**ПАМЯТКА**

об основных способах дистанционного мошенничества

Несмотря на принимаемые правоохранительными органами меры, дистанционные хищения с использованием информационно-телекоммуникационных технологий стремительно набирают силу.

Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву раскрывать всю информацию о себе либо совершать те или иные действия, используют человеческие слабости (стяжательство, алчность), чувства (сострадание, обеспокоенность за близких, жалость) в своих корыстных интересах. Телефоны, компьютеры и электронные архивы позволяют узнать о вас довольно много. Жертвами мошенников с банковскими картами становятся люди совершенно разных возрастов.

Вот ситуации, которые ДОЛЖНЫ ВАС НАСТОРОЖИТЬ:

Вам звонят с сообщением, что ваш родственник или знакомый попал в аварию, за решетку, в больницу, и теперь за него нужно внести залог, штраф, взятку – в общем, откупиться. ЭТО ЖУЛИКИ! Техника сегодня позволяет даже подделать голос человека.

На телефон поступают звонки или сообщения с неизвестных номеров с просьбой положить на счет деньги, чтобы помочь детям или получить якобы выигранный приз. ЭТО ЛОЖЬ!

Вам сообщают о крупном денежном выигрыше по SMS и предлагают отправить SMS ­сообщение или позвонить по указанному номеру для получения приза. НЕ ДЕЛАЙТЕ ЭТОГО! ЭТО, КАК ПРАВИЛО, МОШЕННИЧЕСТВО.БУДЬТЕ БДИТЕЛЬНЫ, СПОКОЙНЫ И НЕ БОЙТЕСЬ ЗАПУГИВАНИЙ И УГРОЗ! ОБЯЗАТЕЛЬНО СВЯЖИТЕСЬ С РОДСТВЕННИКАМИ!

Если социальные работники, контролеры службы газа, слесари, электрики или представители жилищно-эксплуатационной конторы пришли к вам без вызова, это повод насторожиться! Мошенники часто выдают себя за представителей сферы обслуживания. Проверьте его документы или спросите, в какой организации он работает. До того как открыть дверь незнакомцу, позвоните в названную им организацию и уточните, направляли ли оттуда к вам специалиста. Не стесняйтесь – это совершенно нормально!

Киберпреступники все чаще маскируют свой номер под официальные номера банков. Для начала проверьте, точно ли звонит сотрудник банка. Положите трубку, позвоните по официальному номеру банка и уточните, все ли в порядке с вашими счетом и картой. Даже если у вас на телефоне высветился знакомый номер банка, ни в коем случае не делайте на него обратный звонок. Наберите номер горячей линии банка вручную. Обычно преступник обращается к собеседнику по имени и отчеству, может назвать фамилию и даже номер и срок действия карты. Даже если информация звучит очень правдоподобно, лучше перестраховаться и позвонить в банк самому, чтобы общаться точно с его сотрудником, а не с преступником. Преступник представляется сотрудником банка и сообщает о подозрительной операции, которая требует немедленных действий со стороны клиента. Мошенники хорошо знакомы с психологией: говорят быстро и уверенно, используют профессиональные термины, нередко фоном включают звуки, имитирующие работу оживленного колл-центра. Все это помогает им втереться в доверие к клиенту банка и сделать так, что он потеряет бдительность. Например, обманщики говорят, что по карте проводится подозрительный платеж на крупную сумму и чтобы его остановить, нужно срочно сообщить данные карты, ПИН-код или одноразовый пароль из СМС-сообщения. Если человек колеблется или отказывается их назвать, ему угрожают, что деньги с его карты прямо сейчас уйдут к мошенникам. Если преступникам удается узнать нужную им информацию, они получают доступ к счету и снимают с него все деньги.

Как защитить свои деньги от мошенников? Если клиент сам сообщит преступникам секретную информацию, которую нельзя разглашать, вернуть деньги через банк не получится. Поэтому стоит придерживаться основных правил безопасности, чтобы не поддаться на уловки мошенников и не потерять деньги:

1.Всегда набирайте только официальный номер банка. Он указан на обратной стороне карты и на официальном сайте банка.

2.Не перезванивайте и не отправляйте СМС на незнакомые номера, не спешите переходить по ссылкам из сообщений «от банка». В любой непонятной ситуации звоните в банк по официальному номеру и уточняйте информацию у оператора.

3.Если вам звонят из банка, финансовой организации или госоргана, уточните ФИО и должность звонящего и скажите, что перезвоните ему сами. Положите трубку и перезвоните по официальному телефону организации или на горячую линию банка. Номер нужно набрать вручную.

4.Ни под каким предлогом никому не сообщайте личные данные, реквизиты карты и секретную информацию: CVC/CVV-код на обратной стороне карты, коды из СМС и ПИН-коды. Называть кодовое слово можно, только если вы сами звоните на горячую линию банка

ОЧЕНЬ ВАЖНО! Прежде чем принять любое решение, связанное со значительными расходами, обязательно посоветуйтесь с близкими!