

ФИНАНСОВАЯ ГРАМОТНОСТЬ

Безопасность финансовых транзакций в интернете: как защитить свои деньги в цифровую эпоху

Почему это важно каждому? А вы знаете, что сегодня более 70% россиян регулярно совершают онлайн-платежи: оплачивают коммунальные услуги, делают покупки в интернет-магазинах, переводят деньги родственникам. Цифровая финансовая грамотность перестала быть уделом IT-специалистов — это базовый навык современного человека. Каждый день мошенники придумывают новые схемы обмана, и только знания о безопасном поведении в сети могут стать надежной защитой.

И так, основные угрозы при онлайн-платежах:

1. Фишинг — цифровая «удочка»

Мошенники создают поддельные сайты, копирующие интерфейс банков, государственных порталов или популярных магазинов. Жертве приходит письмо или сообщение с просьбой «подтвердить данные» или «проверить безопасность».

Как распознать?

Адрес сайта отличается от оригинального (например, sberbnk.ru вместо sberbank.ru)

Сообщение содержит орфографические ошибки

Требуют срочных действий («ваш счет будет заблокирован через 10 минут»)

2. Вредоносное программное обеспечение.

Программы-трояны, которые попадают на устройство через

- нелегальное программное обеспечение;
- вложения в подозрительных письмах;
- сомнительные мобильные приложения.

А вы знаете, что такие программы могут

- перехватывать данные банковских карт;
- подменять реквизиты платежа;
- блокировать устройство с требованием выкупа.

3. Социальная инженерия

Звонок «из банка» с сообщением о попытке взлома с просьбой назвать код из SMS или данные карты. Мошенники часто представляются сотрудниками службы безопасности, используя психологическое давление.

Вы должны знать основные семь правил безопасности для каждого пользователя

1. Проверьте подключение. Используйте только HTTPS-сайты (замок в адресной строке).

Не совершайте платежи через общественный Wi-Fi в кафе, аэропортах.

При необходимости используйте VPN от проверенных провайдеров.



2. Укрепляйте пароли

Разные пароли для банковских сервисов, почты и соцсетей.

Комбинация букв (верхний/нижний регистр), цифр и спецсимволов.

Используйте менеджеры паролей (LastPass, 1Password).

Двухфакторная аутентификация — обязательно!

3. Банковские карты: цифровая гигиена

Виртуальные карты для онлайн-покупок с ограниченным лимитом.

SMS-уведомления о всех операциях.

Не храните полные данные карты в браузере или на сайтах магазинов.

Отдельная карта с небольшой суммой для повседневных онлайн-платежей.

4. Мобильная безопасность

Устанавливайте приложения только из официальных магазинов (App Store, Google Play)

Проверяйте разрешения приложений (почему простому фонарику нужен доступ к контактам?)

Регулярно обновляйте операционную систему!

5. Распознавание мошеннических схем

Никогда и никому не сообщайте:

- коды из SMS (их запрашивают только мошенники);
- CVC/CVV-код с обратной стороны карты;
- данные паспорта по телефону или в мессенджерах;
- полную информацию о карте (срок действия, номер).

6. Техническая защита

Антивирус на всех устрой-

ствах (включая смартфоны).

Файрволл (брандмауэр).

Регулярное резервное копирование важных данных.

Шифрование дисков на ноутбуках и смартфонах.

7. Проверка получателей платежей

Особенно актуально для оплаты госуслуг, штрафов, коммунальных платежей:

Используйте только официальные порталы (Госуслуги, сайты администраций).

Проверяйте реквизиты через несколько источников.

Для муниципальных платежей (как в Черемхово) используйте QR-коды с официальных сайтов.

Что делать, если вы стали жертвой мошенников?

- Немедленный алгоритм действий:

- позвоните в банк — заблокируйте карту;

- напишите заявление — в отделении или через онлайн-чат банка;

- обратитесь в полицию — заявление о мошенничестве (ст. 159 УК РФ);

- смените пароли — всех сервисов, где использовался аналогичный пароль;

- проверьте устройства на наличие вредоносного ПО.

Важно: у вас есть 24 часа с момента списания средств, чтобы оспорить операцию без доказательств мошенничества. После этого срока потребуются подтверждения.

Особенности муниципальных онлайн-платежей

При оплате услуг администрации (налоги, штрафы, сборы):

- проверяйте реквизиты на официальном сайте муниципалитета (например, admcher.ru для Черемхово);
- используйте портал Госуслуг — самый защищенный канал;
- QR-коды — безопасный способ, если они с официальных источников;
- сохраняйте квитанции — электронные чеки и подтверждения оплаты;
- будущее безопасности: биометрия и блокчейн.

Современные технологии предлагают новые решения:

- распознавание лица и отпечатки пальцев — в смартфонах и банкоматах;
- голосовая биометрия — для подтверждений в кол-центрах банков;
- блокчейн-технологии — для прозрачных муниципальных платежей;
- искусственный интеллект — анализирует поведение пользователя и блокирует подозрительные операции.

И в заключении: безопасность — это привычка!

Защита финансов в интернете

- не разовое действие, а система привычек. Это как пристегиваться в автомобиле, так же, как:

- проверять сайт перед оплатой;
- использовать сложные пароли;
- не поддаваться на психологическое давление по телефону;
- регулярно обновлять программное обеспечение.

Финансовое управление администрации города Черемхово напоминает:

- банки и государственные органы НИКОГДА не запрашивают по телефону полные данные карт, коды из SMS и пароли. Любой такой запрос — 100% мошенничество;
- будьте бдительны, продолжайте обучаться цифровой грамотности и учите этому старшее поколение — именно они часто становятся жертвами из-за недостатка технических знаний;
- берегите свои средства — в цифровом мире ваша безопасность начинается с ваших действий.

Статья подготовлена финансовым управлением администрации города Черемхово

