УТВЕРЖДАЮ:

Директор ООО МКК «Вера»

_____ Д.В. Калабин
01 января 2023 года

Приказ № 30 от 01 января 2023 года

ПАМЯТКА ДЛЯ КЛИЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

город Сарапул
2023 год

1. Рекомендации по защите информации от воздействия программных кодов, в целях противодействия незаконным финансовым операциям. Наиболее характерные внешние проявления вирусов и порядок действий в случае обнаружения вирусов.

1.1. Вирус представляет собой программу, которая разрушает информацию на магнитных носителях или нарушает работу ПЭВМ, а также обладает способностью к размножению, т.е. вирус может самостоятельно внедряться в другие программы, переносить себя на диски и дискеты, передаваться по локальной компьютерной сети.

Можно выделить несколько видов воздействия вирусов на ПЭВМ:

- вирусы разрушительного действия;
- вирусы, замедляющие работу ПЭВМ;
- вирусы рекламного характера;
- вирусы-шутки.

Самые опасные вирусы - это вирусы разрушительного действия. Наиболее характерные внешние проявления вирусов этого вида:

- нетипичная работа программ;
- появление на экране дисплея световых пятен, черных областей или символов, не запланированных рабочими программами;
- самопроизвольная перезагрузка операционной системы;
- зависание компьютера;
- появление неисправных участков (кластеров) на «винчестере»;
- неожиданные действия рабочих программ (не предусмотренные документацией на программы);
- искажения данных в обрабатываемых файлах.

1.2. Вирусы, замедляющие работу ПЭВМ, проявляют себя тем, что работа процессора замедляется в 30-40 раз.

1.3. Вирусы рекламного характера и вирусы-шутки хотя и не портят информацию в ПЭВМ, однако замедляют работу или навязывают пользователю ненужные диалоги, что также замедляет весь процесс решения задачи.

1.4. Некоторые вирусы проявляют себя внешне тем, что изменяют дату и время создания файла, хотя внутренние изменения могут быть и разрушительными.

1.5. При возникновении подозрения на наличие компьютерного вируса необходимо провести внеочередной антивирусный контроль.

1.6. В случае обнаружения при проведении антивирусной проверки зараженных вирусами файлов:

- приостановить работу;
- провести лечение или уничтожение зараженных файлов;
- обратиться к специалистам.

2. В целях предотвращения несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, Общество рекомендует:

2.1. Ограничить доступ третьих лиц к устройству, в том числе:

- не оставлять устройство без присмотра;
- не передавать устройство третьим лицам.

2.2. Ограничить доступ третьих лиц к информации о паролях и логинах, используемых для входа в информационные ресурсы, в том числе:

- использовать пароли, составленные не менее чем из 8 символов;
- использовать пароли, в которых одновременно содержатся буквы различного регистра, цифры и символы;
- использовать разные пароли и логины для входа в разные информационные ресурсы;
- хранить логины и пароли в тайне от третьих лиц;
- не записывать и не хранить логины и пароли для входа в информационные ресурсы на бумажном носителе, к которым возможен доступ третьих лиц;
- не использовать функцию запоминания логина и пароля при входе в информационный ресурс;

- не использовать в качестве пароля имена, памятные даты, номера телефонов и другую подобную информацию, которая может быть получена или угадана третьими лицами.

2.3. Соблюдать режим конфиденциальности в отношении защищаемой информации в информационно-телекоммуникационной сети «Интернет», в том числе:

- ограничивать доступ ресурсам в информационно-телекоммуникационной сети «Интернет» к устройству Клиента;
- использовать только надежные порталы для информационного обмена в информационно-телекоммуникационной сети «Интернет»;
- проверять адрес электронной почты отправителя перед просмотром сообщения;
- внимательно проверять и анализировать ссылки на информационные ресурсы;
- не открывать сообщения и вложения к ним, полученные по электронной почте от неизвестных отправителей;
- не переходить по активным ссылкам, полученным по электронной почте от неизвестных отправителей;
- программам, скачиваемым из информационно-телекоммуникационной сети «Интернет», не разрешать доступ к излишней информации;
- при нахождении в общественных местах и местах скопления людей, располагать экран устройства таким образом, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами;
- при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия вирусов;
- не отключать средства антивирусной защиты информации;
- не подключаться к публичным беспроводным сетям Wi-Fi. незащищенным беспроводным сетям.

2.4. В случае утраты (потере, хищении) клиентом устройства по возможности в кратчайший срок предотвратить несанкционированный доступ к защищаемой информации, в том числе:

- незамедлительно сообщить своему оператору сотовой связи о факте утраты устройства и заблокировать SIM-карту;
- незамедлительно сообщить о факте утраты устройства Обществу;
- незамедлительно сменить все логины, пароли, электронные ключи и прочие средства аутентификации, при помощи которых осуществлялся доступ с утраченного устройства;
- обратиться в правоохранительные органы.

3. В целях контроля конфигурации устройства, с использованием которого клиентом совершаются действия по осуществлению финансовой операции. Общество рекомендует:

3.1. Установить соответствующее программное обеспечение, в том числе:

- использовать только лицензионное программное обеспечение;
- своевременно устанавливать из официальных источников доступные обновления программного обеспечения и операционной системы;
- загружать и устанавливать программное обеспечение только из проверенных источников.

3.2. В целях своевременного обнаружения воздействия вредоносного кода Общество рекомендует:

3.3. Установить соответствующее антивирусное программное обеспечение, в том числе:

- установить известную (проверенную) антивирусную защиту;
- установить автоматическое обновление антивирусных баз;
- осуществлять регулярный контроль антивирусной защиты.

3.4. Соблюдать рекомендации настоящей памятки по защите информации.

ВНИМАНИЕ! Передача карты или ее реквизитов, Логина, ПИН кода, кода CVV2 или CVC2, указанных на оборотной стороне пластиковой карточки, предназначенных для доступа и подтверждения операций, другому лицу (в том числе работнику микрофинансовой организации) означает, что Вы предоставляете возможность другим лицам проводить операции по счетам.

При любых подозрениях на мошенничество следует незамедлительно обратиться в Банк, обслуживающий вашу пластиковую карту по номерам телефонов, указанным на оборотной стороне карты и на Официальном сайте Банка.