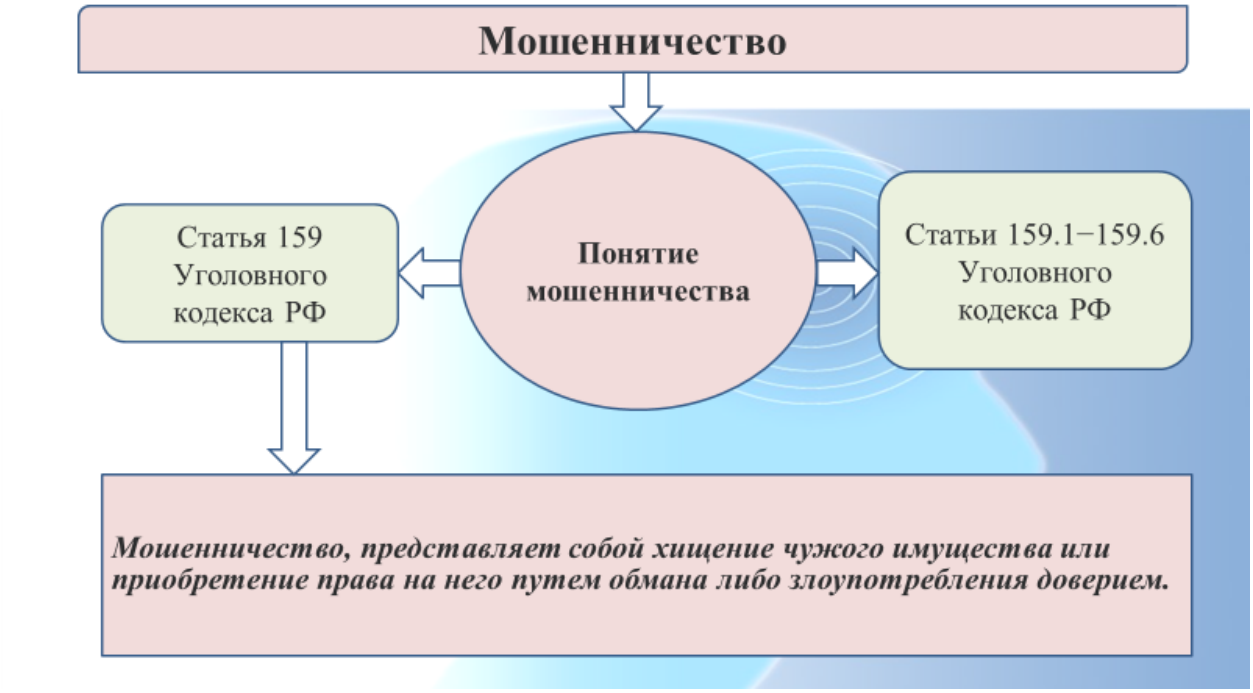
Мошенничество: признаки, наиболее распространенные схемы и способы обмана

Что такое мошенничество

Понятие мошенничества, его виды и меры ответственности прописаны в статьях 159, 159.1−159.6 Уголовного кодекса РФ (далее — УК РФ). Мошенничество, в соответствии со статьей 159 УК РФ, представляет собой хищение чужого имущества или приобретение права на него путем обмана либо злоупотребления доверием.



Признаки мошенничества

Прежде всего признаками являются:

- звонок или СМС с неизвестного номера;
- разговоры о финансах;
- просьбы предоставить персональные (конфиденциальные) данные;
- злоупотребление доверием — неизвестные представляются сотрудниками государственных органов, силовых структур, банков;
- попытки вывести из эмоционального равновесия — оказывается психологическое давление;
- принуждение к незамедлительным действиям, приводящим к поспешным, необдуманным поступкам.

Помимо этого, стоит проявить бдительность, если:

- предлагаемая от сотрудничества выгода является чрезмерно высокой, чтобы быть правдой;
- товар или услуга предлагаются по цене, значительно ниже рыночной;
- до получения товара или услуги просят внести аванс либо их полную оплату;
- отсутствуют какие-либо официальные документы или гарантии, подтверждающие сделку;
- предоставляемые контактные данные компании или лица кажутся подозрительными, у фирмы отсутствует официальный сайт и тому подобное.

Знание указанных признаков поможет распознать потенциальную угрозу быть втянутым в мошенническую схему и вовремя принять меры предосторожности.

Распространенные способы и схемы мошенничества

Рассмотрим самые распространенные схемы и способы мошенничества.

Телефонное мошенничество

- звонок от «сотрудника банка» с сообщением о блокировке банковской карты;
- сообщение о «родственниках, попавших в беду», требующих срочного перевода денег;

- предложение получения выигрыша в лотерее, для получения которого нужно оплатить «налог»;
- «сотрудник Многофункционального центра предоставления государственных и муниципальных услуг (МФЦ)» или «Почта России» сообщает о важном письме из государственного органа, для получения которого необходимо сообщить пришедший на телефон код;
- звонок от «оператора сотовой связи» с сообщением о ближайшей блокировке номера из-за истечения срока действия, с просьбой провести оплату;
- звонок из «поликлиники» с приглашением на диспансеризацию, с последующим выяснением номера СНИЛС и получением смс-сообщения с портала «Госуслуги»;
- звонок от «представителя Центробанка» или «сотрудника ФСБ» с сообщением о спонсировании ВСУ, с последующим требованием перевести все денежные средства на безопасный счет и так далее.

Схемы мошенничества с использованием телефона весьма разнообразны и очень распространены. Мошенники постоянно придумывают все новые и новые способы обмана посредством телефонных звонков.

Интернет-мошенничество

Самыми часто встречающимися способами интернет-мошенничества эксперт назвал:

- фишинговые сайты (очень похожие на настоящие), имитирующие страницы банков или государственных учреждений и организаций;
- фейковые интернет-магазины, продающие несуществующие товары;
- мошенничество в социальных сетях (мошенники присылают сообщение с предложением выгодно купить товар и перевести денежные средства);
- мошенничество с использованием маркетплейсов или площадок с объявлениями с последующим перенаправлением на поддельный сайт или же с просьбой перевести предоплату на банковскую карту;
- фейковые письма на почту (e-mail) от имени банков или иных сервисов с последующим запросом конфиденциальных данных для подтверждения учетной записи.

Нередко практикуется мошенничество с использованием сайтов знакомств, с дальнейшим переходом на личные встречи или общение в социальных сетях, с целью получения денежных средств либо иных данных.

Мошенничества в социальных сетях

«ВКонтакте». «Одноклассники», «Instagram», <<Skype» и т.д.

В данном случае можно выделить три способа совершения мошенничества:

1. Злоумышленник, путем взлома страницы, осуществляют рассылку сообщений всему списку контактов, с различными текстами, которые зачастую начинаются с обычного приветствия. В случае ответа на сообщение, злоумышленник просит оказать материальнуо помощь, под

различными предлогами (необходимость оплаты услуг, оказание помощи больному родственнику) и отправляет данные банковской карты, на которую нужно перечислить денежные средства.

В случае получения такого рода сообщений, обязательно необходимо связаться с лицом, которому принадлежит страница социальной сети, и уточнить, в действительности ли он отправил сообщение.

2. Продажа товаров в группах и страницах социальных сетей. Данный способ мошенничества схож с продажей товаров на сайтах бесплатных объявлений, при которых мошенник размещает объявление о продаже товара, которым в действительности не владеет и в ходе переписки с потерпевшим, просит перевести денежные средства на банковскую карту (всю сумму, либо часть суммы), после чего обязуется отправить товар почтой либо через транспортную компанию.

При заказе товара данным способом, проверяйте добросовестность продавца, путем прочтения комментариев и отзывов.

Мошенничества при знакомствах в социальных сетях сети Интернет.

В данном случае злоумышленники в большинстве случаев представляются иностранцами и входе продолжительной переписки, входят в доверие потерпевших и в последующем под различными предлогами убеждают их перечислить денежные средства.

Мошенничество с банковскими картами

Что касается мошенничества с банковскими картами, то здесь наиболее распространенными являются следующие виды преступлений:

1. Скимминг. В данном случае мошенник устанавливает на банкомат или терминал специальное устройство, которое считывает данные с карты.

2. Социальная инженерия. Как было сказано выше, мошенники могут звонить от имени сотрудника банка с сообщением о блокировке карты и просьбой подтвердить ее данные.

3. Фишинг. Как указывалось выше, при таком виде мошенничества с картами создаются поддельные, очень похожие на настоящие, сайты банков, интернет-магазинов, государственных организаций, через которые преступники просят сообщить данные банковской карты.

4. Взлом системы дистанционного банковского обслуживания (онлайн-банкинга). Взломав приложение банка, злоумышленники перехватывают данные для дальнейшего перевода средств от имени владельца карты на свои счета или для связи с ним, чтобы убедить перечислить деньги, а также для проведения от имени владельца банковской карты различных операций (например, выпуск кредитной карты и прочее).

Очень часто площадкой для использования банковской карты при мошенничестве становятся частные объявления, где преступник может выступать как продавцом, так и покупателем. Например, мошенник под видом покупателя выражает глубокую заинтересованность в товаре, и готов

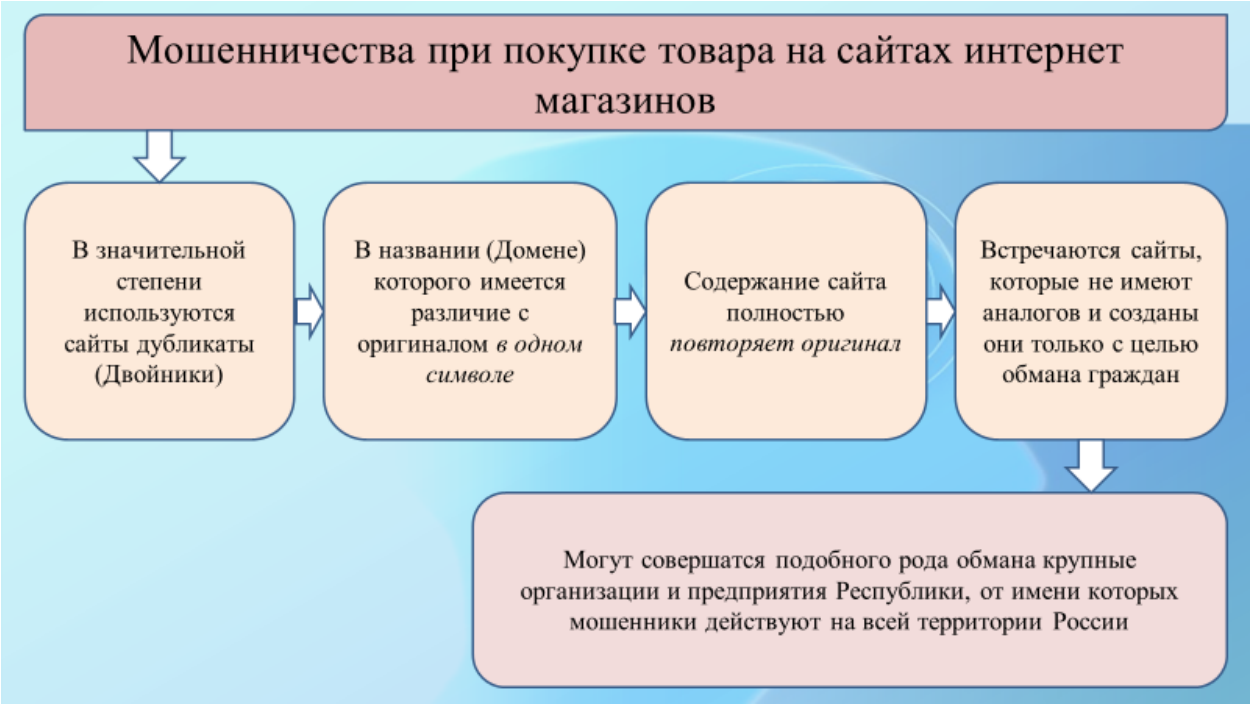
оплатить аванс, прося предоставить данные карты для перевода. При этом он, помимо номера карты, просит сообщить код, указанный на обратной стороне.

Важно! Использование чужой карты банка считается не мошенничеством, а кражей, если человеку, нашедшему или укравшему ее, становится известен PIN-код, и он вводит его при оплате товаров или с его помощью лично снимает деньги с данной карты в банкомате.

Мошенничества при покупке товара на сайтах интернет-магазинов.

В данном случае в значительной степени используются сайты дубликаты (Двойники), в названии (Домене) которого имеется различие с оригиналом в одном символе. При этом содержание сайта полностью повторяет оригинал. Также встречаются сайты, которые не имеют аналогов и созданы они только с целью обмана граждан.

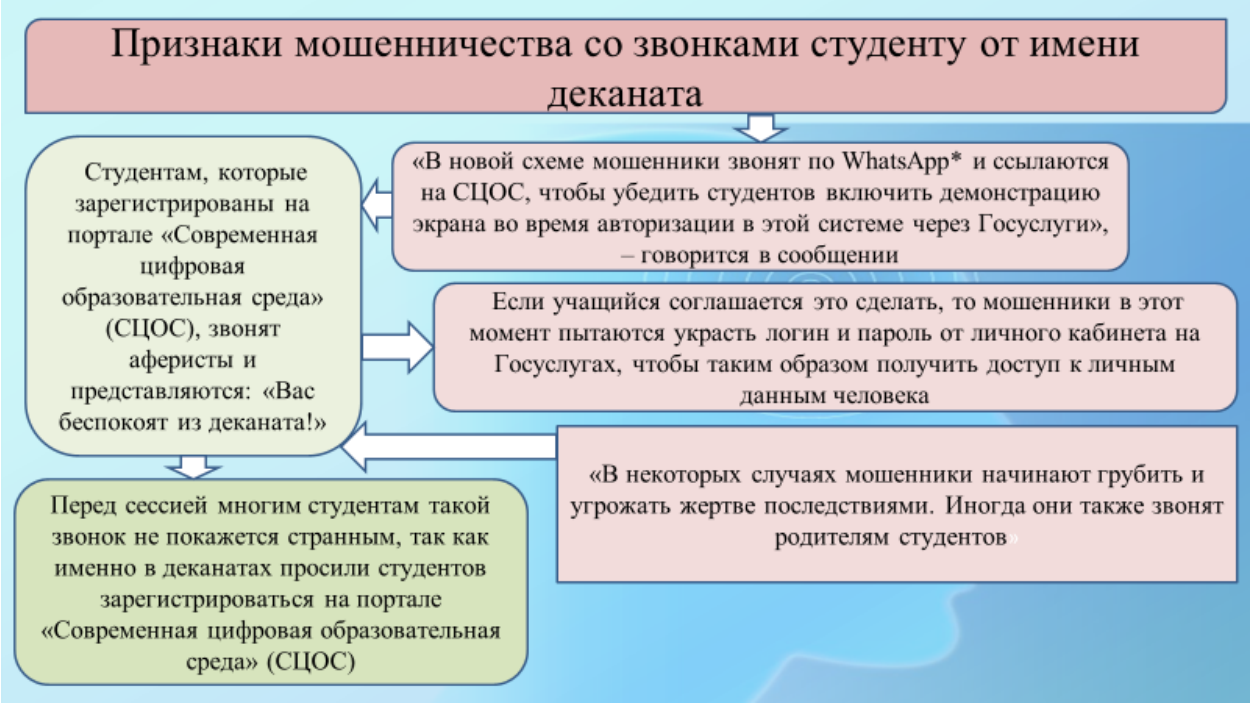
Не застрахованы от подобного рода обмана крупные организации и предприятия Республики, от имени которых мошенники действуют на всей территории России.



Чтобы не стать жертвой таких преступлений, необходимо проверять подлинность интернет-сайтов, на которых осуществляется заказ того или иного товара, путем прочтения комментариев и отзывов, размещенных на просторах сети Интернет. Существует возможность проверить дату создания сайта на ресурсе reg.ru, в результате станет понятно, насколько долго данный сайт существует, как правило сайты, используемые мошенниками, создаются незадолго до самого факта предоставления услуг, продажи товара.

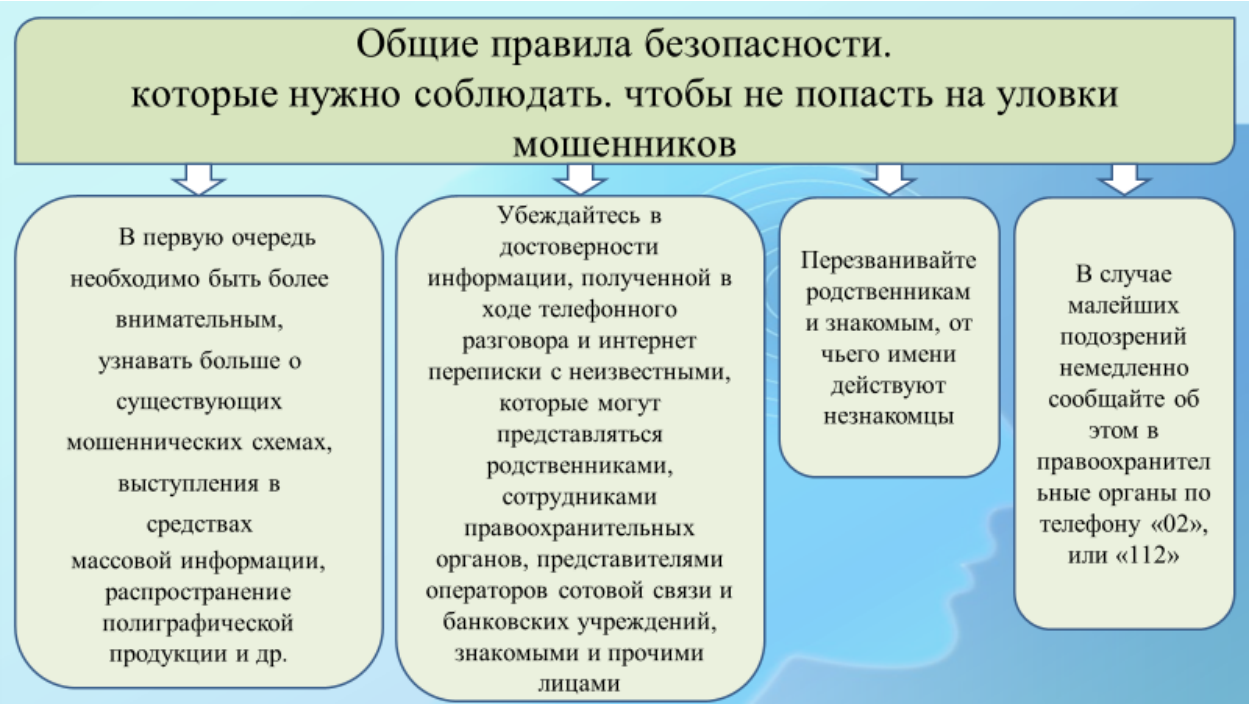
Мошенники начали использовать новую схему, направленную на студентов. Они выдают себя за деканат и просят срочно зарегистрироваться на портале «Современная цифровая образовательная среда», цель злоумышленников,

которые чаще всего звонят студентам через мессенджер WhatsApp*, — добиться от учащихся демонстрации экрана во время авторизации через портал «Госуслуги». Как рассказали заметившие схему студенты, если мошенникам не удается получить желаемое, даже с использованием грубости, через время они звонят их родителям.



Как не стать жертвой мошенников

- не сообщайте личные данные — банки и государственные органы никогда не запрашивают данные карт или пароли по телефону или электронной почте;
- следите за новостями, посвященными теме мошенничества, проверяйте информацию — уточняйте сведения о компаниях и предложениях через официальные источники;
- устанавливайте антивирусное программное обеспечение, регулярно обновляйте антивирусы — защищайте свои устройства от вредоносных программ;
- не переводите деньги под давлением — если вас торопят с решением, это повод насторожиться;
- не ведитесь на предложения о быстром заработке — если вам предлагают «легкие» деньги или выгодные инвестиции, действуйте осторожно, нередко такие предложения исходят от мошенников;
- периодически проверяйте выписки по счетам и уведомления о проведенных транзакциях — это позволит вовремя обнаружить подозрительную активность и станет хорошей профилактикой мошенничества.



Как подать заявление о мошенничестве в полицию

Необходимо выполнить следующие действия:

- собрать все доказательства (чеки, скриншоты переписок, выписки со счетов);
- написать заявление, указав в нем все известные данные о мошеннике (номера телефонов, реквизиты счетов, адреса);
- обратиться в ближайшее отделение полиции с заявлением о мошенничестве.

Не забудьте получить талон-уведомление о принятии заявления
и регистрации его в книге учета сообщений о происшествиях (КУСП),
с присвоением номера.