В последнее года в РФ наблюдается рост хищений, совершаемых с использованием информационно-коммуникационных ресурсов.

Развитие технологий в современном мире обуславливает их проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели, в том числе личное обогащение.

Мошенники используют разные способы обмана людей в интернете: от спама до создания сайтов-двойников. Цель злоумышленников — заполучить персональные данные пользователя, номера банковских карт, паспортные данные, логины и пароли.

**Способы хищений денег с банковских счетов граждан**

- телефонный звонок от лица вымышленных сотрудников банка, службы безопасности, правоохранительных органов, в том числе прокуратуры с сообщением о необходимости предоставления информации о номере карты, ее владельце, сроке действия, трехзначном коде, указанном на оборотной стороне карты, в связи с «проведением профилактических работ», «блокированием карты по подозрению в попытке хищения денег» и т.п.;

- просьбы внесения предоплаты за товар или услуги в Интернете;

- просьбы о получении сведений о номере карты, ее владельце, сроке действия, трехзначном коде, указанном на оборотной стороне карты для «перечисления» денег за купленный товар либо услугу;

- сведения о выигрыше;

- телефонный звонок лицу с сообщением, что у его родственника (знакомого) проблемы, например, попал в ДТП, совершил правонарушение и т.п., и предлагает «решить проблему» с помощью внесения на счет злоумышленника определенной денежной суммы.

- и т.д.



**Чтобы не оказаться жертвой мошенников необходимо знать следующее:**

– сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;

– ни при каких обстоятельствах не сообщать данные вашей банковской карты, а также секретный код на оборотной стороне карты;

– хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;

– не сообщать пин-код третьим лицам;

– остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;

– лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;

– внимательно читайте СМС сообщения приходящие от банка;

– никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС сообщении от банка;

– помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в СМС сообщении от банка;

– сотрудники банка никогда не попросят вас пройти к банкомату;

– если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;

– не покупайте в интернет – магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;

– никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;

– в сети «Интернет» не переходите по ссылкам на неизвестные сайты.

О подобных фактах следует незамедлительно сообщать в правоохранительные органы, в первую очередь – в полицию. Такие сообщения тщательно проверяются в целях установления лиц, причастных к преступной схеме, и их привлечения к уголовной ответственности.

**Пример составления заявления о преступлении.**

Начальнику ОМВД России по г. Кумертау

подполковнику полиции

Абзалилову М.З.

Иванова Александра Ивановича, проживающего по адресу: г. Кумертау, ул. Лесная, д. 155, кв. 203 моб. тел. №87775552222

ЗАЯВЛЕНИЕ

Прошу Вас привлечь к уголовной ответственности неустановленное лицо, которое позвонило мне на сотовый телефон номер 87775552222, около 19 часов 15 июня 2022 года, представилось сотрудником безопасности банка, после чего войдя ко мне в доверие, указав, что с моей карты неустановленные лица пытаются осуществить денежные перевод, попросило продиктовать последние цифры моей банковской карты, после чего сообщить пароли пришедшие мне в смс сообщениях, в результате действий неустановленного лица, с моей карты были похищены все находящиеся там денежные средства в сумме 15 000 рублей.

За заведомо ложный донос по ст. 306 УК РФ предупрежден.

Дата Подпись

**Уголовная ответственность за преступления, совершённые с использованием информационно-телекоммуникационных технологий**

**ст. 158 ч. 3 п. «г» УК РФ - кража** с банковского [счета](http://www.consultant.ru/document/cons_doc_LAW_10699/57b5c7b83fcd2cf40cabe2042f2d8f04ed6875ad/), а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного [ст. 159.3](http://www.consultant.ru/document/cons_doc_LAW_412702/c193654ae5c3bd5b02d92ade18796cd8864ec353/#dst1233) УКРФ) – лишение свободы до 6 лет

ст. 159.3 УК РФ - мошенничество с использованием [электронных средств платежа](http://www.consultant.ru/document/cons_doc_LAW_389164/4f41fe599ce341751e4e34dc50a4b676674c1416/#dst100035) – лишение свободы до 3 лет

ст. 187 УК РФ **-** Изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты (за исключением случаев, предусмотренных [статьей 186](https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=412702&dst=103380&field=134&date=11.05.2022) настоящего Кодекса), а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств, - лишение свободы до 6 лет

ст. 159.6 УК РФ **-** мошенничество в сфере компьютерной информации



**ПРОКУРАТУРА**

**города Кумертау**



**ПАМЯТКА**

Как защитить себя и свои деньги от мошенников.

Безопасный Интернет.

г. Кумертау - 2022