КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ: ОБЩИЕ РЕКОМЕНДАЦИИ

Для хищения денег у граждан злоумышленники используют изощренные сценарии обмана, которые регулярно совершенствуют. Схемы финансового мошенничества выглядят очень правдоподобно. Преступники обычно используют обсуждаемые новости или события, запугивают или, наоборот, обещают внезапную выгоду.

Банк России выявляет такие схемы и публикует их вместе с рекомендациями, **как защититься от мошенников:**

⛔ Не сообщайте никому и никогда паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код. Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте ее в социальных сетях, на форумах и каких-либо сайтах в Интернете, а также не храните данные карт и PIN-коды на компьютере или в смартфоне.

⛔ Если с неизвестного номера звонит сотрудник Центробанка, правоохранительных органов, государственной организации или банка с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет Центробанка и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку. Если подозреваете, что вам звонит мошенник, позвоните в банк по номеру телефона, указанному на обратной стороне карты или на его сайте, или в контакт-центр ведомства, сотрудником которого представлялся звонящий.

⛔ Не совершайте каких-либо действий по счету, если вам звонят из Центробанка с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет, или с предложением об оформлении кредита. Банк России не открывает счета и не работает с гражданами.

⛔ По возможности установите антивирус на все устройства и обновляйте его.

⛔ Совершайте покупки в Интернете только на проверенных сайтах. Заведите специальную карту для онлайн-покупок и пополняйте ее ровно на ту сумму, которая нужна для оплаты. При совершении покупок обращайте внимание на наличие в строке браузера рядом с названием сайта значка безопасного соединения (замочка).

⛔ Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, получить какую-либо выплату и тому подобное. Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

Первоисточник https://cbr.ru/information_security/pmp/