ТЕЛЕФОННЫЕ МОШЕННИЧЕСТВА ПОДСТЕРЕГАЮТ ПОСТОЯННО

Мошенники превосходно освоили все возможности, которые предоставляют современные средства связи. По телефону вас могут обмануть через СМС-уведомления или звонок напрямую, а также при загрузке приложений, файлов.

Как правило, цель мошенников – заставить вас передать собственные средства «добровольно», так, чтобы вы не сразу догадались, что происходит на самом деле.

Мошенники очень хорошо знают психологию и людские слабости. Могут играть на чувствах жалости, страха, всегда торопят и навязывают свои условия в договоренностях. Они рассчитывают на вашу доверчивость, а иногда – на незнание особенностей дистанционных сделок. Часто они используют следующие мотивы:

- беспокойство за состояние своего счета в банке;
- беспокойство за близких и знакомых;
- желание выиграть деньги;
- желание оказать помощь;
- любопытство;

Чтобы противодействовать обману важно знать, какие схемы применяют жулики, не терять самообладания, изучить основы финансовой грамотности.

КАК СЕБЯ ОБЕЗОПАСИТЬ? ПРОСТЫЕ ПРАВИЛА

✓ Никогда не реагируйте на СМС-уведомления с незнакомых номеров;

✓ Помните, что если вам ошибочно перевели деньги, вы не обязаны предпринимать какие-либо шаги! Оператор (банк) вернет средства без вашего участия;

✓ Никогда не сообщайте по телефону данные о своей банковской карте и коды из СМС-уведомлений;

✓ С осторожностью относитесь к звонкам с незнакомых номеров. По возможности установите определитель региона входящих звонков (дистанционные мошенники звонят, как правило, из-за пределов республики);

✓ Изучите суть мобильных сервисов, позволяющих бесконтактно совершать финансовые операции, чтобы понимать, как именно злоумышленники могут вами манипулировать;

✓ Всегда при смене или утере телефона отключайте услугу мобильного информирования о состоянии вашего счета в банке;

✓ Тщательнее следите за тем, где и кому вы оставляете свои персональные данные (указываете Ф.И.О., мобильный номер и т.д.).

СХЕМА «ПОПАЛ В БЕДУ/ НЕПРИЯТНОСТИ»

Среди шума, помех или шепотом, сдавленным голосом к вам обращаются как к родственнику или приятелю, просят помочь деньгами. Иногда в трубке появляется второй голос, он называет имя, звание, должность (и вам становится ясно, что это якобы представитель силовой структуры), он сообщает о каком-либо несчастье, происшествии, пугает серьезными последствиями, предлагает урегулировать ситуацию за деньги.

✓ Не терять самообладания, при возможности прекратить разговор (как правило, мошенники больше не перезванивают)

✓ При невозможности оборвать общение задать уточняющий вопрос, но такой, чтобы настоящего вашего близкого он смутил явной ошибкой. Пример. Нельзя спрашивать «Ты ли это, Иван?», если у вас, действительно есть с таким именем внук, сын, муж, брат, приятель. А, к примеру, если у вас дочь и ее зовут Анна, переспросить «Сынок, Руслан, это ты?» и т.п. Чем дольше вы остаетесь в контакте, тем сильнее вас могут запутать / запугать / разжалобить и т.п.

СХЕМА «ПРОБЛЕМЫ С БАНКОВСКОЙ КАРТОЙ, СЧЁТОМ»

Вам сообщают от имени банковской организации о сбое в работе или попытке несанкционированного списания ваших средств с карты, счёта:

✓ Не паниковать, не верить злоумышленникам, даже если они пугают блокировкой счета;

✓ Не продолжать разговор; не отвечать на СМС.

✓ Обратиться в банк лично или через официальную горячую линию поддержки клиентов (указана на оборотной стороне карты);

Усвоить, что с картой и деньгами в момент тревожного сообщения все в порядке, вас просто пытаются заставить испугаться, ошибиться и назвать нужные мошенникам данные.

3 правила использования банковских карт:

- Не храните ПИН-код рядом с банковской картой;
- Храните втайне и никому не называйте сведения о карте (окончание срока действия, секретный код CVC2/CVV2, ПИН-код). Помните, что мошенник может, зная номер карты, похитить ваши деньги
- Храните телефонные номера службы поддержки клиентов банка и кодовое слово, зафиксированное в договоре, в надежном и, что важно, – в быстродоступном месте. В экстренном случае важно своевременно позвонить в банк и заблокировать карту.

3 правила использования мобильного телефона:

- При решении финансовых вопросов не верьте тому, что слышите, проверяйте информацию в разных источниках;
- Никому ни при каких обстоятельствах не сообщайте подтверждающие коды из СМС-уведомлений
- Помните, что при подключенной услуги удаленного управления счетами у вас в руках не просто мобильный телефон, а ключ от сейфа с вашими сбережениями.

3 правила для сохранности денег на счетах:

- Установите лимиты по удаленным операциям с вашими средствами;
- Чтобы полностью обезопасить себя при покупках в интернете, заведите для онлайн-оплат отдельную карту.
- Не бойтесь проявить недоверие или показаться невежливыми, если речь идет о ваших собственных сбережениях!

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ БАНКОВСКИХ КАРТ :

✓ Никогда и никому не сообщайте пин-код вашей карты!

✓ Ни при каких обстоятельствах и никому не называйте, не пересылайте цифровые пароли из смс-сообщений от банка.

✓ Никогда и никому не называйте три цифры на оборотной стороне банковской карты (cvc- или cvv-код)! Никто (даже сотрудники банка) не вправе требовать их.

✓ Никому не сообщайте парольную информацию для доступа в сервис интернет-банкинга.

✓ С осторожностью относитесь к предоставлению реквизитов своей банковской карты: не диктуйте их вслух, прикрывайте данные карты при использовании в общественных местах!

✓ При возникновении каких-либо подозрений в мошенничестве связывайтесь с клиентской поддержкой банка, номер телефона которой сохраните заранее.

✓ Оплачивайте покупки с использованием реквизитов банковской карты только в проверенных интернет-магазинах

✓ Оформите для сделок в интернете отдельную карту, на которой будет установлен лимит.

19.МВД.РФ

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ СООБЩИТЕ ОБ ЭТОМ В ПОЛИЦИЮ ПО ТЕЛЕФОНАМ:
02 (СО СТАЦИОНАРНЫХ ТЕЛЕФОНОВ),
102 (С МОБИЛЬНЫХ СРЕДСТВ СВЯЗИ),
ДЕЖУРНАЯ ЧАСТЬ ПОЛИЦИИ

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ ПО РЕСПУБЛИКЕ ХАКАСИЯ

ЗАЩИТИ СЕБЯ И СВОИХ БЛИЗКИХ ОТ МОШЕННИКОВ

ПАМЯТКА ДЛЯ ГРАЖДАН

СТОП МОШЕННИЧЕСТВО

ВНИМАНИЕ!