



Цифровой кошелек: как сохранить его в безопасности.

Муниципальное бюджетное образовательное
учреждение города Междуреченск
«Средняя образовательная школа №1»

Работу выполнила:
Богатырева Анастасия Сергеевна



Что такое цифровой кошелек?

Цифровой кошелёк представляет собой электронный аналог традиционного бумажника. Вместо того чтобы носить с собой физический кошелёк с картами, вы храните их цифровую версию на смартфоне.

Чтобы совершить покупку, достаточно поднести телефон к платежному терминалу. Не нужно передавать карту кассиру или вставлять ее в терминал.

Еще одно преимущество электронного кошелька, помимо быстрой и удобства платежей, – это возможность хранить данные различных карт. Больше не нужно носить с собой кучу скидочных карт и карт лояльности магазинов.



Наиболее распространенные угрозы для электронных кошельков:

Скриминг

Данный способ заключается в том, что на банкомат, точнее на щель приема карты мошенники устанавливают считывающее устройство скриммер, при помощи которого делается дубликат карты

Фишинг

При этом способе мошенники копируют мошенниками официальный сайт кредитной организации. Клиенты, войдя на сайт оставляют свои персональные данные, при помощи которых мошенники получают доступ к их счетам

Мошенничество, связанное с системой банковского обслуживания

Заключается в хищении информации по счету клиента, применении вирусной программы, перевыпуске СИМ - карт.

Разглашение информации о картах самими пользователями

Разглашение ПИН, передача данных мошенникам в следствии беспечности

Как обеспечить безопасность Вашего кошелька: несколько простых правил.

1. Не передавать карту другим людям.
2. Установить СМС-уведомления.
3. Держать карту подальше от посторонних глаз.



4. Не передавать другим такие данные по карте, как коды из СМС, CVV2-код (трёхзначный код безопасности), ПИН-код.
5. Совершать платежи только на веб-страницах, которым доверяете.
6. Использовать двухфакторную аутентификацию.
7. Тщательно проверять транзакции.

Что делать, если все же перевел деньги мошенникам?

Шаг 1. Сообщите в банк о мошенничестве. Чем быстрее вы предупредите банк, тем выше шанс остановить перевод и вернуть деньги.

Если клиент назвал мошенникам пароли и коды из СМС, сотрудники банка помогут обновить данные для входа в личный кабинет и перевыпустить все карты. Это мешает преступникам оформить на жертву кредиты или досрочно закрыть вклады.



Шаг 2. Заблокируйте номер мошенников. Сотрудники проверяют информацию и при необходимости отключают подозрительную сим-карту, а данные ее владельца передадут полиции.

Шаг 3. Подайте заявление в полицию (подайте заявление в ближайшем отделении полиции или на сайте МВД) и сообщите о проблеме в Роскомнадзор.



Будьте аккуратнее!
Следуйте правилам и не
ведитесь на
мошенников.

Всем спасибо за внимание!

