Мошенничество через интернет-сайт «Авито».

В ОП «Юрюзанское» ОМВД России по Катав-Ивановскому району обратился житель города Юрюзань, сообщив, что неизвестное лицо, похитило со счета принадлежащему ему банковской карты денежные средства в размере 19 000 рублей.

В ходе проведения проверки установлено, что данный гражданин 29.08.2020 года выставил на продажу на сайте Авито свой сотовый телефон марки «Xiaomi Redmi Note 7» за сумму 9 500 рублей. 30.08.2020 данным телефоном заинтересовалось неизвестное лицо, которое написало с номера 8-963-029-**** на сотовый номер 8 -982-******* через приложение «ВотсАп». В ходе переписки покупатель поинтересовался, может ли потерпевший отправить данный сотовый телефон через доставку «Авито», на что потерпевший согласился. Далее в ходе переписки, покупатель с номера 8-963****** присылал в приложении «ВотсАп» инструкцию и ссылку, по которой нужно пройти, чтобы он забрал свои денежные средства за телефон перед отправкой. Покупатель пояснил, что через данный сайт уже деньги списались с его счета и потерпевший пройдя по данной ссылки, может забрать себе денежные средства в размере 9 500 рублей. Далее потерпевший пробовал зайти на сайт по данной ссылки, но у него высвечивалась ошибка при входе на данный сайт. Затем он решил позвонить оператору «Сбербанк» и поинтересоваться. Почему он не может забрать денежные средства за товар, так как он осуществлял все действия через свою карту ПАО «Сбербанк». Оператор «Сбербанка» пояснила, чтобы забрать денежные средства с сайта ему необходимо пополнить счёт своей банковской карты на такую же сумму, а то и немного больше, то есть не мене 9 500 рублей. 03.09.2020 он пополнил счёт своей банковской карты на сумму 6000 и 5000 рублей, затем перешёл по ссылке, которую отправлял ему покупатель. Пройдя по данной ссылке, потерпевший ввел все данные своей банковской карты ПАО «Сбербанк» и у него произошло денежное списание в размере 9 500 рублей, о данном факте потерпевший сообщил покупателю, на что последний написал ему ещё одну ссылку сайта «Помощи». Перейдя на данный сайт, потерпевший общался в чате с оператором, который пояснил, что ему вновь необходимо пополнить счёт своей банковской карты на сумму 9 500 рублей и повторить операцию. Затем потерпевший пополнил счёт своей банковской карты на сумму 10 000 рублей и повторил вышеуказанную операцию, в результате чего с его счёта повторно списались денежные средства в размере 9 500 рублей. Так, неустановленное лицо, путём обмана похитило денежные средства со счета банковской карты ПАО «Сбербанк» потерпевшего на общую сумму 19 000 рублей.

В настоящий момент в указанном материале проверки усматриваются признаки преступления предусмотренные ч.2 с.159 УК РФ.

Сотрудники полиции ОМВД России по Катав-Ивановскому району в очередной раз напоминают гражданам о мере безопасности при использовании мобильного приложения. Использовать только официальные приложения банка, доступных только на официальных сайтах, установить на телефон антивирусную программу и своевременно её обновлять. При установки новой программы для андроид, всегда обращайте внимание на разрешение, которые требует программа для своей работы, особенно на возможность доступа к смс сообщениям, возможность доступа к SMS- сообщениям. Если разрешения вызывают подозрения или явно не соответствуют функционалу программы, лучше отказаться от ее использования. Своевременно устанавливать обновления операционной системы. Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS MMS Email - сообщения. Установить парольную защиту на телефоне-смартфоне. Данная возможность доступна для любых современных моделей телефонов. Не использовать мобильный телефон для доступа к полнофункциональной версии интернет-банка, для этого существуют специализированные приложения, разработанные Банком. Завершать работу с мобильным приложением через завершение сессии (кнопка «Выход»).

Мошенничество!!!!!

В ОП «Юрюзанское» ОМВД России по Катав-Ивановскому району обратилась жительница города Юрюзань, сообщившая, что неизвестное лицо, похитило со счета принадлежащей ей банковской карты денежные средства в размере 8 997 рублей.

В ходе до следственной проверки было установлено, что потерпевшая выполнила последнее пополнение на счёт своей карты рассрочки «Халва», после чего счёт его карты-рассрочки составил 30 000 рублей. В вечернее время 02.09.2020 года, на сотовый телефон потерпевшей поступил звонок с номера +74954******, звонил молодой человек, который представился как сотрудником службы безопасности. Он пояснил потерпевшей, что по её счёту банковской карты в данный момент происходят мошеннические действия, по какой именно карте, он не уточнил. В ходе разговора потерпевшая пояснила ему, что у нее карта ПАО «Сбербанк» на которой всего 700 рублей, и во время разговора по телефону с ним, потерпевшая увидела, что все приложения на её сотовом телефоне начали меняться местами. Он пояснил, что это работает их «робот», который устраняет мошеннические действия, которые по его словам происходят в данное время с счетами потерпевшей так вовремя не длительного разговора со счета банковской карты-рассрочки «Халва» у потерпевшей списались денежные средства общей суммой в 8997 рублей, разговор с ним закончился во время списания.

Так, неустановленное лицо, путём обмана похитило денежные средства со счета потерпевшей на общую сумму 8 997 рублей.

В настоящий момент в указанном материале проверки усматриваются признаки преступления предусмотренные п «г» ч.3 с.158 УК РФ.

Сотрудники полиции ОМВД России по Катав-Ивановскому району в очередной раз напоминают гражданам о мере безопасности при использовании мобильного приложения. Использовать только официальные приложения банка, доступных только на официальных сайтах, установить на телефон антивирусную программу и своевременно её обновлять. При установки новой программы для андроид, всегда обращайте внимание на разрешение, которые требует программа для своей работы, особенно на возможность доступа к смс сообщениям, возможность доступа к SMS- сообщениям. Если разрешения вызывают подозрения или явно не соответствуют функционалу программы, лучше отказаться от ее использования. Своевременно устанавливать обновления операционной системы. Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS MMS Email - сообщения. Установить парольную защиту на телефоне-смартфоне. Данная возможность доступна для любых современных моделей телефонов. Не использовать мобильный телефон для доступа к полнофункциональной версии интернет-банка, для этого существуют специализированные приложения, разработанные Банком. Завершать работу с мобильным приложением через завершение сессии (кнопка «Выход»).