КИБЕРМОШЕННИЧЕСТВО

Кибермошенничество — это умышленное противоправное деяние, совершаемое с использованием информационно-телекоммуникационных сетей (включая Интернет) и компьютерных технологий, целью которого является хищение денежных средств или иного имущества путем обмана или злоупотребления доверием.

Ключевые характеристики:

- ☑ **Использование цифровых технологий:** Преступление совершается через интернет, мобильную связь, компьютерные системы.
- ☑ **Дистанционность:** Преступник и жертва не встречаются лично.
- ☑ **Анонимность и трансграничность:** Злоумышленник может находиться в другой стране, что затрудняет его поимку.
- ☑ **Массовость:** Одна схема может быть направлена на тысячи потенциальных жертв одновременно.

Основные виды кибермошенничества:

- ☑ **Фишинг:** Создание поддельных сайтов, писем или сообщений, имитирующих официальные ресурсы (банки, госорганы, соцсети), для кражи логинов, паролей и данных карт.

- ☑ **Социальная инженерия:** Манипуляция людьми для совершения определенных действий или раскрытия информации. Сюда относятся:
  - **Звонки от "банка" или "полиции":** Мошенник, представляясь сотрудником службы безопасности, выманивает у жертвы данные карты, коды из SMS или убеждает перевести деньги на "безопасный счет".
  - **"Помощь родственнику":** Звонок с сообщением, что близкий человек в беде и срочно нужны деньги.

- ☑ **Скимминг**: Установка специальных устройств на банкоматы для считывания данных с магнитной полосы карты и скрытых камер для подсматривания PIN-кода.

- ☑ **Вредоносное ПО (трояны, кейлоггеры):** Программы, которые заражают компьютер или телефон и перехватывают вводимые данные, включая банковскую информацию.
- ☑ **Мошенничество в интернет-магазинах:** Продажа несуществующих товаров, создание фальшивых сайтов-однодневок.
- ☑ **Фиктивные предложения работы ("дропперство"):** Вербовка людей для "легкого заработка", которые на самом деле становятся соучастниками по отмыванию украденных денег.

- ☑ **Инвестиционное мошенничество:** Предложение вложить деньги в "супердоходные" проекты, криптовалюты или финансовые пирамиды.
- ☑ **Мошенничество с использованием ресурсов (Avito, Youla и т.д.):** Предоплата за товар, который не будет отправлен, или обмен с использованием поддельных платежных систем.

Ответственность за кибермошенничество

В Уголовном кодексе РФ нет отдельной статьи "кибермошенничество". Ответственность наступает по общим статьям о мошенничестве, но с учетом использования IT-средств.

- ☑ **Основные статьи УК РФ:**
- ☑ **Статья 159 УК РФ «Мошенничество»** — основная статья.
  - × Ч. 2: Мошенничество, совершенное группой лиц по предварительному сговору, с причинением значительного ущерба гражданину. → **Лишение свободы до 5 лет.**
  - × Ч. 3: Мошенничество с использованием своего служебного положения. → **Лишение свободы до 6 лет.**
  - × Ч. 4: Мошенничество, совершенное организованной группой либо в особо крупном размере. → **Лишение свободы до 10 лет.**
  - × **Примечание:** С 2013 года в ст. 159 есть примечание, прямо указывающее, что мошенничество с использованием электронных средств платежа (банковских карт) приравнивается к мошенничеству с отягчающими обстоятельствами (п. "з" ч. 2 ст. 159), что ужесточает наказание.
- ☑ **Статья 159.3 УК РФ «Мошенничество с использованием электронных средств платежей»** (устарела, но применяется к преступлениям до 2019 г.).
  - × С 2019 года эти составы включены в общую ст. 159.
- ☑ **Статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации»** — применяется, когда преступник вводит, удаляет или блокирует компьютерную информацию с целью хищения чужого имущества (например, взламывает электронный кошелек).
- ☑ **Статья 272 УК РФ «Неправомерный доступ к компьютерной информации»** — если мошенничеству предшествовал взлом баз данных или персональных устройств.
- ☑ **Статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»** — за создание троянов и другого ПО для кражи данных.

Важно: Даже если мошенник действовал один и был задержан при первой же попытке, его действия все равно подпадают под уголовную статью.

Меры безопасности (для граждан)

Защита от кибермошенничества строится на трех китах: **бдительность, техническая защита и знание основных схем.**

Финансовая и личная бдительность:

- ☑ **Никогда и никому не сообщайте:**
  - × **ПИН-код** от карты.
  - × **CVC/CVV-код** на обороте карты.
  - × **Коды из SMS** (даже если звонящий представляется сотрудником банка).
  - × **Данные карты** (номер, срок действия, имя владельца) на подозрительных сайтах.

- ☑ **Правило "Банк никогда не звонит":** Сотрудник банка не будет просить вас назвать коды из SMS, перевести деньги или установить какое-либо приложение. Если такой звонок поступил — положите трубку и перезвоните на официальный номер банка, указанный на обороте вашей карты.
- ☑ **Критическое мышление:** Не поддавайтесь панике и давлению. Если звонят и сообщают о проблеме с родственником, проверяйте информацию через прямые, известные вам контакты.
- ☑ *Технические меры защиты:*
- ☑ **Защита устройств:**
  - Устанавливайте антивирус на ПК и смартфон.
  - Регулярно обновляйте операционную систему и приложения.
- ☑ **Защита связи:**
  - Используйте **сложные и разные пароли** для почты, соцсетей и банковских приложений.
  - Включите **двухфакторную аутентификацию (2FA)** везде, где это возможно.
- ☑ **Безопасные платежи:**
  - Пользуйтесь официальным приложением своего банка.
  - Для онлайн-покупок заведите **виртуальную карту** с ограниченным лимитом.
  - Подключите **SMS-уведомления** или **push-оповещения** о всех операциях по карте.
- ☑ **Проверка сайтов:**
  - Всегда смотрите на адресную строку. Адрес настоящего сайта банка начинается с https:// (иконка замка). Остерегайтесь сайтов-клонов с похожими названиями.
- ☑ *Что делать, если вы стали жертвой:*
- ☑ **Немедленно позвоните в банк** по официальному номеру и **заблокируйте карту**.
- ☑ **Напишите заявление в банк** о несанкционированной операции. Банк может оспорить транзакцию по процедуре чарджбэк.
- ☑ **Обратитесь в полицию** с заявлением о преступлении (через ближайшее отделение или онлайн на сайте МВД). Обязательно сохраните номер КУСП (Талона-уведомления).

Вывод

Кибермошенничество — это постоянно эволюционирующая угроза. Преступники постоянно придумывают новые уловки, но основа защиты остается неизменной: личная осведомленность, критическое мышление и использование современных средств технической безопасности. Помните: ваша финансовая безопасность в цифровом мире в первую очередь в ваших руках.