ГУ МВД России по Красноярскому краю предупреждает об участившихся случаев мошенничества, совершаемых в сети Интернет, с помощью средств сотовой связи, а также при использовании банковских карт.

В последнее время наблюдается рост числа случаев мошенничества, совершаемых в сети Интернет, с помощью средств сотовой связи, а также при использовании банковских карт. ГУ МВД России по Красноярскому краю рекомендует следовать правилам безопасности:

- **НИКОМУ И НИКОГДА НЕ СООБЩАТЬ ПИН-КОД КАРТЫ.** Постарайтесь его запомнить. Не храните ПИН-код рядом с банковской картой, в том числе в кошельке. Также не следует указывать ПИН-код на самой банковской карте. Если Вы не можете запомнить ПИН-код, то попросите сотрудника банка его изменить на другой, который Вы сможете с легкостью вспомнить в любой ситуации. Помните: хранение реквизитов банковской карты и ПИН-кода в тайне – это Ваша ответственность.
- **НИКОМУ И НИКОГДА НЕ СООБЩАЙТЕ РЕКВИЗИТЫ СВОЕЙ БАНКОВСКОЙ КАРТЫ.** Если на номер Вашего телефона пришло СМС-сообщение с уведомлением о том, что Ваша карта заблокирована, сверьте номер телефона отправителя с официальным номером банка, предназначенным для информирования. Официальные номера банка обычно указаны на самой банковской карте, а также на официальном сайте банка. Если номера не идентичны, то ни в коем случае не отвечайте на сообщение. Если Вам позвонили с незнакомого номера и в ходе телефонного разговора представились сотрудником банка (Пенсионного фонда РФ и т.п.), просят под разным предлогом (например, для получения кредита, уменьшения процентной ставки по кредиту, перечисления бонусов за пользование банковской карты, зачисления премии, надбавки к пенсии от Пенсионного фонда Российской Федерации и т.п.) сообщить реквизиты банковской карты, CVV(CVC)-код (указан на оборотной стороне банковской карты, состоит из трёх цифр), паспортные данные, а также назвать пароль, отправленный Вам на ваш номер телефона, ни в коем случае не сообщайте ничего из вышеперечисленного, скорее всего кто-то пытается ввести Вас в заблуждение и похитить Ваши денежные средства. Если Вы хотите убедиться, что Ваши сбережения в целости и сохранности, прекратите разговор и позвоните в службу поддержки банка.
- **НИКОГДА НЕ ОСУЩЕСТВЛЯЙТЕ ПЕРЕВОД ДЕНЕЖНЫХ СРЕДСТВ ПОД КАКИМ-ЛИБО ПРЕДЛОГОМ.** Если, например, в ходе телефонного разговора неизвестное лицо просит Вас осуществить перевод денежных средств через банкомат в счет взноса для каких-либо целей (первоначальный взнос для снижения процента по кредиту, получение компенсации за приобретенные Вами ранее некачественные товары, снятие порчи/сглаза и т.п.), ни в коем случае не осуществляйте требуемые действия! Таким образом мошенник с вашей помощью осуществляет хищение Ваших денежных средств.
- **НЕ ПЕРЕДАВАЙТЕ КАРТУ ДРУГИМ ЛИЦАМ - ВСЕ ОПЕРАЦИИ С КАРТОЙ ДОЛЖНЫ ПРОВОДИТЬСЯ НА ВАШИХ ГЛАЗАХ.** В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.
- **НИКОГДА НЕ ПЕРЕХОДИТЕ ПО ИНТЕРНЕТ-ССЫЛКАМ, УКАЗАННЫМ В ПОДОЗРИТЕЛЬНОМ ПИСЬМЕ.** Если Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами (выиграли приз, необходимы для разблокировки банковской карты и т.п.), не спешите переходить по указанным в письме Интернет-ссылкам, поскольку они могут вести на сайты-двойники, созданные мошенниками для обмана добропорядочных граждан.
- **НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ В СЛУЧАЕ ЕЕ УТЕРИ**. Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.
- **ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ**. При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

- **БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ».** Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.
- **ОПАСАЙТЕСЬ ПОСТОРОННИХ.** Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом. Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.
- **СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ.** Никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой. Свяжитесь с Вашим банком - он обязан предоставить консультацию по работе с картой.
- **СВОЕВРЕМЕННО ПРИНИМАЙТЕ МЕРЫ ПО ОТКЛЮЧЕНИЮ УСЛУГИ «МОБИЛЬНЫЙ БАНК» И ИНЫХ СЕРВИСОВ.** При прекращении использования абонентского номера необходимо отключить его от электронных сервисов (Интернет-банк, мобильный банк, платежные системы, социальные сети, почтовые сервисы и др.).
- **ИСПОЛЬЗУЙТЕ ПРОВЕРЕННЫЕ ИСТОЧНИКИ ДЛЯ УСТАНОВКИ ПРОГРАММ-МОБИЛЬНЫХ ПРИЛОЖЕНИЙ.** Кроме того, для предотвращения незаконного доступа мошенников к Вашим данным установите современное лицензионное антивирусное программное обеспечение. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.
- **НИКОГДА НЕ ПЕРЕВОДИТЕ ДЕНЬГИ В СЧЁТ ВЫКУПА.** Если Вам позвонил неизвестный (чаще всего в ночное время), представляется сотрудником правоохранительного органа, требует выкуп или взятку за освобождение Вашего знакомого или родственника, немедленно прекратите разговор и сразу же перезвоните на мобильный телефон Вашему другу или родственнику, который стал «героем» истории. Если его телефон окажется вне зоны доступа сети, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации. Поступайте аналогичным образом, если Вам пришло **SMS-сообщение с просьбой о помощи**/требованием перевести определённую сумму на указанный номер. Обычно мошенники используют обращение «мама», «друг», «сынок» и т.п.
- **ПРОЯВЛЯЙТЕ БДИТЕЛЬНОСТЬ ПРИ ПОСТУПЛЕНИИ ИНФОРМАЦИИ О ВЫИГРЫШЕ.** Оформление выигрыша никогда не происходит только по телефону или Интернету. Если Вас не просят приехать в офис организатора акции с документами – это мошенничество.
- **В СЛУЧАЕ ПОСТУПЛЕНИЯ ИНФОРМАЦИИ ОБ ИЗМЕНЕНИИ ТАРИФНЫХ УСЛОВИЙ УСЛУГ МОБИЛЬНОЙ СВЯЗИ, ВСЕГДА СОВЕРШАЙТЕ ЗВОНКИ НА ОФИЦИАЛЬНЫЙ НОМЕР ОПЕРАТОРА СВЯЗИ.** Если в СМС-сообщении Вам угрожают штрафными санкциями и отключением номера якобы за нарушение договора с оператором Вашей мобильной связи, не ленитесь перезванивать своему мобильному оператору для уточнения правил акции, новых тарифов и условий разблокирования якобы заблокированного номера.
- **ПРОЯВЛЯЙТЕ БДИТЕЛЬНОСТЬ ПРИ ОБЩЕНИИ В СОЦИАЛЬНЫХ СЕТЯХ.** Нередко мошенники отправляют сообщения в социальных сетях с просьбой перевести денежные средства или сообщить реквизиты банковской карты под разными предлогами. Прочитав сообщение с подобным содержанием необходимо позвонить лицу, от чьего имени оно отправлено и поинтересоваться действительно ли именно он Вам написал. Если оказалось, что личную страницу Вашего знакомого «взломали» недоброжелатели, то предложите ему сообщить о случившемся своим друзьям и знакомым, в целях пресечения умысла мошенников заполучить денежные средства. Если Вы не имеете возможности позвонить, то задайте своему собеседнику вопрос в текстовом сообщении, ответ на который знаете только Вы двое. Кроме того, следует обратить внимание на стиль изложения текста в сообщении, характерен ли он для вашего собеседника.

Полиция обращает Ваше внимание о необходимости проявлять бдительность, поделиться предложенными советами со своими родными и знакомыми. Если Вы стали жертвой мошенников или в отношении Вас была совершена такая попытка – незамедлительно обратитесь в полицию!

ГУ МВД России по Красноярскому краю