Как не стать жертвой мошенников под предлогом оформления кредита либо получения прибыли на Интернет-бирже.

Злоумышленник с целью хищения кредита, представившись сотрудником службы безопасности, сообщает, что Вам оформлен кредит. Для того, чтобы проценты по одобренному кредиту не начислялись, необходимо оформить заявку на еще один кредит, чтобы погасить ранее взятый и перевести его на защищенный счет. **Не оформляйте никаких кредитов по просьбе неизвестных Вам лиц и не переводите денежные средства на якобы защищенные счета.**

Вам поступает телефонный звонок либо поступает в сети Интернет рекламный баннер с предложением заработать денежные средства на Интернет-бирже. Предлагают зарегистрироваться на биржевой платформе, куда необходимо внести начальный капитал. **Не регистрируйтесь на неизвестных биржевых платформах, не осуществляйте на них никаких сделок, не переводите никаких денежных средств.**

При пользовании банковскими картами:

Для предупреждения несанкционированных действий с использованием карты необходимо требовать проведения операций с ней только в Вашем присутствии, никогда не позволять уносить третьим лицам карту из поля Вашего зрения.

В случае обращения к Вам какого-либо лица лично, по телефону, в сети Интернет, через социальные сети или другим способом с целью узнать полные данные Вашей банковской карты: шестнадцатизначный номер, срок действия, трехзначный код проверки подлинности карты, расположенный на оборотной стороне на полосе для подписи держателя карты и т.д. (пароли или другая персональная информация), будьте осторожны – это явные мошенники. При любых сомнениях следует прекратить общение и обратиться в банк по телефону, указанному на обратной стороне банковской карты.

Во избежание использования карты другим лицом необходимо хранить ПИН-код отдельно от карты, не указывайте его на карте и не сообщайте другим лицам (в том числе родственникам).

Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие по SMS/MMS/электронной почте/мессенджерам (Viber, WhatsApp и др.), в том числе от имени банка. Помните, что банк не рассылает своим клиентам ссылки или указания подобным образом.

ПРОКУРАТУРА
КОСТРОМСКОЙ ОБЛАСТИ

ПРОКУРАТУРА
КОСТРОМСКОГО РАЙОНА

ПАМЯТКА

На предмет информирования о видах и способах мошенничеств и иных преступлений, совершенных с использованием информационно-коммуникационных технологий (средств связи, сети Интернет и др.), в целях недопущения их совершения в будущем

г. Кострома
2024

Как не стать жертвой «мобильного» мошенничества.

Злоумышленники могут обратиться к Вам:

- Путем рассылки SMS-сообщений о блокировке Вашей банковской карты, о переводе денежных средств за покупку товара по объявлению и последующему информированию о необходимости дальнейшего введения ряда команд с банкомата. Это мошенники! (Никому нельзя сообщать реквизиты своей банковской карты, в том числе сотруднику банка, об этом всегда информирует банк при получении пароля к карте. Впоследствии необходимо лично обратиться в ближайшее отделение банка для выяснения возникших проблем с банковской картой);
- Путем рассылки SMS-сообщений с неизвестных номеров о выигранном призе, с просьбой перевести деньги на телефон или вернуть деньги, т.к. они были переведены ошибочно. Это обман! (Человек не может выиграть приз, не участвуя в лотереях. Не отвечайте на такие сообщения, не переводите денежные средства);
- Под видом сотрудников полиции с информацией о нарушении близкими родственниками законов с целью передачи Вами денежных средств через посредников или перевода через терминалы оплаты для освобождения родственников от ответственности (административной либо уголовной). (В этой ситуации не продолжайте разговор, не позволяйте себя убедить. Вам звонит мошенник. Обратитесь в полицию!)

Как не стать жертвой мошенников в сети Интернет.

- Злоумышленник, с целью хищения Ваших денежных средств, размещает в сети Интернет объявление о продаже какого-либо объекта (телефон, машина, квартира и т.д.) по заниженной цене и оставляет свои контактные данные. После того, как Вы собираетесь приобрести товар, злоумышленник сообщает, что для покупки необходимо внести предоплату (на расчетный счет Яндекс-деньги, счет Веб-мани и т.д.).
- Наиболее часто встречающимися площадками для размещения подобных объявлений являются сайты социальных сетей «В контакте», «Одноклассники», также такими сайтами могут выступать ресурсы бесплатных объявлений «Авито», «Юла», «avto.ru». Злоумышленник объясняет внесение предоплаты тем, что живет в другом регионе и отправит товар сразу после того, как удостоверится в оплате товара. Злоумышленник может выслать копию паспорта (поддельную).
- Также распространенным способом мошенничества в сети Интернет является создание сайтов интернет-магазинов. Злоумышленник по электронной почте высылает договор, который заполняет заказчик, после чего просит внести предоплату за товар. **Не перечисляйте денежные средства за неполученные товары и услуги!**

Как не стать жертвой мошенничества с банковскими картами при использовании услуги «Мобильный банк».

В случае потери мобильного телефона с подключенной услугой «Мобильный банк» или мобильным приложением «Сбербанк Онлайн» следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в контактный центр банка для блокировки услуги «Мобильный банк» или «Сбербанк Онлайн».

При смене номера телефона, на который подключена услуга «Мобильный банк», необходимо обратиться в любой филиал (внутреннее структурное подразделение) для отключения услуги «Мобильный банк» от прежнего номера и подключения на новый.

Не следует оставлять свой телефон без присмотра, чтобы исключить несанкционированное использование мобильный банковских услуг другими лицами.

Не подключайте к услуге «Мобильный банк» абонентские номера, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников банка.