

Следственное управление разъясняет о безопасном киберпространстве



Поскольку в современном обществе без сети Интернет уже не обойтись, то и мошенничество с использованием «всемирной паутины» является одним из наиболее распространенных видов хищения. В сети можно совершать различные денежные операции, осуществлять товарообмен, работать и получать заработную плату. Все это является объектом посягательства со стороны мошенников. В связи с тем, что в сети зарегистрировано огромное количество людей, такая разновидность мошенничества является наиболее опасной и серьезной. Тем более преступления могут совершаться на дальних расстояниях.

Наиболее часто в сети встречаются следующие разновидности данного мошенничества:

- предложения об участии в разнообразных проектах. Для того чтобы стать участником, нужно внести первоначальный взнос;

- взлом и блокировка учетных записей в социальных сетях. Для того чтобы вновь получить доступ к своим страницам, злоумышленники предлагают отправить сообщение на конкретный номер за высокую стоимость, при этом без всяких гарантий на разблокировку;
- блокировка оперативной системы, установленной на персональном компьютере, с помощью вирусных программ, для снятия которой также требуется совершить аналогичные действия;
- призывы перечислить денежные средства на благотворительные счета или на дорогостоящее лечение;
- мошенничество на торговых интернет-площадках (махинации с предоплатой, когда деньги переводятся, а товар к покупателю не доходит, или приходит по низкой стоимости; с кредитными карточками; с платным участием в конкурсе по трудоустройству и другие способы мошенничества);
- распространение сообщений путем рассылки писем на адреса электронных ящиков с информацией о блокировке доступа к электронному кошельку или кредитной карточке. Для того чтобы разблокировать преступники рекомендуют перейти по указанной ссылке, и на странице требуется ввести личные сведения (коды, пароли).

Если вы стали жертвой злоумышленников в сети, вне зависимости от суммы похищенных денежных средств, то обращаться за восстановлением нарушенных прав следует в правоохранительные органы.

Дополнительно можно обратиться в банковскую организацию для приостановления операции по переводу денег (если перечисление еще не было осуществлено).

Следственное управление призывает граждан соблюдать простые правила финансовой безопасности: 1) не совершать финансовых операций по инструкциям, полученным в ходе телефонных разговоров; 2) не сообщать никому реквизиты банковских карт, PIN-код, CVC/CVV-коды и одноразовые пароли для подтверждения операций.

Если вам звонят и представляются сотрудником правоохранительного органа, проверяйте озвученную информацию по телефонам «горячих линий» соответствующего госоргана. В случае, если мошенники представляются следователями СК России, можно воспользоваться телефонами, размещенными на официальных сайтах региональных следственных управлений (по месту вашего жительства), а также телефоном доверия СК России 8 (800) 100-12-60 (работает только на прием входящих вызовов).

Адрес страницы: <https://altai.sledcom.ru/news/item/1862076>