Рекомендации
для клиентов ООО РНКБ Страхование по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям

В целях обеспечения информационной безопасности при работе в информационных системах, а также для минимизации рисков информационной безопасности, обращаем Ваше внимание на необходимость выполнения следующих рекомендаций:

1. Обеспечение безопасности персонального компьютера (ПК) или мобильного устройства

1. Управление доступом посторонних лиц к ПК путем создания персонифицированных (личных) учетных записей с ограничением прав на выполнение и установку постороннего программного обеспечения (в случае мобильного устройства – использование код-пароля для разблокировки и выполнения определенных действий).
2. Исключение бесконтрольного доступа к ПК и/или мобильному устройству.
3. Использование на ПК или мобильном устройстве только лицензионных операционных систем или сертифицированного свободно распространяемых операционных систем с актуальными установленными обновлениями, в том числе обновлениями безопасности.
4. Установка на ПК или устройстве минимально необходимого набора программ. Также не должны запускаться программы, полученные из непроверенных источников.
5. Обязательно наличие сертифицированного антивирусного программного обеспечения с регулярно обновляемыми базами. Необходимо периодически осуществлять полную проверку ПК или устройства на предмет наличия вирусов.
6. По возможности рекомендуется установить на ПК персональный межсетевой экран.
7. Работать на ПК в операционной системе рекомендуется под правами пользователя.
8. Не должны быть заведены учетные записи без паролей или с паролями по умолчанию. Учетная запись «Гость» должна быть заблокирована.
9. Не устанавливать и не использовать программы удаленного доступа к ПК (TeamViewer, RAdmin и аналогичные). Ограничить доступ «Удаленного помощника».

2. Обеспечение безопасности при работе в сети Интернет

1. Обращать внимание на адрес Интернет-сайтов, на которых производите онлайн-оплату. Адрес должен начинаться с https:// (а не с http://).
2. Не посещать Интернет-сайты сомнительного содержания.
3. Не использовать для подключения к Интернету беспроводные непроверенные и общедоступные точки доступа.
4. Регулярно менять пароли от аккаунтов в социальных сетях и почтовых ящиков, не использовать один и тот же пароль для разных сервисов.
5. Использовать дополнительный (специальный) почтовый ящик для регистрации на сайтах, маркетплейсах, в социальных сетях.
6. При онлайн покупках в информационно-телекоммуникационной сети "Интернет" рекомендуется использовать отдельную банковскую карту.
7. Ознакамливаться с политикой конфиденциальности сайтов.
8. Закрыть свои аккаунты в социальных сетях и включить двухфакторную аутентификацию;
9. Не выкладывать в социальных сетях личную информацию и фотографии документов;
10. Не принимать cookie-файлы на сайтах автоматически.

3. Обеспечение безопасности при работе с паролями

1. Пароль необходимо устанавливать самостоятельно и никому его не сообщать.
2. В качестве пароля необходимо использовать последовательности длинной не менее 8 символов (желательно - 12 символов).
3. Для формирования паролей использовать комбинации, состоящие из строчных и прописных символов латинского алфавита, цифр, а также специальных символов (!, @, #, $, % и т.д.);
4. Генерацию новых паролей необходимо осуществлять на основе псевдослучайных функций.
5. Пароли, содержащие имена, названия городов, клички животных, номера телефонов, даты рождения, общепринятые слова и выражения, а также пароли типа "p@ssw0rd123", "qwerty12345" являются ненадежными.
6. Смену паролей необходимо производить не реже, чем раз в 90 дней (при смене пароля необходимо менять его полностью, не ограничиваясь добавлением нескольких символов к прежнему паролю).
7. Желательно настроить механизмы защиты от подбора аутентификационных данных, использовать меры по временной блокировке учетных записей.
8. Пароли недопустимо записывать на листках и хранить под клавиатурой, на мониторе, иных доступных местах, а также недопустимо хранить в текстовых файлах на ПК в незашифрованном виде.
9. По возможности необходимо включить двухфакторную аутентификацию.
10. Нельзя сообщать постоянные и одноразовые пароли, в том числе полученные посредством SMS-сообщений и PUSH-уведомлений.
11. В случае утраты мобильного устройства, к номеру которого «привязаны» Интернет-сервисы, необходимо срочно заблокировать SIM-карту.

4. Противодействие фишинговым рассылкам

Фишинговые письма могут содержать вредоносные вложения (архивы, текстовые и исполняющие файлы), предложение перехода на сторонние ресурсы, например, в целях принятия участия в онлайн-конференциях или ознакомления с копиями бухгалтерских документов.

Конечная цель таких запросов может быть различной, начиная от рекламы коммерческих образовательных программ и обеспечения прохождения Интернет-трафика на рекламных страницах, заканчивая попытками внедрения вредоносного программного обеспечения.

Для того, чтобы не стать жертвой фишинговых рассылок рекомендуется:

1. С подозрением относиться к любым письмам с вложениями и ссылками, полученными от неизвестных отправителей.
2. Обязательно проверять известные URL-адреса, по которым рекомендуется перейти, на наличие незначительных ошибок в написании.
3. Использовать безопасные https-соединения;
4. Получив подозрительное сообщение от имени знакомого отправителя, но с незнакомого адреса электронной почты, стоит связаться с отправителем каким-либо альтернативным способом.
5. Внимательно относиться к сообщениям, содержащим гиперссылки;
6. Перед пересылкой писем от незнакомых источников необходимо производить проверку источников таких запросов, принадлежность домена, к которому относится адрес электронной почты отправителя, а также принадлежность домена и хостинга интернет ресурса, на который предлагается перейти, согласно таким письмам.

5. Действия при обнаружении попыток несанкционированного доступа

Для предупреждения несанкционированного доступа к Вашему ПК важно обращаться внимание на нестандартную работу ПК.

Типичными признаками несанкционированного доступа к ПК являются:

– самопроизвольный запуск программ и процессов;

– самостоятельные движения указателя мыши и открытие каталогов;

– всплывающие уведомления антивирусного программного обеспечения;

– самопроизвольное отключение антивирусного программного обеспечения;

– сбои в работе операционной системы (наличие периодических сообщений об ошибках);

– крайне медленная работа ПК с малым количеством запущенных программ.

При обнаружении попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть осуществлены, необходимо незамедлительно отключить ПК от сети Интернет и произвести полное его сканирование на наличие вирусов. Также рекомендуется с помощью другого устройства, подключенного к сети Интернет, скачать бесплатную утилиту для антивирусной проверки (например, Dr.Web CureIt или Kaspersky Virus Removal Tool) и осуществить ее запуск с целью дополнительной проверки ПК на наличие вирусов.

Выполнение вышеуказанных рекомендаций позволит минимизировать риски информационной безопасности, в том числе снизить риски несанкционированного списания денежных средств.