**Вор в мобильнике**

***СМС-сообщениями «Мама, срочно положи 50000 на карту … Мне не звони, потом все объясню» или «Вы победили в конкурсе и выиграли денежный приз! Срочно перезвоните по номеру …» уже никого не удивить. Все знают – их используют мошенники для обмана доверчивых граждан.***

Но жажда быстро и незаконно нажиться заставляет преступников придумывать новые способы получения персональных данных для снятия средств. Например, часто на удочку злоумышленников попадают люди, устанавливающие на смартфон различные приложения для работы с банковскими картами, разработчик которых неизвестен.

По предложенному функционалу в таком приложении все отлично: мошенники предлагают удобную программу для управления банковскими картами различных банков с помощью всего одного приложения или сервис перевода денежных средств с одной карты на другую без комиссии. Как правило, в этих программах использованы логотипы известных банков, их реквизиты и схожий интерфейс. Пользователю остается только ввести логины и пароли от онлайн-кабинетов банков и… попрощаться со своими сбережениями.

«Чтобы не быть обманутыми, устанавливайте приложения только по ссылке с официального сайта банка. Перед скачиванием приложения внимательно изучите его название и содержание, чтобы убедиться, что это не сайт-двойник», - советует управляющий Отделением по Курской области ГУ Банка России по Центральному федеральному округу Евгений Овсянников.

«Если вы все же попались на уловку мошенников, незамедлительно звоните в банк, выпустивший карту, по номеру телефона, который можно найти на обороте карты, на официальном сайте банка и в договоре о выпуске и обслуживании карты. Сообщите о мошеннической операции и заблокируйте карту. Кроме того, срочно обратитесь в правоохранительные органы с заявлением о хищении. Это поможет расследовать схожие преступления и, возможно, предотвратит их в дальнейшем», - добавляет Евгений Овсянников.