

Как не стать жертвой преступного обмана

Мошенничество - одна из самых распространенных форм хищения. Злоумышленники пользуются доверчивостью граждан, приспосабливаются к изменяющейся социально-экономической ситуации, изобретая новые способы хищения денежных средств и имущества граждан!

Мошенники создают сайты, внешне схожие по дизайну и доменным именам с официальными сайтами госорганов, и предлагают получить различные меры поддержки и компенсационные выплаты. Не переходите по сомнительным ссылкам и не открывайте сомнительные интернет-страницы. Помните, что меры государственной поддержки предоставляются без предоплаты, комиссии и только государственными органами (органы соцзащиты населения и ПФР). Злоумышленники предлагают покупателям приобрести товары по заниженным ценам. Потом выясняется, что товар находится в другом городе, и жертве предлагают оформить доставку, для чего направляют ссылку.

Страница оплаты по этой ссылке полностью копирует страницу легитимного ресурса. Покупатель вводит данные банковской карты и оплачивает товар. После этого мошенники исчезают. При общении с потенциальным продавцом постарайтесь получить как можно больше фотографий товара, не спешите переводить деньги за доставку, убедитесь, что реквизиты для перевода действительно принадлежат службе доставки. Киберпреступники связываются с клиентами банка и сообщают им, что банковский счет под угрозой, произошла попытка снятия денежных средств или смена номера мобильного телефона он-лайн банка.

После клиента просят установить приложение для удалённого управления смартфоном.

Если доверчивый клиент устанавливает приложение для удалённого доступа, то злоумышленники получают полный доступ ко всем учетным записям. Под аналогичными предложениями мошенники могут позвонить клиенту банка и обманным путем получить персональную информацию по банковской карте, что даст им возможность быстро похитить денежные средства, находящиеся на счете. Ни при каких обстоятельствах не сообщайте посторонним лицам номер банковской карты, ее пин-код и код безопасности, не устанавливайте сомнительные мобильные приложения или антивирусные программы на свой телефон или компьютер.

Если Вам поступил звонок лучше самостоятельно связаться с кредитной организацией и выяснить что произошло. Помните, что техническая поддержка банка никогда не просит удаленный доступ к смартфону или компьютеру пользователя.

Ключевая задача любого мошенника - заставить человека врасплох! Если Вам позвонили и сообщили, что родственник, знакомый или близкий человек попал в беду и необходимо срочно перевести или передать денежные средства для его спасения... не торопитесь! Позвоните якобы попавшему в беду. После такого звонка как правило все встает на свои места. Если Вы стали жертвой или свидетелем мошенничества – незамедлительно сообщите в полицию (02, с мобильного - 102).

Прокурор района
старший советник юстиции



А.С. Титов