**Предупрежден – значит вооружён: как не попасть в сети мошенников**

Сотрудники полиции дают советы о профилактике преступлений в сфере IT-технологий, защите своих персональных данных, о том, что нужно знать гражданам, чтобы не стать жертвой злоумышленников.

В последнее время все больше жителей Ульяновской области становятся жертвами мошеннических действий, совершаемых с использованием мобильной связи и сети Интернет.

Как правило, гражданам звонят мошенники, которые представляются сотрудниками службы безопасности банка и сообщают о несанкционированных попытках оформления на граждан кредитов, о фиксации системой безопасности неправомерных доступов к счетам граждан, о выявлении среди сотрудников банка лиц, распространяющих конфиденциальные сведения, после чего, как правило,

убеждают граждан в необходимости оформления кредитов, чтобы таким образом вернуть банку средства, незаконно оформленные мошенниками;

 просят сообщить реквизиты карт **(CVV- или CCV-код, код из СМС) якобы** для идентификации личности клиента, перевода средств на «безопасный счет», для установления специальной программы удаленного доступа;

могут попросить выполнить ряд операций через банковский терминал, в результате которых граждане подключают посредством приложения «Мобильный банк» чужой номер к своей карте или сами переводят денежные средства на незнакомые счета.

*Чтобы не стать жертвой мошенников, не сообщайте никому реквизиты ваших карт. Чтобы проверить поступившую информацию о попытке несанкционированного списания средств, оформлении кредита, необходимо позвонить в клиентскую службу поддержки банка, номер которой указан на обратной стороне карты.*

*Помните, что сотрудники банка никогда не просят клиентов сообщить конфиденциальные сведения, не требуют совершать активные операции с картами.*

Еще одним из распространенных видов мошеннических действий является обман пользователей сети Интернет, продающих и покупающих товары на сайтах бесплатных объявлений. Мошенники, предлагая несуществующий товар, взымают за него предоплату или полную стоимость, после чего перестают выходить на связь. Другие предлагают оформить «безопасную сделку» и для ее успешного оформления сбрасывают ссылку, как правило, на фишинговый сайт, на котором после заполнения формы для получения средств, со счетов граждан списываются денежные средства. Также мошенники могут запросить реквизиты карт, включая защитные коды и коды из смс – сообщений, под предлогом невозможности проведения платежной операции.

*При совершении покупок через сайты бесплатных объявлений, страницы интернет - магазинов обязательно обратите внимание на подозрительно низкую стоимость, отсутствие возможности приобрести товар за наличные, самовывоза. Если на сайте указана только электронная почта или сотовый телефон и отсутствует географический адрес офиса или склада, лучше воздержаться от приобретения товаров.*

*Прежде чем воспользоваться услугами интернет – магазина или сайта компании проверьте отзывы о них.*

*Обязательно попросите продавца подтвердить реальное наличие товара фотографиями с нескольких ракурсов. Не вносите предоплаты, пока не убедитесь, что покупаемый вами товар существует, а продавец – реальный человек.*

*Если продавец или покупатель настойчиво предлагает перейти из чата на сайте объявлений в другой мессенджер - это повод насторожиться. Чаще всего так поступают те, кто распространяет ссылки на вредоносные ресурсы.*

*Имейте в виду, что внося 100% оплату до получения товара, вы рискуете потерять всю сумму.*

*Для проведения денежных операций заведите отдельную карту.*

Телефонные аферисты стали применять новый способ психологического воздействия на граждан. Например, звонят от имени сотрудников правоохранительных органов и сообщают о расследовании уголовных дел по фактам мошеннических действий, о проведении совместных с банками мероприятий по выявлению недобросовестных банковских сотрудников, якобы «сливающих» данные клиентов. Звонок от представителя правоохранительных органов убеждает граждан в серьёзности происходящего, поэтому последующий разговор с якобы сотрудником службы безопасности банка не вызывает подозрений и пострадавшие сообщают им реквизиты своих карт, включая защитные коды, оформляют кредитные обязательства.

При этом мошенники, используя возможности IP-телефонии, производят подмену своего номера телефона таким образом, что при входящем звонке отображаются реальные телефонные номера дежурных частей отделов полиции. Проверив такие номера в поисковых системах, можно убедиться, что они действительно принадлежат официальным организациям.

*Необходимо помнить, что сотрудники правоохранительных органов не звонят гражданам, чтобы сообщить об утечке личных данных клиентов банков, о несанкционированных доступах к счетам граждан, никогда не запрашивают по телефону конфиденциальную информацию и не требуют проведения каких-либо финансовых операций.*

*Просьбы подобного характера являются действиями мошенников!*

Взломы страниц аккаунтов в социальных сетях – распространенный способ мошенничества. Если вам пришло сообщение от друзей или родственников с просьбой об оказании финансовой помощи в связи с внезапно возникшими обстоятельствами, не поддавайтесь первоначальному порыву.

*Сразу же свяжитесь с данным человеком по телефону или посредством в смс – переписки, в ходе которой задайте вопросы, ответы на которые сможет дать только настоящий ваш знакомый или родственник.*

Люди пенсионного возраста довольно часто лишаются своих сбережений в результате мошеннических действий по типу «Ваш родственник попал в ДТП». Злоумышленники в телефонной беседе представляются сотрудниками полиции либо имитируют голоса родственников и сообщают о виновности близких в ДТП. Чтобы не привлекать виновника к ответственности, смягчить наказание или решить вопрос с пострадавшим в результате ДТП человеком мошенники озвучивают определенную сумму. Взволнованные пенсионеры соглашаются передать имеющиеся сбережения, за которыми, как правило, приезжает курьер.

*В случае поступления звонка с плохими известиями о близких, не впадайте в панику. Не называйте своего имени и имен своих родственников. Пусть звонивший назовет их сам. Сразу же перезвоните своему родственнику, который якобы попал в беду. Даже если вы уверены, что только что с ним разговаривали.*

*Если вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он отделения полиции, после чего позвоните
на номер «02» и узнайте номер дежурной части данного отделения,
по которому уточните, действительно ли к ним доставлялся ваш родственник или знакомый.*

Основная ошибка всех пострадавших от мошеннических действий- это участие в разговоре, который на самом деле нужно немедленно прекратить.

Пресс – служба УМВД России по Ульяновской области