Как уберечь себя и близких от финансового мошенничества. Кибермошенничество.

Списание денег со счета без ведома владельца, кража паролей и ПИН-кодов, легкий заработок в интернете и вклады под невероятные проценты, онлайн-казино – все это виды финансового мошенничества. Преступники будут спекулировать на ваших чувствах, обещать золотые горы, маскироваться под сотрудников банков или государственные организации, чтобы выманить деньги. Как распознать мошенника и что делать, если вас все-таки удалось обмануть? Сегодня мы поговорим о кибермошенничестве.

Допустим, вы всегда снимаете деньги только в кассе банка, а картой и вовсе не расчитываетесь. Вы чувствуете себя в безопасности. Вдруг вам приходит СМС или письмо якобы от банка со ссылкой, просьбой перезвонить по неизвестному номеру или с уведомлением о неожиданном крупном выигрыше. Или звонят от имени банка и просят сообщить личные данные, ПИН-код от карты или номер СМС – подтверждения. Или пишут в социальных сетях от имени родственников или друзей, которые внезапно попали в беду (угодили в полицию, сбила машина, украли сумку) и просят перевести энную сумму денег на неизвестный счет. Вы имеете дело с мошенниками. За ссылками скорее всего таятся вирусы, на другом конце провода – специалисты по обману, которые всеми правдами и неправдами хотят выманить необходимые ими данные, а по ту сторону экрана – злоумышленники, которые играют на ваших желаниях, чувствах и заботе о близких.

Как не попасться

- Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках.

- Если вам приходит СМС о зачислении средств (и сообщение похожее на привычное уведомление банка), а затем звонит якобы растяпа, который по ошибке зачислил вам деньги и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС - не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.

- Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок опять же от рассеянного человеку, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас код, чтобы списать с вашего счета деньги или подписать вас на ненужный платный сервис.

- Никому не сообщайте персональные данные, а уж тем более пароли и коды. Сотрудникам банка они не нужны, а мошенникам откроют доступ к вашим деньгам.

- Не храните данные карт на компьютере и смартфоне.

- Проверяйте информацию. Если вам говорят, будто вы что-то выиграли или с вашей карты случайно списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты.

- Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.

- Установите на компьютер антивирус – и себе, и родственникам.

- Объясните пожилым родственникам и подросткам эти простые правила.

Что делать, если вас обманули?

- Позвоните в банк (номер всегда есть на обороте карты и на главной странице сайта банка), сообщите о мошеннической операции и заблокируйте карту.

- Обратитесь с заявлением в ОМВД России «Пожарский» или позвоните в отдел полиции Пожарского округа по телефону 8(42357) 33-0-30. Или обратитесь в отдел полиции той территории, на которой вы находитесь.

Пресс-служба ОМВД России «Пожарский»