Безопасность онлайн-платежей

Онлайн-покупки стали частью повседневности, а значит - и мишенью для злоумышленников. Чтобы не оказаться среди потерпевших, важно соблюдать простые, но действенные правила цифровой финансовой гигиены.

Отдельная карта для интернета

Для покупок в сети рекомендуется использовать отдельную карту с ограниченным лимитом и балансом. Пополнять её стоит непосредственно перед оплатой, только на нужную сумму. Такой подход сводит возможные потери к минимуму, даже если данные карты будут скомпрометированы.

Проверка магазина и адреса сайта

Перед оплатой убедитесь, что покупка совершается на официальном сайте. Адрес должен содержать корректное имя компании. Любые странные буквы, символы или лишние домены - сигнал остановиться. Отзывы покупателей и упоминания в поиске помогут подтвердить, что площадка настоящая.

Только личное устройство и защищённая сеть

Оплачивайте покупки с личного смартфона или компьютера. Не используйте чужие устройства и открытые Wi-Fi-сети - они уязвимы для перехвата данных. Если приходится подключаться вне дома, лучше активировать режим «Инкогнито».

Никогда не вводить PIN-код и SMS-коды

Интернет-магазины и банки не запрашивают PIN-код. Код из SMS или push-уведомления вводится только внутри официального приложения банка. Если сайт требует эти данные - это мошенничество. Немедленно прекратите операцию и сообщите банку.

Электронные чеки и история операций

После каждой транзакции сохраняйте электронный чек - до момента получения товара. Проверяйте выписки в мобильном банке: любая незнакомая операция - повод заблокировать карту и обратиться в поддержку.

Только официальные приложения

Устанавливайте приложения магазинов и платёжных систем только из официальных площадок - Google Play, App Store, RuStore.

Не переходите по ссылкам на скачивание из мессенджеров или писем: под видом «акций» часто распространяют фишинговые копии.

SMS-уведомления и лимиты

Подключите уведомления обо всех действиях с картой, и установите лимиты на онлайн-платежи. Это позволит оперативно заметить подозрительные списания и предотвратить ущерб.

Что делать при утечке данных

Если появились подозрения, что информация о карте могла попасть в чужие руки - немедленно обратиться в банк и запросить перевыпуск карты. Чем быстрее заблокирован доступ, тем выше шанс сохранить средства.

Признаки фишинга: сообщение о «подарке» или «блокировке счёта» с ссылкой на оплату; домен с орфографическими ошибками или цифрами в названии; требование ввести данные карты целиком; страница оплаты не содержит сертификата HTTPS.

Главное правило: любое действие с картой должно проходить только на официальных сайтах и в приложениях, без спешки и под контролем владельца. Безопасность финансов в онлайне - не сложность, а привычка.

ОИОС по материалам управления по противодействию киберпреступности КМ УВД