.
- ⇒ Помните, что ни одно финансовое учреждение не будет отправлять электронные письма или звонить и запрашивать конфиденциальную информацию, которая у них уже имеется.
- ⇒ Предполагайте, что запрос на получение информации из банка, где вы никогда не открывали счет, является мошенничеством.
- ⇒ Перед предоставлением личной информации проверяйте достоверность подозрительного электронного письма или всплывающего окна. Обратите особое внимание на адрес электронной почты.

Управление учетными записями

- ⇒ Требуйте, чтобы для входа в ваши сервисы клиенты использовали надежные идентификаторы пользователей и пароли. Посоветуйте им не использовать пароль, который уже используется для других учетных записей.
- ⇒ Для проверки реальных клиентов и снижения возможности мошенничества используйте мгновенную верификацию, проверку в реальном времени, пробную проверку вклада, проверку личности и/или ответы на личные вопросы.
- ⇒ Предлагайте, а лучше — требуйте от клиентов прохождения двухфакторной аутентификации при входе в ваши сервисы.
- ⇒ Регулярно проверяйте учетные записи пользователей на наличие признаков мошенничества.

Защита данных

- ⇒ Подумайте о том, какие данные клиентов организация *должна* собирать для предоставления своих услуг, и соблюдайте осторожность при сборе дополнительных данных клиентов.
- ⇒ Разработайте и распространите политики хранения данных. Ликвидируйте данные клиентов, которые больше не будут использоваться.
- ⇒ Обеспечьте шифрование передаваемых и неиспользуемых данных клиентов.
- ⇒ Внедрите политики безопасности данных, чтобы четко обозначить разрешенные и запрещенные методы передачи данных и укажите допустимые процедуры для всех сотрудников при работе с данными клиентов. Убедитесь, что эти политики задокументированы, доведены до сведения всех сотрудников и периодически пересматриваются и обновляются.

Защита общедоступных веб-приложений

- ⇒ Обеспечьте внедрение протокола HTTPS в общедоступных веб-приложениях организации и перенаправляйте весь HTTP-трафик по протоколу HTTPS.
- ⇒ Используйте политику защиты содержимого на ваших веб-сайтах для предотвращения атак, связанных с межсайтовым скриптингом, кликджекингом и другими методами внедрения кода.
- ⇒ Активируйте закрепление публичного ключа на своих веб-сайтах для предотвращения атаки с применением технологии «злоумышленник в середине».

⇒ Убедитесь, что в общедоступных веб-приложениях не используются файлы «cookie» для хранения особо важной или критичной информации о клиентах (например, паролей), и что эти файлы имеют даты истечения срока действия (лучше раньше, чем позже). Рассмотрите возможность шифрования информации, хранящейся в используемых файлах «cookie».

⇒ Рассмотрите возможность найма службы проверки на проникновение для оценки безопасности общедоступных веб-приложений не реже одного раза в год.

Обучение сотрудников

⇒ Обучайте своих сотрудников подотчетности и стратегиям минимизации человеческих ошибок, которые могут привести к раскрытию данных клиентов. Посоветуйте им:

- свести к минимуму доступ к данным клиентов и их передачу, получая его только для выполнения своих должностных обязанностей;
- [придерживаться строгих методов обеспечения безопасности](#) на всех устройствах и учетных записях, которые работают с данными клиентов, посредством использования надежных паролей, двухфакторной аутентификации, обновления ПО, и воздерживаться от перехода по подозрительным ссылкам;
- сообщать о любых потенциальных внутренних или внешних инцидентах в сфере безопасности, угрозах или неправильном обращении с данными техническим специалистам организации и/или высшему руководству.

⇒ Убедитесь, что ваши сотрудники понимают эти требования и подписали документы, обеспечивающие соблюдение политик защиты данных и безопасности организации.

Следите, чтобы они не нарушали эти политики и не взаимодействовали с клиентами в незащищенной среде.

Уведомление клиентов

⇒ Обеспечьте понимание нормативных требований организации в отношении нарушений безопасности данных клиентов, чтобы гарантировать готовность к их соблюдению в случае подобных инцидентов.

⇒ Когда ваша организация узнает о несанкционированном доступе к конфиденциальной информации клиентов, необходимо срочно провести расследование и определить вероятность того, что информация была или будет незаконно использоваться. Используйте передовые способы уведомления и незамедлительно сообщите пострадавшим клиентам следующие данные:

- Общее описание происшествия и информацию, к которой был получен несанкционированный доступ.
- Номер телефона для получения дополнительной информации и помощи.
- Напоминание «сохранять бдительность» в течение следующих 12–24 месяцев.
- Рекомендация о необходимости незамедлительного информирования о подозрениях в краже персональных данных.
- Общее описание мер, предпринятых финансовым учреждением для защиты информации от дальнейшего несанкционированного доступа или использования.
- Контактная информация бюро кредитных историй.
- Любая другая информация, которая требуется в соответствии с соблюдаемыми организацией нормативными требованиями.