**Специальный раздел о мошеннических схемах на сайте Банка России**

Сегодня тысячи людей теряют свои деньги от действий злоумышленников, которые используют все более изощренные сценарии обмана для дистанционного хищения денежных средств. Мошенники оказывают психологическое воздействие на человека по телефону, вынуждают раскрыть личные или финансовые данные (например, данные счета или банковской карты) или перевести им деньги. Зачастую аферистам удается убедить свою жертву взять кредит для последующей передачи средств в чужие руки.

Они также могут направлять электронные письма и сообщения со ссылкой на поддельные (фишинговые) сайты как финансовых, так и любых других организаций, компаний или интернет-магазинов, где легко можно потерять свои деньги. Схемы мошенников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события.

Для противодействия мошенническим практикам на сайте Банка России создан специальный раздел, посвященный наиболее распространенным схемам, которые используют кибермошенники для кражи денег у граждан. В разделе не только представлено описание самих схем, но и даны рекомендации о том, как противостоять злоумышленникам в той или иной ситуации.

– Предупрежден – значит вооружен! Эти знания помогут в нужную минуту принять правильное решение и не стать жертвой обмана. Информация о новых мошеннических схемах, а также рекомендации по защите от них будут регулярно дополняться, – отмечают эксперты по безопасности регионального отделения Банка России.

***Ссылка на раздел на сайте Банка России:*** *http://www.cbr.ru/information_security/pmp/*

Помните, если по телефону (как правило, с подменой номера) неизвестные вам люди представляются сотрудниками банка или других организаций, говорят о деньгах, пытаются вывести вас из спокойного состояния – запугивают, торопят и оказывают давление – вы общаетесь с мошенниками. Такое психологическое воздействие представляет собой методы социальной инженерии. Просто прервите разговор и положите трубку.

Самостоятельно позвоните в свой банк по телефону, указанному на обратной стороне карты или на официальном сайте банка и убедитесь в сохранности ваших средств. Вы так же можете сообщить обо всех подозрительных звонках на горячую линию вашей кредитной организации, в ее онлайн-чат или на круглосуточную горячую линию Банка России – 8-800-300-30-00.

Если вы стали жертвой кибермошенников:

- Немедленно заблокируйте карту через мобильное приложение или сайт банка.
- Напишите заявление о несогласии с операцией в течение суток после получения сообщения о списании средств.
- Обратитесь с заявлением о хищении денег в любое отделение полиции.

Если человек самостоятельно перевел деньги мошенникам или предоставил им банковские данные, то банк не обязан возвращать похищенную сумму.

*Источник: пресс-служба Отделения Уральского ГУ Банка России по Пермскому краю*