

Новые технологии сделали нашу жизнь проще и комфортнее. Однако не стоит забывать о мерах финансово-цифровой безопасности. Какие правила нужно установить и соблюдать в семье, чтобы не допустить кражи денег мошенниками? Рассказываем в этой статье.

Современный человек несколько раз в день вводит пароли: в онлайн-банке, на портале налоговой, в приложении мобильного оператора, соцсетях. Пароль нужен ему, когда он заходит на свой аккаунт на маркетплейсе или в стриминговом сервисе. Последние часто предлагают подключить семейный аккаунт. Через него все члены семьи могут оформлять доставку, заказывать такси, смотреть кино и сериалы по одной подписке.  «Главный бухгалтер» семьи может устанавливать лимиты трат для всех домочадцев, а также контролировать расходы через приходящие SMS или push-уведомления.

Для финансовой безопасности всех членов семьи важно установить для такого аккаунта надёжный пароль. Эксперты рекомендуют придерживаться базовых правил:

* Чем сложнее, тем лучше. Не стоит использовать очевидные комбинации, типа «123456». Лучше если пароль будет состоять из маленьких и больших букв, цифр, а также дополнительных символов: «+», «$», «?» и тому подобных.
* Не используйте очевидные личные данные при генерации пароля: имя, год рождения, кличка питомца, название компании-работодателя. Мошенники могут подобрать этот ключ, используя информацию из ваших соцсетей.
* Используйте максимальную длину. Лучше использовать не менее 12 символов (там, где это возможно). Чем длиннее пароль, тем сложнее его подобрать.
* Один пароль для всех аккаунтов – это опасно. Если пароль один раз будет скомпрометирован, вы рискуете потерять доступ сразу ко всем аккаунтам.

Устанавливайте двухфакторную аутентификацию, что предполагает второй уровень защиты аккаунта – например, введение в специальное поле кода из push-уведомления

Есть специальные парольные карты – сервисы в интернете, которые помогают генерировать безопасные пароли.

Нужно не забывать периодически менять пароли. Желательно это делать каждые две недели.

**Где хранить пароли?**

Мало придумать безопасный пароль, важно еще его правильно хранить. Оповестить домочадцев о смене пароля от банковского приложения в семейном чате может быть удобно, но точно не безопасно.

Не стоит хранить пароли на холодильнике (он может случайно попасть на фото, и таким образом пароль попадет в руки мошенников), а также в заметках телефона.

Эксперт рекомендует пользоваться менеджерами паролей – инструментом, который генерирует, хранит и управляет уникальными и сложными паролями для различных онлайн-аккаунтов.

**В каждой семье должно быть кодовое слово**

По данным Банка России, мошенники в 2023 году похитили у клиентов банков 15,8 млрд рублей. Это на 11,5% больше, чем годом ранее. Главная причина в том, что атаки злоумышленников стали адресными и продуманными.

Современные технологии позволяют мошенникам не только писать от имени родственников, но и звонить – отличить голос абонента от голоса мамы, дочери, сестры, брата, сына может быть крайне сложно. Эксперты советуют в таких случаях задавать персонализированные вопросы.

Также можно придумать с домочадцами кодовое слово. При возникновении подозрений спрашиваем его у того, кто говорит на том конце трубки. Если он не может назвать кодовое слово, завершаем звонок – с большой вероятностью это мошенник.

**Особое внимание детям и пожилым**

Скорее всего, вы лучше знакомы с правилами поведения в финансово-цифровой среде, чем ваши дети или пожилые родственники. Ваша задача – обучить их. Если у школьника есть банковская карта, то нужно ему объяснить, что давать карту другим людям нельзя, как и сообщать пин-код от нее и трехзначный номер на обратной стороне. При этом карта ребенка должна быть привязана к онлайн-банку взрослого, который может устанавливать лимиты и контролировать траты.

Не меньше внимания нужно уделять бабушкам и дедушкам, которым всегда сложнее освоить цифровые устройства. Они же являются наиболее уязвимой группой для обмана. Важно рассказывать пожилым родственникам о новых схемах мошенничества, а также проговаривать правила цифровой безопасности.

Важно оставаться в доступе и вовремя отвечать на вопросы пожилых родственников. При звонке мошенников это успокоит родного человека и, возможно, позволит сохранить деньги.

**Резюме**

Правила финансово-цифровой безопасности семьи:

1. Придумывайте надежные пароли для аккаунтов и время от времени их меняйте.
2. Семейные аккаунты – это удобно, но важно защищать их конфиденциальность.
3. Храните пароли в надежном месте, дверь холодильника или семейная группа в мессенджере – неподходящие варианты.
4. Придумывайте кодовые слова либо задавайте контрольные вопросы для идентификации абонента – вашим собеседником может оказаться мошенник.
5. Терпеливо объясняйте правила цифровой гигиены детям и пожилым родственникам.