Приложение

**ВНИМАНИЕ, МОШЕННИКИ!**

**ОМВД России по г. Салехарду информирует жителей об участившихся случаях мошенничеств**

**Наиболее распространенные способы совершения мошенничеств:**

1. **Покупки товаров и услуг в интернет-магазинах**

Преступники размещают в интернете заведомо ложную информацию на сайтах-двойниках о продаже товаров и услуг. После оплаты лжемагазины прекращают свою деятельность. **( Прежде чем совершить покупку на каком-либо интернет-магазине, предварительно тщательно и подробно ознакомьтесь отзывами о данном магазине. Осуществляйте заказ товаров на проверенных интернет-магазинах)**

**!!!Перед оформлением доставки товара услугами «Почты России» попросите продавца оформить, перед отправкой товара, опись наложенного имущества в почтовом отправлении. Таким образом, при получении товара в отделении «Почты России» вы сможете убедиться в содержимом почтового отправления!!!**

1. **«Покупки товаров на различных интернет-магазинах»**

**2.1.**Преступники звонят, по объявлениям, размещенных на интернет сайтах «Авито», «Юла» и т.д., соглашаются на покупку товара и просят продиктовать номер банковской карты, а также приходящие по СМС пароли, под предлогом перевода предоплаты или полной стоимости товара. На самом деле преступники дистанционно подключают к Вашей карте услугу «Сбербанк-онлайн» и похищают все денежные средства, хранящиеся на счетах. **(Не называйте свои конфиденциальные, банковские данные неизвестным лицам, не доверяйте предложению о внесении предоплаты. Совершайте сделки лишь после того как лично убедитесь в личности звонящего Вам человека)**

**2.2.** С целью ввода в заблуждение и обмана, злоумышленник предлагает осуществить покупку через раздел «Безопасная сделка» и отправляет ссылку на запрограммированный веб-сайт. При осуществлении покупки через такой веб-адрес, злоумышленник получит доступ к Вашим банковским данным. **(Осуществляйте сделки только убедившись в личности продавца. Не переходите по ссылкам и веб-адресам отправленным Вам неизвестным продавцом)**

1. **«Телефонные мошенники»**

**3.1** На телефон с неизвестного номера приходит СМС «Ваша карта заблокирована, перезвоните по телефону 8-800-………», далее преступники также предлагают подойти к банкомату и набрать комбинацию цифр или продиктовать номер карты и приходящие СМС-пароли, после чего подключают услугу «Сбербанк-онлайн» и похищают все денежные средства, хранящиеся на счетах. **(Сотрудники банков не осуществляют звонки своим клиентам. При сомнительных СМС-уведомлениях о блокировке Вашей банковской карты, обращайтесь в ближайшее отделение банка, либо же свяжитесь по номеру на оборотной стороне Вашей банковской карты)**

**3.2** На телефон с неизвестного номера приходит СМС с предложением пройти по ссылке «vk/3564///cjv». Зайдя на указанную в СМС страницу, на телефон автоматически устанавливается вредоносная программа(ВИРУС), впоследствии данные, хранящиеся на телефоне (в том числе пароли) становятся известными преступникам. **(Не переходите по неизвестным Вам ссылкам и веб-адресам. Не просматривайте и не открывайте данные СМС-сообщения, не устанавливайте какие-либо неизвестные Вам программы на Ваш мобильный телефон и ноутбук)**

**3.3** На телефон с различных абонентских номеров поступают звонки, злоумышленник представляется сотрудником банка и предлагает перевести бонусы «Спасибо от Сбербанка» на счет банковской карты в денежном эквиваленте, для чего ему необходимо знать номер банковской карты, имя владельца карты и СМС-пароли, после чего с банковской карты потерпевшего происходит списание денежных средств. **(Сотрудники банка не предлагают своим клиентам обменять накопившиеся бонусы «Спасибо» на денежный эквивалент и не спрашивают у своих клиентов банковские данные. Обменять накопившиеся бонусы «Спасибо» вы можете лишь сами через приложение «Сбербанк Онлайн».)**

**3.4** На телефон с различных абонентских номеров, в том числе и со стационарных (8-495-\*\*\*, 8-499-\*\*\*), поступают звонки, далее мошенник представляется сотрудником службы безопасности банка и поясняет, что с банковской карты неизвестные лица пытаются снять денежные средства и чтобы предотвратить данные операции, необходимо назвать все данные банковской карты, а также сообщить СМС-пароли поступающие на мобильный телефон от услуги «Мобильный банк», при этом мошенники могут называть имя и отчество владельца карты, а также последние цифры банковской карты. **(Обратитесь лично в ближайшее отделение Вашего банка и уточните всю информацию об операциях по вашей банковской карте. Не называйте свои банковские данные по телефону)**

**3.5.**На телефон поступают звонки от неизвестных лиц, которые, используя подмену абонентских номеров, представляются действующими сотрудниками органов исполнительной власти (МВД, ФССП и тд.) и под различными предлогами просят осуществить перевод денежных средств. **(Обратитесь в ближайший орган исполнительной власти и уточните информацию о сотруднике, который Вам звонил. Внимательно сверяйте номера территориальных органов исполнительной власти и номера, с которых Вам поступают абонентские звонки. Не называйте какие-либо свои банковские данные неизвестным Вам лицам. Не осуществляйте каких-либо денежных переводов в ходе телефонного разговора)**

**4. «Заработок на биржевой торговле и акциях крупных компаний»**

**4.1.**В сети Интернет и социальных сетях появляются различные объявления о денежных вложениях в биржевую торговлю с высоким процентом заработка при минимальных рисках. Под предлогом заработка злоумышленники предлагают оставить свои банковские реквизиты и тем самым осуществить перевод денежных средств на различные лицевые счета с целью пополнения брокерского счета. Дальнейший вывод денежных средств оказывается невозможен. **(Не переходите по неизвестным ссылкам и не оставляйте в сети Интернет свои банковские реквизиты. Не соглашайтесь на предложения неизвестных лиц о быстром и высоком заработке. Ни одна биржа Вам не гарантирует высокий заработок при минимальных рисках.)**

**4.2.** На телефоныпоступают СМС-сообщения от неизвестных номеров с предложениями о покупке акций банков и крупных компаний, после чего направляется ссылка переходя по которой открывается лже-сайт компании. После перевода денежных средств на лицевые счета, лже-сайт компании оказывается недоступен. **(Не осуществляйте покупки акций и ценных бумаг на сомнительных сайтах. Осуществить покупку акций можно лишь на официальных сайтах компании или же в отделении банка. Не осуществляйте переводы на неизвестные Вам банковские счета)**

**5. «Денежные переводы и сборы в социальных сетях»**

**5.1.** В социальных сетях поступают СМС сообщения от близких и знакомых с просьбой о займе денежных средств, после чего высылается номер банковской карты или номер телефона на который необходимо перевести денежные средства. После перевода денежных средств, личная страница знакомого лица оказывается недоступна или заблокирована. **(Перед переводом денежных средств своему знакомому, убедитесь в его личности. Не поддавайтесь уговорам и мнимым ситуациям.)**

**5.2.** В социальных сетях на странице знакомого человека появляется объявление о сборе денежных средств на лечение, в котором указаны банковские реквизиты, на которые можно осуществить денежный перевод. После перевода денежных средств на указанные в сообщении банковские реквизиты, страница знакомого оказывается недоступной. **(Не осуществляйте переводы по мнимым объявлениям в социальных сетях. Убедитесь в достоверности размещенного объявления. Свяжитесь со знакомыми и уточните всю информацию)**

**6. «Покупки билетов и путевок в санатории»**

**6.1.** В сети Интернет размещаются преступные дубликаты оригинальных сайтов по продаже авиа и жд/билетов, в том числе путевок. При переходе на указанные лже-сайты и оформлении мнимой сделки по продаже авиабилетов, предлагается осуществить ввод своих банковских реквизитов и конфиденциальных паролей для доступа к транзакциям, после чего с банковской карты происходит хищение денежных средств. **(Перед покупкой билетов и путевок, убедитесь в достоверности просматриваемого сайта. Внимательно сравните название сайта с оригинальным. Злоумышленники могут изменить один символ в названии сайта. Пользуйтесь проверенными ссылками)**