ПАМЯТКА КЛИЕНТАМ БАНКА О СОБЛЮДЕНИИ БЕЗОПАСНОСТИ ДЛЯ МИНИМИЗАЦИИ РИСКОВ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ КАРТ И ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СИСТЕМАМ БАНКОВСКОГО ОБСЛУЖИВАНИЯ

В связи со значительным ростом мошенничества с использованием информационно-коммуникационных технологий необходимо знать основные схемы и признаки мошеннических схем:

1. **Здравствуйте, это «служба безопасности» банка**

Мошенник представляется сотрудником службы безопасности. Звонит с номера, который начинается на 8-495 и, кажется, что звонок действительно из банка (на заднем фоне слышны звуки, напоминающие службу поддержки/call-центр), чтобы у Вас создалось впечатление, что действительно звонит сотрудник банка. Злоумышленник обращается к Вам по имени и отчеству и просит подтвердить расходную операцию, которые Вы, естественно, не совершали.

Мошенник будет пытаться выудить у Вас реквизиты банковской карты для отмены операции: полный номер, срок действия, CVC/CVV, код из смс-сообщения, PIN-код. Или предложит пройти к ближайшему банкомату, перезвонить и потребует перевести деньги с Вашей банковской карты на «безопасный счет»: электронный кошелек, карту стороннего банка или телефон.

Сотрудник банка никогда не будет запрашивать указанные выше реквизиты карты и/или коды. Для отмены операции достаточно услышать, что Вы её не подтверждаете. Если есть малейшие сомнения или подозрения, что звонивший не является сотрудником банка, то перезвоните по официальным телефонам банка, указанным на Вашей карте или сайте банка.

2. **Ваша карта заблокирована**

Мошенники направляют Вам смс-сообщение о блокировке банковской карты. Для разблокировки необходимо перезвонить в банк по указанному номеру или перейти по ссылке:

– если Вы перезвоните, то Вам сообщат, что мошенники пытались перевести деньги с банковской карты и в целях безопасности карта была заблокирована. Для разблокировки потребуется ввести код безопасности из смс-сообщения. Прямо во время разговора Вам поступит смс-сообщение с кодом от банка, которое якобы подтверждает разблокировку. Если Вы сообщите код, то мошенники смогут перевести деньги с банковской карты;

– также мошенники могут переключить Вас на IVR (интерактивное голосовое меню). Зачастую автоответчик вызывает большее доверие, а потом уже попросят ввести код в тоновом режиме после сигнала. Если Вы сообщите код, то мошенники смогут перевести деньги с банковской карты;

– если Вы перейдете по ссылке из смс-сообщения, то откроется форма для ввода реквизитов банковской карты. Данных сведений будет достаточно для воровства Ваших денег.

Сотрудник банка никогда не будет запрашивать реквизиты карты и/или коды для блокировки. Заблокировать карту Вы можете следующими способами: позвонив по официальным телефонам банка, указанным на Вашей карте, сайте банка или с использованием мобильного приложения/интернет-банка. Если есть малейшие сомнения или подозрения, что смс-сообщение мошенническое, то перезвоните по официальным телефонам банка, и ни в коем случае не переходите по ссылкам из смс.

3. **Удаленный доступ**

Мошенник звонит Вам от имени «службы безопасности» банка и сообщает, что были зафиксированы попытки несанкционированного входа в мобильный банк/интернет-банк/проведения мошеннической операции. По ходу общения Вам сообщат, что банк заблокировал попытку входа/подозрительную операцию, и чтобы окончательно отменить платёж или установить дополнительную защиту, потребуется Ваше содействие.

Мошенник НЕ запрашивает реквизиты карты, код из смс, CVC/CVV, логин или пароль для входа в мобильный банк/интернет-банк и тем самым не вызывает подозрений. Злоумышленник обманом вынуждает установить TeamViewer, AnyDesk, RDP, RMS, которые позволяют удалённо управлять Вашим телефоном или компьютером. Далее Вас попросят назвать ID программы и после этого мошенник получит полный доступ к Вашему счету(-ам).

Сотрудник банка никогда не станет просить ни о чём подобном. Если Вы всё же установили программу для удаленного доступа и предоставили мошеннику свой ID, то доказать в банке несанкционированный доступ и кражу денег будет невозможно, так как Вы самолично предоставили мошенникам доступ к своему телефону/компьютеру.

4. **Мошенничество в интернете**

При оплате товаров, услуг банковскими картами в интернете пользуйтесь только проверенными сайтами. Обращайте внимание, указано ли в адресной строке браузера соединение «https://», если да, это значит, что сайт работает по протоколу безопасности Secure Sockets Layer (SSL).

Обращайте внимание на содержание смс-сообщения с кодом для подтверждения операции. Если есть расхождения в сумме, наименовании интернет-магазина, указан тип операции «P2P» (перевод с Вашей карты на стороннюю карту), а не «оплата», то не совершайте данную операцию.

Проверяйте все смс-сообщения от банка о списании денег с банковской карты.

Дорогие Клиенты, будьте бдительны! Обращайте внимание, с какого номера телефона осуществляется звонок или поступает сообщение. Мошенникам не известен номер Вашей банковской карты, счета, логина и пароля для входа в мобильный или интернет-банк. Поэтому при звонке мошенники запрашивают конфиденциальные сведения: полные реквизиты банковской карты, учетные данные для входа в систему дистанционного банковского обслуживания. В сообщении мошенники указывают: «Ваша карта», «Ваш счет».

При любых сомнениях обращайтесь в АО «РОСКОСМОСБАНК» по официальным телефонам, которые размещены на оборотной стороне карты или на официальном интернет-сайте — https://roscosmos-bank.ru.