Прокуратура Ленинградского района г. Калининграда разъясняет:

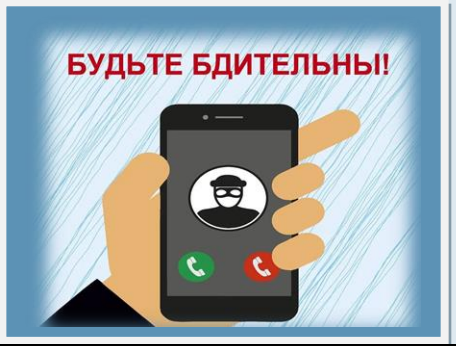
В настоящее время, в 21 веке, Интернет проник во все сферы общественной жизни. К сожалению, этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие цель личного обогащения путем совершения противоправных действий в отношении людей, через доступ к информации с помощью сети Интернет для общения с потенциальными жертвами обмана.

Способы хищений при помощи сети Интернет:

1. Преступник, под видом сотрудника банка, звонит человеку, являющемуся владельцем банковской карты, и узнает пароль, все реквизиты банковской карты, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке либо путем предложения кредитов на очень заманчивых условиях.

2.Обман доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или о перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их родственников от уголовной ответственности. Нередко злоумышленники сами представляются сотрудниками правоохранительных органов.

3.Преступник посылает потерпевшему e-mail, подделанный под официальное письмо – от банка или платежной системы – требующее проверки определенной информации, или совершения определенных действий. Это письмо, как правило, содержит ссылку на фальшивую веб-страницу, которая является полной копией официального интернет-источника. На фальшивой странице пользователю требуется ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.



4.Злоумышленники зачастую используют и активно распространяют вредоносные программы, такие как "Троянский конь". Злоумышленник направляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса. Это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой, при переходе по которой на устройство пользователя скачивается вредоносная программа. После чего преступник получает удаленное управление и возможность осуществления перечисления денежных средств со счета привязанной к абонентскому номеру банковской карты.

Для того, чтобы избежать совершения в отношении себя преступлений, оградить себя от хищения денежных средств необходимо быть предельно внимательными при осуществлении банковских операций с использованием сети «Интернет» и мобильных телефонов. Не сохраняйте банковские реквизиты, номера банковских карт, коды на сайтах непроверенных компаний, банков и т.д., лучше при необходимости вводить свои данные при осуществлении тех же платежей каждый раз. Не поддавайтесь на уловки мошенников и всегда перепроверяйте полученную информацию, всегда найдите способ связаться с родственниками, чтобы проверить полученную информацию.

Чтобы не оказаться жертвой мошенников необходимо знать– 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;

– не 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;

– 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.