

Предотвращение вовлечения обучающихся в противоправную деятельность с использованием информационно-телекоммуникационной сети «Интернет»

Материал подготовлен с использованием электронного ресурса -
Официальная страница Свердловской области.

<https://vk.com/svo196>

- Новые технологии уверенно вошли в нашу повседневную жизнь: мы пользуемся банковскими картами, совершаем покупки и оплачиваем различные услуги через интернет.
- При этом важно быть бдительными и защитить себя от действий мошенников.

Общие правила для защиты банковских карт

1. Никогда и никому не сообщайте ПИН-код и код с обратной стороны карты
2. Немедленно блокируйте карту в случае ее утери
3. Храните ПИН-код отдельно от банковской карты
4. Не отдавайте карту третьим лицам (официантам, продавцам и т.п.)



Внимание! Мошенничества с банковскими картами

Скиммеры —
считывающие устройства
для копирования
магнитной полосы



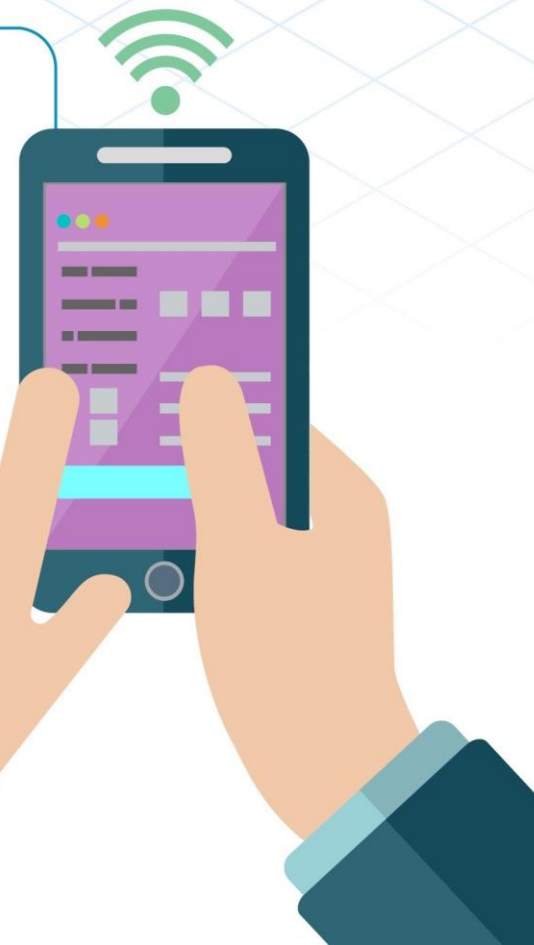
Ливанская петля —
блокиратор, чаще всего
изготовленный из обычной
фотопленки, который
препятствует возврату
карты из банкомата



Внимание! Мошенничества с банковскими картами

Просьба привязать номер
вашей банковской карты
к какому-либо номеру
телефона или счету

Покупка «липовых»
услуг (авиабилетов,
полисов ОСАГО)



Типичные методы интернет-мошенников

1. Хищение денег под видом продажи товара ненадлежащего качества, не соответствующего заявленному, с использованием интернет-площадок.
2. Продажа несуществующей в реальности продукции в лже-интернет-магазинах

При осуществлении входа на сайт уже известных вам банков и организаций внимательно изучите открывшуюся страницу — она может быть двойником





Основные виды мошеннических схем



Финансовые пирамиды



Кибермошенничество



Мошенничество с использованием
банковских карт



Мошенничество при онлайн-покупках



Фейковые просьбы от родственников



• Как уберечь себя от мошенников?

СМИ пестрят заголовками о многомиллионных долгах жертв мошенничества, героями таких сюжетов становятся не только пенсионеры, но и молодёжь. Злоумышленники придумывают новые схемы обмана доверчивых граждан.

Рассказываем в деталях об уловках преступников и делимся правилами безопасности, которые уберегут вас и ваши финансы. Читайте и делитесь информацией с близкими.



Новые схемы мошенничества



Поступает звонок или СМС с предложением поддержать благотворительный фонд или проведение СВО и перечислить средства через СМС на короткий номер

! Не реагируйте на данные сообщения, помогайте только проверенным организациям



После заказа лекарства поступает звонок по телефону и якобы представитель Минздрава/ налоговый инспектор/ полицейский сообщает, что препарат оказался подделкой и покупателю положена компенсация, для её получения необходимо заплатить налог

! Прервите разговор с мошенником





Новые схемы мошенничества



Поступает сообщение в мессенджере якобы от руководителя, который предупреждает сотрудника о телефонном звонке от ФСБ/ МВД/ министерства с целью предотвращения совершения мошеннических действий

! Проверяйте сомнительные сообщения у реального руководителя





Новые схемы мошенничества



Поступает звонок о продлении обслуживания/перерегистрации сим-карты, для чего необходимо сообщить СМС-код в виде пароля от Госуслуг

! Не сообщайте никому данные СМС, прервите разговор



Поступает предложение подключить новые функции в мессенджерах через покупку «голосов» или «бустов». Злоумышленники просят выслать деньги обычным переводом

! Не переводите деньги мошенниками или чат-ботам





Правила безопасности при пользовании банковскими картами



никому не сообщайте пин-код, CVC- или CVV- коды банковской карты и одноразовые пароли



в торговых точках, ресторанах все действия с банковской картой должны происходить в присутствии держателя карты



при получении СМС о несанкционированном списании средств со счета, заблокируйте карту



установите лимит выдачи денег



всегда будьте осторожны и не доверяйте подозрительным запросам или предложениям



Если вы стали жертвой мошенников



Позвоните в банк, сообщите о проблеме и заблокируйте карту. Попробуйте отменить транзакцию в личном кабинете банка или в мобильном приложении



позвоните по телефону горячей линии **МВД 8-800-222-74-47**



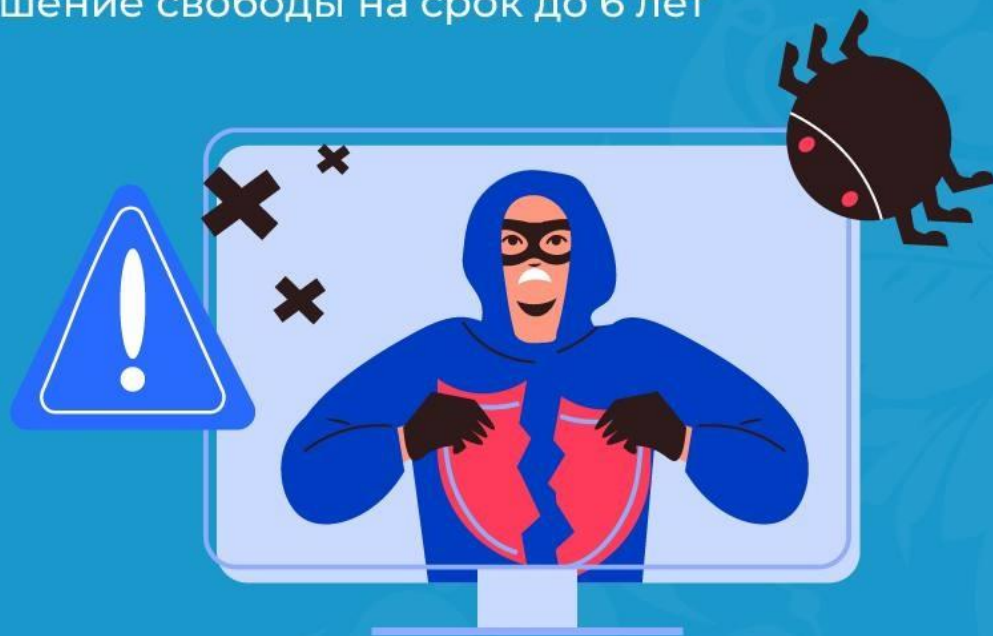
оставьте заявление о действиях мошенников в отделении полиции по месту жительства





Уголовная ответственность

Статья 159 УК РФ. Уголовная ответственность за мошенничество наступает за хищение чужого имущества или приобретение права на чужое имущество путем обмана.
Наказание – лишение свободы на срок до 6 лет





КАК НЕ ПОПАСТЬСЯ НА УДОЧКУ МОШЕННИКОВ



НЕТ!



Правила
безопасности,
которые уберегут
ваш кошелек



Как противостоять телефонным мошенникам

- интервью с начальником отдела по борьбе с мошенничеством Управления уголовного розыска ГУ МВД России по Свердловской области Артёмом Лаздынем

https://vk.com/wall-146815974_227766



Фишинг*

распространенный вид интернет-мошенничества, целью которого является получение доступа к личным данным для последующей кражи средств

Мошенники посредством манипуляций убеждают пользователей перейти по поддельным ссылкам и сайтам, чтобы завладеть их паролями, данными банковских карт и получить доступ к цифровым сервисам



* термин произошел от англ. *fishing* – «рыбалка»

- **Фишинг** — один из самых распространённых видов киберпреступлений, направленных на мошенничество с целью кражи личных данных пользователей.

Злоумышленники используют различные методы, чтобы обмануть жертву и заставить её раскрыть конфиденциальную информацию, такую как пароли, номера кредитных карт или данные учетных записей.

Обычно фишинг осуществляется через электронную почту, сообщения в социальных сетях или поддельные веб-сайты, имитирующие известные сервисы.

Как защитить себя в интернете?

Основные приемы фишинга

- Рассылка поддельных электронных писем от имени популярных брендов, банков или государственных органов с вирусными ссылками и файлами

- Распространение поддельных QR-кодов оплаты квитанций или форм регистрации

- Создание копий сайтов, досок объявлений, сервисов поиска услуг, маркетплейсов, интернет-провайдеров, управляющих компаний и банков





Как мошенники обманывают своих жертв?

Чтобы заставить вас пройти по ссылке или скачать файл, мошенники входят в доверие с помощью приемов социальной инженерии:

- копируют манеру общения руководителя, коллег, представителей власти, правоохранительных органов
- дублируют аккаунты в мессенджерах
- используют для рассылки адреса электронных почт, схожие с оригинальными
- апеллируют к поручениям авторитетных лиц
- торопят жертву, чтобы не дать возможности и опомниться. Остерегайтесь слов «срочно», «немедленно», «прямо сейчас»
- угрожают блокировкой или списанием средств
- просят передать конфиденциальные сведения: пароли, личные данные, финансовые реквизиты, просят открыть доступ к корпоративным системам



При фишинговой рассылке по электронной почте мошенники часто маскируют вредоносные файлы и ссылки под:

- уведомления об оплате онлайн-сервисов

- сообщения от портала Госуслуги

- письма от сервисов доставки

- письма от туроператоров

- уведомления о проблемах с учетной записью от техподдержки

- предложения пройти опрос или получить выигрыш



Как распознать обман?

- **Email-адрес содержит лишние символы, ошибки** или ранее вам не встречался

- **Поступают просьбы ввести логин, пароль**, а также предложения перейти по сомнительным ссылкам

- **Присутствует обезличенное обращение** или подпись в конце письма. Остерегайтесь слов «Уважаемый сотрудник», «Дорогой друг» и т.д.

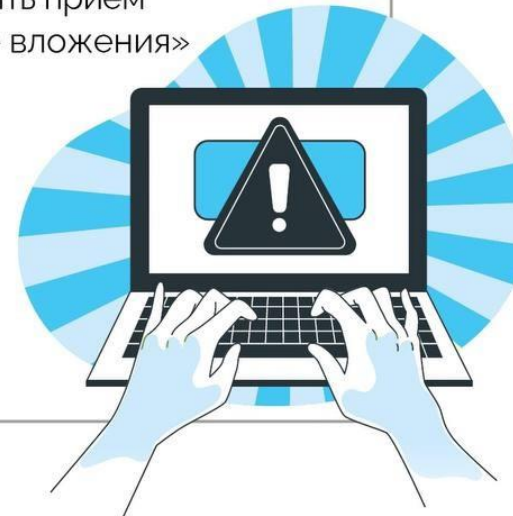
- Прикрепленная в письме ссылка имеет сокращенный вид или **начинается с http вместо https**

- **Имеются ошибки в словах и названиях брендов.** Мошенники намеренно совершают орфографические ошибки, чтобы обойти спам-фильтры



Как защитить себя от утечки данных?

- Не переходите по подозрительным ссылкам, не скачивайте и не открывайте незнакомые файлы
- Установите и регулярно обновляйте антивирусную программу
- Внимательно относитесь к переписке с незнакомыми
- Заведите отдельную почту для регистрации на сервисах и оформления подписок
- Регулярно меняйте пароли на новые и более сложные. Не используйте единый пароль для всех аккаунтов.
- В настройках почты включите «запретить прием сообщений, содержащих исполняемые вложения»
- Не храните в почте пароли и копии личных документов
- Никому не сообщайте реквизиты банковской карты, включая трехзначный код с обратной стороны, а также ПИН-коды и СМС от банка





Куда обратиться, если вы стали жертвой мошенников?

- Обратитесь в **отдел полиции по месту жительства** или через форму на официальном сайте **Министерства внутренних дел Российской Федерации** https://мвд.рф/request_main
- Подать жалобу о вредоносном ресурсе можно в информационной системе мониторинга фишинговых сайтов **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации** <https://paf.occsirt.ru/>
- Обратиться за бесплатной юридической помощью вы можете в **Центр правовой помощи гражданам в цифровой среде Роскомнадзора** <https://4people.grfc.ru>