

Обезопасить личные финансы позволит соблюдение базовых правил:

- пользоваться отдельной виртуальной картой для покупок, пополнять ее лучше разово
- только при совершении оплаты;
- создавать сложные пароли и использовать разные данные для почтовых ящиков, социальных сетей, других сайтов;
- не кликать по неизвестным ссылкам, которые приходят по электронной почте, в мессенджерах, социальных сетях, особенно если предлагают что-то бесплатное или на выгодных условиях;
- не сообщать посторонним личные данные карты и не вводить их на незнакомых сайтах, не указывать коды безопасности из смс-сообщений;
- критически оценивать любую информацию, сообщения, объявления в Интернете, а также не верить на слово внезапным обращениям от друзей и родственников – скорее всего неожиданная просьба о деньгах поступила от мошенника, который взломал аккаунт.



При подозрении на Интернет-мошенничество необходимо незамедлительно позвонить в банк и заблокировать карту, после чего обратиться с заявлением в правоохранительные органы:

Дежурная часть УМВД России по г. Краснодару



г. Краснодар, ул. Октябрьская, 121



тел.: 268-40-45, 102;

Отдел полиции (Центральный округ) УМВД России по г. Краснодару:



г. Краснодар ул. Садовая, 110



тел.: 255-78-66;

Отдел полиции (Прикубанский округ) УМВД России по г. Краснодару:



г. Краснодар, ул. Им. Космонавта Гагарина, 103



тел.: 226-52-22;

Отдел полиции (Карасунский округ) УМВД России по г. Краснодару:



г. Краснодар, ул. Ставропольская, 205



тел.: 231-80-13;

Отдел полиции (п. Калинино) УМВД России по г. Краснодару,



г. Краснодар, ул. им. 40-летия Победы, 146/6, корп. 1;

Прокуратура г. Краснодара:



г. Краснодар, ул. Октябрьская, д. 31/2



тел.: 268-62-58;

Если заявление принято не было –
обращаться в прокуратуру г. Краснодара:
г. Краснодар, ул. Октябрьская, д. 31/2,
тел.: 268-62-58.

Любое **МОШЕННИЧЕСТВО** – это уголовно-наказуемое преступление, ответственность за которое предусмотрена статьями 159-159.6 УК РФ.



Мошенничество в сети Интернет – это совокупность преступлений, характеризующихся использованием технологических и коммуникационных возможностей компьютерных систем, подключенных к глобальной сети Интернет. В настоящее время в сети Интернет осуществляется огромное количество различных мошеннических действий.

Так, **максимальный срок лишения свободы** за мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) и в сфере компьютерной информации (ст. 159.6 УК РФ) – **до 10 лет,**

а максимальный размер штрафа – до миллиона рублей.



Условиями совершения мошеннических действий в сети Интернет являются:

- анонимность пользователей;
- возможность бесплатного доступа к сети Интернет;
- возможность охватить большую аудиторию;
- бесконтактность;
- скорость распространения информации.

Активный рост рынка электронных платежей и онлайн-шопинга – это причины развития новых форм мошенничества в сфере информационных технологий.

САМЫМИ РАСПРОСТРАНЕННЫМИ ВИДАМИ ТАКОГО МОШЕННИЧЕСТВА ЯВЛЯЮТСЯ:



ФИШИНГ

– это кража идентификационных данных (ФИО, пароль и номер банковской карты). Злоумышленники пользуются невнимательностью граждан и завладевают конфиденциальной информацией путем создания сайтов-клонов, фальшивых аккаунтов в мессенджерах и социальных сетях, электронной рассылки писем.



ВИШИНГ

– это один из методов мошенничества с использованием социальной инженерии. Мошенники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя), под различными предлогами выманивают конфиденциальную информацию у владельца платежной карты или побуждают его совершить определенные действия со своей картой посредством угроз и манипуляций.



КАРДИНГ

– это кража конфиденциальной информации о пользователях и снятие денежных средств со счетов граждан без их ведома. Осуществляется посредством взлома серверов интернет-магазинов, расчетных и платежных систем, для чего используются вирусные программы.



МОШЕННИЧЕСТВО ЧЕРЕЗ ЭЛЕКТРОННУЮ ПОЧТУ – так называемые «нигерийские письма». Они содержат в себе легенду о наследстве от мифического родственника и просьбу перевести деньги на счет для получения оплаты услуг адвоката или выплаты комиссии.



МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ФИНАНСОВЫХ ПИРАМИД – это маскировка под инвестиции в криптовалюту, кэшбек-сервисы, сетевые магазины, совместные покупки, майнинг.



МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-КОШЕЛЬКОВ – чаще всего в таких случаях покупатель переводит предоплату продавцу на интернет-кошелек, но в итоге не получает ни товара, ни денег.



МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ САЙТОВ-ПОДДЕЛОК – они же сайты-клоны, которые внешне (дизайн, интерфейс, оформление) не отличаются от оригинальных сайтов. Создаются наподобие популярных социальных сетей и сайтов с целью выманивания денежных средств или взлома аккаунтов.



ИНТЕРНЕТ-ПОПРОШАЙНИЧЕСТВО – выражается в просьбе пожертвовать какую-либо сумму денежных средств.

