«01» июня 2019г.

Утверждаю:

Генеральный директор ООО «Фианит – Ломбард»

_____ С.Е. Боронин

Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям

Общество с ограниченной ответственностью «Фианит – Ломбард» (ИНН 7452031712, ОГРН 1027403767368, адрес местонахождения: Россия, Челябинская область, г.Челябинск, ул. Братьев Кашириных, д. 60А, 2 этаж, помещение 18) во исполнение п. 2 Положения Банка России № 684-П от 17.04.2019г. «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» доводит до сведения Клиентов рекомендации по защите информации от воздействия программных кодов во исполнение

1. Используемые понятия

1.1. Ломбард – ООО «Фианит – Ломбард»;

1.2. Устройство – мобильный телефон, персональный компьютер, ноутбук или иное электронное устройство, используемое для получения информации, в том числе содержащей персональные и конфиденциальные данные;

1.3. Вредоносный код (Вирус) – программа, наносящая вред Устройству, на котором запускается. По своему виду деятельности Вирусы могут быть направлены на одно или несколько следующих действий:

- шифрование информации на Устройстве стойким методом для дальнейшего вымогательства денежных средств с владельца информации;
- несанкционированное копирование данных (а том числе о банковских картах, паролей доступа к различным ресурсам) пользователя Устройства с целью дальнейшей перепродажи этих данных и/или шантажа владельца Устройства;
- уничтожение данных на устройства, нанесение ущерба программному и/или аппаратному обеспечению Устройства;
- завладение информацией для осуществления интернет платежей от имени пользователя Устройства;
- введение Устройства в специализированную сеть (ботнет), используемую для последующих атак на ресурсы сети Интернет;
- распространение копий вируса на иные Устройства пользователя, Устройства пользователей из контактов владельца зараженного Устройства, иные Устройства в локальной сети, Устройства третьих лиц;

1.3. Антивирусная программа (Антивирус) – специализированная программа, применяемая для борьбы с Вредоносным кодом, в том числе для недопущения установки, запуска и распространения Вредоносного кода на Устройстве;

1.4. Браузер – специализированная программа, применяемая для обмена информацией в сети Интернет;

1.5. Личный кабинет – специальный раздел на сайте Ломбарда, предназначенный для самостоятельного получения информации, в том числе содержащей персональные и конфиденциальные данные.

2. Рекомендуем использовать следующее:

1. Обновляйте операционную систему Ваших Устройств. Зачастую, Вирусы используют уязвимости в операционных системах. Регулярные обновления операционной системы Устройства позволяет защититься от Вирусов, использующих уже исправленные уязвимости в операционной системе.

2. Используйте актуальную версию браузера. Другим популярным способом распространения вирусов является использование уязвимостей в браузере. Всегда пользуйтесь последней версией браузера, следите за тем, чтобы браузер регулярно автоматически обновлялся.

3. Используйте Антивирус. Современные антивирусные программы способны не только бороться с установленными на Устройство Вирусами, но и предотвращать их установку. Также некоторые Антивирусы предлагают дополнительные меры по защите Устройства. Не игнорируйте данные рекомендации, так как они основаны на анализе настроек, а также версиях программ, установленных на Устройство. Следование предлагаемым мерам защиты поможет уберечь Устройство от заражения. Вне зависимости от регулярной работы Антивируса регулярно проводите полную проверку устройства на наличие уязвимостей и вирусов. Также не забывайте следить за тем, чтобы Антивирус регулярно получал обновления.

4. Используйте исключительно легальное программное обеспечение. Под видом программ для взлома, а также совместно с программами для взлома могут распространятся Вирусы. Такое заражение Устройства является одним из самых опасных, так как происходит с явного согласия пользователя (обычно, чтобы программа взлома сработала, необходимо отключить Антивирус и использовать для запуска права с максимальным доступом к Устройству). Установочные комплекты программного обеспечения следует использовать исключительно с официальных сайтов производителей.

5. Проверяйте все загруженные файлы Антивирусом перед их распаковкой и запуском. Вне зависимости от источника (друг, коллега, служебная рассылка и т.д.) и способа получения (электронная почта, сайт, мессенджер, SMS, MMS и прочее) всегда проверяйте полученные файлы. Помните, что от имени известного вам контакта файл может быть отправлен Вирусом, который заразил иное Устройство.

6. Не переходите по неизвестным ссылкам, которые Вы получили по электронной почте, в социальных сетях, мессенджерах и иными способами от неизвестных контактов. Помните, что ссылка может вести на зараженный сайт или иной опасный для Устройства ресурс в сети.

7. Используйте сложные пароли. При создании учетной записи и дальнейшей ее эксплуатации всегда используйте разные и сложные пароли. Для каждой Вашей учетной записи в сети Интернет пароль должен быть уникальным. Также рекомендуем использовать сложные пароли (размер более 8 символов, использование заглавных и строчных букв, цифр, спец символов).

8. Регулярно меняйте пароли. Зачастую взлом зашифрованного пароля – вопрос времени. Регулярная смена паролей позволит сделать процесс взлома паролей бесполезным, так как к моменту взлома пароль уже будет иной.

9. Используйте многофакторную авторизацию. Многие ресурсы позволяют использовать дополнительные методы верификации. Например, кроме пароля на электронную почту приходит письмо-подтверждение, в котором находится ссылка для входа или дополнительный пароль. Также дополнительным методом защиты могу быть пароли из SMS или специализированных приложений.

10. Не сохраняйте пароли на Устройстве. Всегда вводите пароль самостоятельно. Пароль, сохранный на Устройстве подвержен риску быть украденным.

11. Проверяйте съемные носители (флеш-диски, карты памяти, внешние жесткие диски и так далее) на наличие Вирусов перед запуском/открытием/копированием данных на Устройстве.

12. Делайте резервные копии. Создание копий информации на съемных носителях (флеш-диски, карты памяти, внешние жесткие диски, иные Устройства и так далее) и/или облачных хранилищах позволит восстановить ее в случае уничтожения из-за заражения, поломки или утраты Устройства.

13. Используйте стандартные средства защиты (блокировки) Устройства для входа. Используйте пароли для входа на устройство, дополнительные датчики (сканеры лица и/или отпечатков пальцев). Кроме того, используйте средства удаленной блокировки, стирания информации на Устройстве. Такая защита позволит обеспечить безопасность данных на Устройстве в случае его утраты.

14. Не указывайте свои персональные данные (в том числе номер телефона, реквизиты платежных карт) на неизвестных и подозрительных сайтах.

15. При заражении Устройства Вирусом обратитесь к специалистам. Смените все пароли (в том числе, от личного кабинета финансовой организации, сайтов, социальных сетей, электронной почты). Если были скомпрометированы данные платежных карт – обратитесь в соответствующие организации для блокировки операций, а также для перевыпуска карт.