УТВЕРЖДЕНО
ПРЕДСЕДАТЕЛЕМ ПРАВЛЕНИЯ
БАНКА «ПРОХЛАДНЫЙ» О О О
ПРИКАЗ № 17 ОТ «07» февраля 2019 г

Рекомендации по защите информации от воздействия вредоносного кода.

1. Вредоносные программы.

Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» (типа «гуляющих» по монитору картинок) до полного разрушения информации, хранящейся на дисках компьютера.

2. Антивирусные программы ваши первые защитники.

Антивирусные программы – основное средство борьбы с вредоносными программами. Установите современное лицензионное антивирусное программное обеспечение, осуществляющее постоянный контроль за компьютером и мобильным устройством. Периодически запускайте полную проверку компьютера. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

3. Обновления - это полезно и безопасно.

Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки. Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы, устанавливая самые последние обновления. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

4. Проверяйте новые файлы

Будьте очень осторожны при получении сообщений с файлами-вложениями. Обращайте внимание на расширение файла. Вредоносные файлы часто маскируются под обычные графические, аудио и видео файлы. Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов. Подозрительные сообщения лучше немедленно удалять.

При открытии ссылок, полученных по электронной почте, скопируйте ссылку, вставьте в адресную строку используемого браузера и убедитесь, что адрес соответствует интересующему Вас ресурсу.

Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять. Проверяйте все новые файлы, сохраняемые на компьютере. Периодически проверяйте компьютер полностью.

5. Будьте бдительны и осторожны

По возможности не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их. При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой.

При использовании браузера не переходите по ссылке и не нажимайте на кнопки во всплывающих окнах. Старайтесь избегать сайтов, которые могут иметь незаконное и/или вредоносное содержание.

Проверяйте все съемные носители информации (USB-Flash, CD/DVD-диски, карты памяти SD и т.п.) до начала их использования.

Избегайте использования привилегированных учетных записей (например, Администратор) для ежедневного использования. Для выполнения большинства операций достаточно прав обычного пользователя.

Периодически удаляйте программное обеспечение, которое больше не нужно.

6. Резервное копирование гарантия безопасности

Регулярно выполняйте резервное копирование важной информации. Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой.

7. Тактика борьбы с вредоносными программами

Вредоносные программы представляют собой файлы, которые срабатывают при активировании на компьютере. Тактика борьбы с ними достаточно проста:

а) не допускать, чтобы вредоносные программы попадали на Ваш компьютер;

б) если они к Вам все-таки попали, ни в коем случае не запускать их;

в) если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба.

Самый действенный способ оградить от вредоносных программ свой почтовый ящик – запретить прием сообщений, содержащих исполняемые вложения.

9. Расширение файла – это важно!

Особую опасность могут представлять файлы со следующими расширениями:

***ade, *adp, *bas, *bat;*chm, *cmd, *com, *cpl;*crt, *eml, *exe, *hlp;**
***hta, *inf, *ins, *isp; *jse,*lnk, *mdb, *mde; *msc,*msi, *msp, *mst; *pcd,**
***pif, *reg, *scr; *sct,*shs, *url, *vbs; *vbe,*wsf, *wsh, *wsc.**

Помните, что в сети Интернет действует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы.

Если Ваш компьютер или мобильное устройство подверглось заражению, рекомендуется обратиться к квалифицированным специалистам, а также сменить пароли от Интернет-Банка, электронной почты, учетных записей в социальных сетях и т.п. с помощью не зараженного устройства.