Уважаемые клиенты! Обращаем Ваше внимание на то, что системы электронного документооборота (СЭД) и системы дистанционного банковского обслуживания (ДБО) являются постоянной мишенью для разного рода злоумышленников. Создаваемые и распространяемые ими вредоносные программы направлены на кражу денег со счетов клиентов. Вы сможете защитить свой компьютер от вредоносного кода, если будете следовать приведенным ниже рекомендациям:

Используйте только лицензионное программное обеспечение, полученное из надежных источников. Взломанное или загруженное с сомнительных интернет ресурсов программное обеспечение может содержать в себе вредоносный код.

Регулярно устанавливайте (или не отключайте автоматическое) обновления для операционной системы и программ, выпускаемые их производителями.

Вредоносные программы зачастую используют уязвимости, которые уже были устранены поставщиками программного обеспечения, в том числе корпорацией Майкрософт. Поэтому важно устанавливать исправления, чтобы обеспечить актуальность программ. Корпорация Майкрософт упрощает эту задачу, предлагая Центр обновления Windows.

Очень важно обновлять и программное обеспечение других разработчиков. Такие поставщики, как Adobe, Sun, Apple и т. д., регулярно публикуют обновления программного обеспечения на своих веб-сайтах.

Используйте на своем компьютере учетную запись с правами администратора/root только тогда, когда Вам нужно изменить настройки системы или установить программное обеспечение. Для повседневной работы создайте и используйте учетную запись с ограниченными правами.

Используйте современные антивирусные программы и регулярно обновляйте как антивирусные базы, так и компоненты самих антивирусных программ. Регулярно проводите полное сканирование системы антивирусной программой.

Скачивайте файлы только с надежных сайтов. При скачивании файла из Интернета убедитесь, что его источник вам известен. Следует скачивать только файлы, предоставленные хорошо известными компаниями. Если вы сомневаетесь, не скачивайте файл. В качестве дополнительной предосторожности можно скачивать файлы не на жесткий диск компьютера, а, например, на USB-накопитель, а затем проверять их с помощью антивирусной программы.

Не посещайте сомнительные интернет сайты и сайты, распространяющие пиратское программное обеспечение или аудио/видео файлы. Большинство подобных сайтов может заразить Ваш компьютер различного рода вирусами.

Соблюдайте осторожность при получении писем с вложениями или гиперссылками. Вирусы и программы-шпионы обычно рассылаются по электронной почте, зачастую в так называемых "поддельных" сообщениях, которые якобы получены от надежного отправителя. Если вы неожиданно получили сообщение с вложенным файлом или ссылкой, внимательно изучите его, даже если в нем указан надежный отправитель. Насколько вероятно, что это человек отправил вам такое вложение или ссылку? Похоже ли сообщение по стилю на другие

его сообщения? Если у вас возникли сомнения, свяжитесь с отправителем и убедитесь, что он действительно отправил вложение или ссылку, прежде чем их щелкать.

Не доверяйте настройку вашего компьютера и установку программ случайным людям.

Мобильные устройства также могут быть подвержены заражению вредоносным кодом, если вы используете мобильный банкинг, Банк рекомендует следовать приведенным ниже правилам:

Так же, как и в случае с почтой на компьютере, будьте очень внимательны, когда проходите по ссылкам, присланным адресатами из Вашего списка контактов, и ни в коем случае не проходите по ссылкам, присланными неизвестным адресатом.

При получении сообщения с предложением посмотреть открытку или фотографию, ни в коем случае не делайте этого, как бы заманчиво это не звучало.

Никогда не делайте неофициальную перепрошивку Вашего устройства для расширения прав доступа к системе.

Устанавливайте все программы на мобильное устройство лично и только из проверенных источников.

Проверяйте, какие программы запущены на Вашем устройстве и что они выполняют.

Будьте особенно внимательны, подключаясь к wi-fi в общественных местах, и ни в коем случае не подключайтесь к неизвестным wi-fi точкам. Владелец такой точки может загрузить на Ваше устройство вредоносную программу.

Внимательно следите за предложениями Банка о внедрении новых средств защиты. Новые угрозы появляются постоянно и оперативное внедрение современных средств защиты - важное условие обеспечения сохранности Ваших финансов.

В случае подозрения на заражение Вашего компьютера или мобильного устройства программами, содержащими вредоносный код, рекомендуем проверить остаток денежных средств на Вашем банковском счете и прекратить использовать данный компьютер или мобильное устройство для осуществления банковских платежей, а также незамедлительно обратиться к квалифицированным IT специалистам.