Общество с ограниченной ответственностью

«Шахтинский Городской Ломбард»

Индекс и адрес регистрации
346500 Ростовская область г. Шахты пер. Красный Шахтер д.61
ИНН\КПП 6155058283\615501001
ОГРНИП 1106182000760
Свидетельство серия 61 №006957756 от 22.03.2010 г.
т. 8(8636)25-58-73

Р/с 40701810052090038840
в ЮГО-ЗАПАДНЫЙ БАНК ПАО "СБЕРБАНК РОССИИ"
К/с 30101810600000000602
БИК 046015602

Рекомендации клиентам ООО «Шахтинский Городской Ломбард» по соблюдению защиты информации при использовании сети интернет.

В соответствии с требованиями Положения Банка России от 17.04.2019 № 684-П ООО «Шахтинский Городской Ломбард» доводит до Вашего сведения основные рекомендации по соблюдению информационной безопасности.

1. Термины

1.1 Вредоносное программное обеспечение («компьютерный вирус») — это программное обеспечение, предназначенное для получения несанкционированного доступа к средствам вычислительной техники (компьютеры, телефоны и т. д.), далее СВТ, с целью несанкционированного использования ресурсов ЭВМ или для получения информации: личной, коммерческой или иной другой; с целью нанесения вреда владельцу информации, СВТ, локальных вычислительных сетей, путем копирования, искажения, подмены, удаления или вывода из строя СВТ.

Вредоносное программное обеспечение способно самостоятельно, без ведома владельца СВТ, создавать свои копии, распространяться различными способами (самокопирование, заражение файлов, создание новых копий отличающихся от оригинала -полиморфизм и др.), что в последующем приводит к уничтожению информации хранящийся на устройстве.

1.2 Антивирусное программное обеспечение — это специальное программное обеспечение для обнаружения вредоносного программного обеспечения, а так же служит для восстановления зараженных файлов к их исходному коду, путем извлечения вредоносной части программы.

Является профилактической мерой для предотвращения заражения СВТ от вредоносного программного обеспечения.

2. Обеспечение безопасности СВТ

2.1 В целях минимизации риска получения несанкционированного доступа к СВТ и информации, ООО «Шахтинский Городской Ломбард» рекомендуем клиентам следующие защитные меры:

Обеспечение безопасности СВТ (компьютер, телефон и др.):

• использование лицензионного программного обеспечения;

• использование антивирусного программного обеспечения;

• ограничение доступа третьих лиц к СВТ;

• использование блокировки СВТ в случае временного прекращения работы;

• при завершении работы — выключение СВТ;

• регулярное обновление комплекса программ: операционных систем, антивирусного программного обеспечения, стороннего программного обеспечения.

Безопасное использование сети-Интернет:

• не отвечать на сомнительные, подозрительные письма от неизвестных адресатов приходящих на Ваш электронный ящик;

• не посещать сомнительные интернет-ресурсы: не известные вам сайты, социальные сети и т.д.;

• обращать внимание на правильное написание адреса сайта в адресной строке браузера. Злоумышленники могут использовать сайты двойники, к примеру: vk1.com, vvk.com, vkk.com и многие другие варианты;

• не сохранять и не устанавливать сторонние программы полученные по электронной почте от неизвестных адресатов, скачанные с неизвестных сайтов, полученные от сомнительных источников;

• при посещении сайтов, не нажимать на всплывающие окна и находящиеся в них ссылки.

Парольная защита:

• использование надежных паролей. Длина не менее 8 символов, использование верхнего и нижнего регистра, цифр. Пример: zyR3ck1P;

• запрещено передавать пароли, хранить в открытом виде, хранить пароли в браузерах;

• систематическое обновление паролей;

• не применять одинаковые пароли к различным системам.

Контроль подключения к личному кабинету ООО «Шахтинский Городской Ломбард»:

• не подключаться к личному кабинету через общественные сети (Wi-Fi, сети Ethernet);

• не подключаться к личному кабинету используя СВТ третьих лиц;

• удостовериться что в том, что сайт использует безопасное соединение https:// (зеленая строка с замочком, верхний левый угол в адресной строке браузера);

• прекратить работу в личном кабинете, если у Вас возникли подозрения, что СВТ

заражен вредоносным программным обеспечением.

• в случае утери СВТ с которого осуществлялся в ход в личный кабинет, обратиться

в ООО «Шахтинский Городской Ломбард» с целью временной блокировки личного кабинета и смены

пароля.

Общие рекомендации:

• проверять полученные файлы антивирусным программным обеспечением;

• проводить регулярную проверку Ваших СВТ антивирусным программным

обеспечением на предмет заражения вредоносными программами;

• проверять расширение файла. Многие вредоносные программы подменяют

расширение файла, при этом оставляя иконку файла нетронутой. К примеру: файл с

расширением 123.xls, при его заражении, может смениться на 123.xls.exe (в данном

случае он стал исполняемым файлом), при его запуске вначале запуститься

вредоносное программное обеспечение, при этом же откроется файл 123.xls, чтобы не

вызвать у Вас подозрение;

• перед запуском сомнительных файлов проверять файл с помощью антивирусного

программного обеспечения на наличие заражения вредоносным программным

обеспечением;

Настоящие рекомендации о рисках получения несанкционированного доступа к

защищаемой информации, о защите информации от воздействия вредоносных кодов и их

своевременному выявлению и нейтрализации, о мерах по предотвращению

несанкционированного доступа к защищаемой информации, доводятся ООО «Шахтинский Городской Ломбард»» до сведения клиентов на основании требования Положения 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 № 684-П,

утвержденного Банком России.