|  |
| --- |
| **http://post.mvd.ru/Session/36860-5LrH7m4BipoRiSJ0K1q1-kmbdubw/MIME/INBOX-MM-1/805-02-B/image-11.jpg**  **http://post.mvd.ru/Session/36860-5LrH7m4BipoRiSJ0K1q1-kmbdubw/MIME/INBOX-MM-1/805-02-B/image-11.jpg Внимание! Полиция предупреждает!**  **Дистанционные мошенники!**  **Чтобы не стать жертвой злоумышленников, соблюдайте следующие правила финансовой безопасности:**  **1. Не сообщайте никому свои пороли, ПИН и СVV-коды от банковских карт, даже сотрудникам банка!**  **2. Сообщите банку о смене абонентского номера мобильного телефона, к которому привязаны «Сбербанк Онлайн» и**  **«Мобильный банк», есть риск, что Ваши данные попадут новому владельцу.**  **3. Используйте антивирусы. Приложение «Сбербанк Онлайн» на Андроид имеет бесплатный антивирус.**  **4. Не переходите по подозрительным ссылкам, мошенники могут заразить Ваш компьютер или телефон вирусом и**  **похитить Ваши данные!**  **5. Используйте только официальные приложения банка в AppStore, GooglePlay и MikrosoftStope.**  **При использовании банкоматов:**   1. **Прикрывайте клавиатуру рукой, когда вводите пин-код.** 2. **Не принимайте помощь от незнакомцев, находясь у банкомата, и не совершайте операции под диктовку.** 3. **Осмотрите банкомат перед использованием и убедитесь, что на нем нет подозрительных устройств.**   **Злоумышленники используют мобильные средства связи, различные интернет ресурсы, социальные сети и сайты**  **бесплатных объявлений, наиболее распространенными по способу совершения являются:**   1. **Получение сведений о банковской карте при купле-продаже товаров на сайтах бесплатных объявлений;** 2. **Покупка и продажа товара на интернет - площадках, когда используются сайты-двойники, в домене которых имеется небольшое различие с оригиналом, зачастую лишь в одном символе;** 3. **Просьба в предоставлении денежных средств родственнику или знакомому, чаще всего через социальные сети, доступ к которым взламывается злоумышленниками или по телефону;** 4. **Злоумышленники используют популярные «мессенджеры» и рассылают сообщения якобы от имени банков –«ваша карта заблокирована», «по вашей карте произведено списание денежных средств» и т.д.** 5. **Мошенники выдают себя за сотрудников банка. (При звонке к клиенту сотрудник банка всегда обращается по имени отчеству, никогда не просит конфиденциальные сведения: полные реквизиты банковской карты (номер карты, ПИН и CVV-код, указанный на оборотней стороне карты) CVC-пароли банка, никогда не требует совершать операции с банковской картой. Для контакта с клиентами Сбербанк использует три номера: 900, 8(800)555-55-50, +7(495)500-55-50. Мошенники нашли способ подмены номера, в связи с чем, даже если к Вам поступит звонок с указанных номеров, лучше поставить трубку, заново набрать номер и перезвонить самим в банк.**   **Не теряйте бдительность и трезво оценивайте происходящее!** |