***Уважаемые получатели социальный услуг!***
***Специалисты КГБУ СО «КЦСОН «Пировский» предлагают вашему вниманию очередное занятие по финансовой грамотности на тему «Сбербанк предупреждает о мошенничестве. Специфика схемы преступления «судебных приставов»***

Вредоносные сообщения мобильной связи нередко атакуют мобильные номера с расчетом на доверчивость абонентов. Злоумышленники маскируются под федеральную службу судебных приставов и, запугивая пользователей несуществующими долгами, опустошают банковские счета и крадут пароли. О том, как не стать жертвой мошенников, а заодно и обезопасить кровно заработанные средства мы с вами сегодня и поговорим.

В 2018 году случаи такого мошенничества с приставами наблюдаются реже, но по-прежнему существуют. В то время как представители Сбербанка предпочитают воздержаться от оценки происходящего, сотрудники ФССП сообщают, что не практикуют уведомление граждан о задолженности посредством СМС, а подобные оповещения однозначно дело рук злоумышленников. Мошенничество с использованием электронных средств платежа - один из самых массовых видов правонарушений. Специфика схемы нацелена в первую очередь на то, чтобы вникнуть в доверие владельца устройства. Оценивая маржинальность (займы, кредиты) аферы, мошенники усложняют схему взаимодействия с жертвой, стараясь сделать ее более совершенной и неприметной. Во многом, поэтому важно понимать принцип ее действия, который заключается в следующем: Абоненту приходит СМС-оповещение, замаскированное под домен ФССП, с информацией о якобы непогашенной задолженности и предложением перейти по указанной ссылке для уточнения обстоятельств. После перехода по ссылке пользователя «выбрасывает» на рабочий стол, а устройство перезагружается. В процессе перезагрузки в операционную систему смартфона внедряется вредоносное программное обеспечение, считывая пароли и личные данные жертвы, а баланс на счете, привязанном к онлайн-банку, становится отрицательным. При включении устройства доступ к приложениям некоторое время ограничен, но затем работа официального сайта возобновляется. По альтернативной схеме телефон не перезагружается, а пользователя направляют на копию официального сайта ФССП - в это время вирус делает свою работу. В некоторых случаях абонента просят авторизоваться в системе, чтобы получить информацию о задолженности.

**Могут ли деньги списаться с карты автоматически при открытии сообщения или нужно именно кликать на ссылку?**

Учитывая многочисленные призывы пострадавших не открывать СМС-сообщения, присланные мошенниками, может показаться, что этого будет достаточно для заражения устройства вредоносной программой. Однако с технической точки зрения это редко удается реализовать, так как вирус не может внедрится в операционную систему без предварительного скачивания. К тому же, по словам абонентов, ставших жертвами цифрового обмана, обнуление счета происходило после перехода по ссылке, а не в момент открытия сообщения. Ничто не может гарантировать безопасность лучше, чем скептически настроенный пользователь в отношении ссылок с неизвестным содержанием.

**Какие мошеннические схемы с банковскими картами существуют и что делать, если деньги все-таки были украдены?**
**Куда обратиться, если избежать обмана не удалось?**

Чтобы добиться справедливости, стоит придерживаться следующего плана действий: Заморозить (заблокировать) счет, обратившись в местное отделение банка, воспользовавшись услугами онлайн-банка, либо связавшись с сотрудниками по телефону. Обратиться в банк и написать заявление, сообщив о несогласованном снятии средств со счета (составляется в 2-х экземплярах, где один из них остается у заявителя с отметкой о принятии). С экземпляром заявления обратиться в местное отделение полиции, зафиксировав акт хищения средств. Действовать следует незамедлительно и обратиться в указанные учреждения не позднее 3-х суток с момента кражи. Ввиду того, что методы мошенников могут разниться, не всегда удается выяснить, каким именно образом были списаны деньги. В случаях, когда речь идет о заражении системы вирусом, банк в праве сослаться на то, что устройство не было оснащено необходимыми средствами защиты и отказать в возврате. Если клиент ввел свои данные на поддельном сайте, то это может расцениваться как нарушение правил пользования. В этом и заключаются трудности, но вероятность возврата средств все-таки существует. Полиции не всегда удается установить личность преступников, так как последние используют различные методы шифрования адресов, стремясь сохранить анонимность. Лучшим гарантом сохранности личных сбережений является бдительность их владельца. Не стоит доверять информации из подозрительных источников, а лучше - оперативно проверять. Удостовериться либо опровергнуть наличие задолженности можно на официальном сайте ФССП. Ни в коем случае не нужно переходить по неизвестным ссылкам, а устройство следует защищать лицензионным антивирусом.

**<u>Основные меры безопасности:</u> не сообщать никому, даже сотрудникам банка, подтверждающие пароли, ПИН- и CVV-коды банковских карт, использовать официальные мобильные приложения и антивирусы для ваших устройств, не переходить по ссылкам на незнакомые ресурсы. Важно также, что Сбербанк отправляет СМС только с номера 900.**
Только в этом случае можно быть уверенным в том, что личные сбережения не перейдут в руки мошенников.


# СБЕРБАНК ПРЕДУПРЕЖДАЕТ О МОШЕННИЧЕСТВЕ