Небанковская кредитная организация «МОНЕТА» (общество с ограниченной ответственностью) 424000, г.Йошкар-Ола, ул. Гоголя, д.2, стр. «А» , тел. (8362) 45-43-83 ОГРН 1121200000316 ИНН/КПП 1215192632/121501001 БИК 048860734	

ПАМЯТКА ПО ЗАЩИТЕ
ОТ ВРЕДОНОСНОГО КОДА
НЕБАНКОВСКОЙ КРЕДИТНОЙ ОРГАНИЗАЦИИ
«МОНЕТА» (общество с ограниченной ответственностью)

(Версия № 1.1)

Йошкар-Ола, 2018

1. Вредоносный код

Вредоносный код - компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспеченье, средства вычислительной техники, телекоммуникационное оборудование, приводящего к несанкционированному уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации.

Вредоносный код обычно представляется в виде компьютерных вирусов, программ «троянских коней», систем несанкционированного удаленного управления, программ вымогателей и других вредоносных программ.

Вариантов проникновения вредоносного кода на компьютер или мобильное устройство большое количество, наиболее распространенными являются:

- посещение мошеннических web-сайтов, либо web-сайтов, зараженных вредоносным кодом;
- получения сообщения, содержащего вредоносный код или ссылку на вредоносный код через электронную почту, систему обмена сообщениями, SMS, MMS или из социальной сети;
- просмотр или запуск файлов на флэшках, оптических дисках и других носителях, содержащих вредоносный код;
- скачивания файлов, содержащих вредоносный код с файлообменных сайтов или систем обмена файлами;
- скачивание программ из магазинов приложений (Google Play, Apple store и других) содержащих вредоносный код;
- не отключать антивирусное программное обеспечение ни под каким предлогом.

Вредоносный код, может содержаться практически в любых файлах начиная с файлов приложений, плагинов к браузерам, заканчивая электронными документами и файлов мультимедиа.

2. Средства защиты от вредоносного кода

Использование средств антивирусной защиты. Специализированные программы-антивирусы являются довольно эффективным средством защиты от вредоносного кода, хотя и не гарантируют 100% защиту. При выборе антивируса рекомендуется отдать предпочтение решениям, обеспечивающим комплексную защиту и включающими в себя антивирус, межсетевой экран и систему оценки репутации сайтов (так называемые решения класса Internet Security). В качестве рекомендаций по использованию антивируса предлагается:

- настроить антивирус на работу в режиме автоматического лечения файлов;
- проверять все файлы, скачанные из Интернет или полученные на флеш-накопителях или оптических дисках, а также регулярно проводить полную антивирусную проверку;
- настроить антивирус на автоматическое обновление антивирусных баз и обеспечить обновления не реже одного раза в день;
- устанавливать пароль на отключения системы антивирусной защиты либо на деинсталляцию.

Для выбора подходящего и наиболее эффективного средства защиты, рекомендуется изучить исследовательские отчеты от экспертов в области информационной безопасности. В качестве примера, можно обратиться к порталу www.anti-malware.ru, где регулярно публикуются обзоры средств защиты.

Одним из лидеров в области антивирусной защиты информации является «Лаборатория Касперского». Ежегодно данный разработчик представляет новые решения не только в области защиты от вредоносного кода, но и обеспечения комплексной защиты

информации как в домашних условиях, так и в условиях бизнеса. С точки зрения домашнего использования, решения «Лаборатории Касперского» представляют собой интуитивно понятную систему, с которой в состоянии справиться обычный пользователь компьютера.

«Лаборатория Касперского», сайт - www.kaspersky.ru.

Другим отечественным производителем средств защиты от вредоносного кода является «Dr.WEB». Данная компания очень давно существует на рынке и обладает большим опытом в своей области. Одной из особенностей продуктов компании «Dr.WEB» является гибкая политика лицензирования, которая позволит подобрать для себя именно тот продукт, который необходим для решения поставленной задачи. Более того, у «Dr.WEB» хорошо развита партнерская сеть, что иногда позволяет использовать продукты «Dr.WEB» абсолютно бесплатно, не нарушая лицензионных соглашений.

«Dr.WEB», сайт - www.drweb.ru.

Одним из самых популярных антивирусов является «Avast! Internet Security. Данный продукт выполнен, как в платной, так и в бесплатной версиях. Разница в версиях заключается в количестве инструментов, обеспечивающих безопасность компьютерной системы. Однако даже в бесплатной версии предусмотрен файловый антивирус, который, по данным www.anti-malware.ru определяет порядка 67% заражений.

«Avast!», сайт - www.avast.ru.

В ситуациях, когда нет возможности использовать средство защиты от вредоносного кода, но существует потребность проверки файла на наличие вредоносного кода, можно воспользоваться сервисом, расположенным по адресу - www.virustotal.com. Данные сервис осуществляет проверку файла сразу несколькими антивирусными решениями. При использовании данного сервиса, стоит помнить, что вы направляете файл, со всем его содержимым в недоверенную среду, следовательно, при наличии информации конфиденциального характера в проверяемом файле, есть риск её раскрыть как минимум для владельцев данного сервиса.

3. Организационные меры по защите от вредоносного кода

Необходимо убедиться в правильности адресов интернет-сайтов, к которым происходит подключение и на которых есть потребность совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

Необходимо использовать личную учетную запись в операционной системе, доступа к которой более ни у кого нет. Кроме того, учетная запись, с которой происходит работа в интернете, не должна обладать правами администратора операционной системы.

По возможности не стоит пренебрегать использованием систем многофакторной аутентификации – одноразовые SMS-пароли, Google Authenticator и прочее.

Необходимо повышать свою осведомленность в области информационной безопасности. Это поможет быть в курсе текущих событий в данной области и, возможно, избежать действий, которые могут повлечь за собой заражение вредоносным кодом.