**Осторожно! Телефонное мошенничество!**

Сотрудники полиции призывают держателей банковских карт быть бдительными: Имеются ряд способов списания денежных средств с банковских счетов владельцев:

-   хищение денежных средств с банковской карты через вирусное программное обеспечение, заражающее как персональный компьютер, так и мобильное устройство клиента. При попытке клиента открыть «зараженное» вирусом сообщение, произошла установка мобильного приложения, после чего, вирусная программа самостоятельно от имени клиента получала и пересылала злоумышленникам SMS-пароли для входа и подтверждения мошеннических операций в Сбербанк Онлайн.

-«Услуга «Мобильный банк», позволяющая по телефону управлять денежными средствами, находящимися на банковском счету, при невнимательности владельца карты может привести к снятию денег мошенниками» кроме этого, неиспользуемый номер телефона может быть перепродан и новый владелец через «мобильный банк» получит доступ к вашей банковской карте. Если он «не чист на руку», получив SMS-уведомление на полученный номер, имеет возможность воспользоваться этим в корыстных целях.

- Снятие денег с карты может произойти и в случае, если Вы потеряли телефон или у вас его украли – подобные заявления об исчезновении денег со счетов ООО «Сбербанк России», к которым «привязана» сим-карта телефона, в полицию поступают довольно часто.

-«Для защиты от данного вида мошенничества достаточно соблюдать несколько простых правил»:

 -Не устанавливайте на мобильный телефон, устройство, на которые Банк отправляет SMS-сообщения с подтверждающим одноразовым паролем, приложения, полученные от неизвестных вам источников. Помните, что банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS, MMS, Email-сообщения;

-Важно знать, что банк никогда не запрашивает пароли для отмены операций. Если Вам предлагается ввести пароль для отмены операции, то прекратите сеанс использования услуги и срочно обратитесь в банк;

-Для входа в личный кабинет требуется только идентификатор и пароль. В случае если от Вас требуют любую другую персональную информацию, то прекратите сеанс использования услуги и срочно обратитесь в Банк;

-Вводить одноразовые пароли следует только в том случае, если операция инициирована Вами. При получении SMS с одноразовым паролем внимательно ознакомьтесь с его содержанием. Вводить пароль в систему следует, только если реквизиты Вашей операции соответствуют реквизитам в полученном SMS-сообщении;

- Проверяйте, что установлено защищенное SSL-соединение с официальными сайтами услуги. При любых подозрениях на компрометацию паролей посторонними лицами или запросах на выполнение неинициированных Вами операций, следует незамедлительно обратиться в службу помощи Банка.