Простые рекомендации по безопасности позволят избежать риска мошенничества при работе в Интернет-банке или Мобильном банке

1. **Храните ваши пароли в тайне**

Запоминайте ваш пароль и нигде не записывайте его. Выбирайте пароли самостоятельно и никому их не сообщайте. Если ваш пароль стал доступен кому-то еще, незамедлительно измените его. Не используйте в качестве паролей последовательности символов такие как, номера телефонов, даты рождения, регистрационные номера автотранспортных средств и т.п. Также не рекомендуется использовать в качестве паролей имена и фамилии, последовательность букв или цифр расположенных подряд в раскладке клавиатуры

2. **Подключите SMS-информирование по картам**

Подключите SMS-информирование в Интернет-банке, АТМ или отделении Банка и получайте в реальном времени уведомления о всех операциях по вашим картам. Если вы получили сообщение об операции, которую не совершали, обратитесь службу поддержки банка по телефонам: +7(495) 745-79-69, +7(495) 925-80-00 (в Москве) или 8(800) 200-23-26 (в регионах)

3. **Проверяйте адрес сайта при входе в Интернет-банк**

Перед вводом логина и пароля для входа в Интернет-банк проверяйте адрес сайта. Вход в Интернет-банк ВТБ Банка Москвы осуществляется по адресам, которые заканчиваются на **bm.ru** или **mmbank.ru.** Убедитесь в том, что адресная строка в браузере при входе в Интернет-банк начинается с **https://**

ВТБ Банк Москвы использует следующую защищенную ссылку для входа в Интернет-банк https://online.bm.ru

4. **Проверяйте отправителей в sms и e-mail**

Банк Москвы направляет e-mail с адресов, которые заканчиваются **@msk.vtb.ru, @mmbank.ru**, а sms – только с адреса **VTB_BMoskvy**. Не переходите по ссылкам в подозрительных письмах. Помните, что сотрудники банка никогда не просят сообщить ваши личные данные (такие как логин и пароль от Интернет-банка или Мобильного банка, а также ПИН-код к карте) по телефону, в электронном письме или по sms. Если полученное письмо вызывает у вас подозрение, обратитесь в банк по телефонам: +7(495) 745-79-69, +7(495) 925-80-00 (в Москве) или 8(800) 200-23-26 (в регионах)

5. **Используйте современные антивирусы**

Установите на ваш компьютер или мобильный телефон популярный антивирус и поддерживайте его в актуальном состоянии. Современные антивирусы самостоятельно устраняют все угрозы безопасности, шифруют ваши пароли и защищают от программ-шпионов

6. **Используйте лицензионное программное обеспечение**

Устанавливайте программы для обновления только с официальных сайтов или магазинов мобильных приложений. Для повышения безопасности и стабильности работы вашего компьютера или мобильного телефона регулярно обновляйте программное обеспечение

7. **Берегите мобильное устройство**

Не передавайте третьим лицам ваш мобильный телефон, на который приходят SMS с одноразовыми кодами. Если у вас изменился номер телефона для получения одноразовых кодов по SMS, незамедлительно сообщите об этом в банк. Если вы потеряли мобильное устройство, как можно скорее заблокируйте утерянную SIM-карту у вашего оператора и получите новую. Если это

невозможно - незамедлительно позвоните в банк, чтобы заблокировать доступ в Интернет или Мобильный банк

8. Берегите USB-токен

Не передавайте ваш USB-токен третьим лицам даже на короткое время. В случае если вы потеряли USB-токен или у вас есть подозрения, что ключи оказались у третьих лиц, незамедлительно обратитесь в банк для блокировки по телефонам: +7(495) 745-79-69, +7(495) 925-80-00 (в Москве) или 8(800) 200-23-26 (в регионах)

Если вы подозреваете, что кто-то получил доступ к вашим картам, Интернет-банку или Мобильному банку, срочно позвоните в банк по телефонам: +7(495) 745-79-69, +7(495) 925-80-00 (в Москве) или 8(800) 200-23-26 (в регионах)