Рекомендации по соблюдению мер информационной безопасности при использовании информационных сервисов

Выполнение настоящих рекомендаций по информационной безопасности позволит обеспечить защиту информационного обмена с поставщиком информационных услуг и минимизировать риски возможных потерь.

1. Общие положения

1.1 Кража учетных данных – хищение личных данных клиента и их незаконное использование для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.

1.2 Задачи защиты информации сводятся к минимизации ущерба и предотвращению злонамеренных воздействий. Для обеспечения надлежащей степени защищенности необходимо использование комплексного подхода, когда вопросам информационной безопасности уделяется достаточно внимания.

1.3 Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью получения конфиденциальных сведений – личных данных, логинов, паролей и др.), а также воздействием вредоносного кода.

1.4 «Фишинг» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

1.5 Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах (смартфонах, планшетах), с которых осуществляется работа с информационным сервисом, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе логинов/паролей.

2. Рекомендации по защите информации от воздействия вредоносного кода

2.1 На персональном компьютере Клиента должно быть установлено лицензированное антивирусное программное обеспечение (ПО). Антивирусное ПО должно регулярно обновляться. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов производится антивирусным ПО в автоматическом режиме.

2.2 Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного ПО.

2.3 Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т.п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

2.4 При использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное ПО, поддерживающее проверку почтовых клиентов.

2.5 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т.п.) или нарушения работоспособности компьютера необходимо осуществить внеплановую проверка на наличие вредоносного ПО. После удаления вирусов и восстановления работоспособности компьютера необходимо произвести смену паролей на новые, удовлетворяющие требованиям п. 4.1.

2.6 Не открывайте файлы, полученные по электронной почте от неизвестных отправителей.

3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

3.1 Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, Банка), и предназначены для сбора конфиденциальной информации обманным путем.

3.2 Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

3.3 Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.

3.4 Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашему счету угрожает опасность, если Вы немедленно не обновите критически важные данные.

3.5 Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1 Рекомендуется регулярно менять пароли для работы со своими учетными данными в различных системах. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное, неповторяющееся сочетание строчных и прописных букв, цифр и символов.

4.2 Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные (например, портал Госуслуг, онлайн-Банкинг и т. д.).

4.3 В случае компрометации или подозрениях на компрометацию пароля, рекомендуется незамедлительно сменить пароль на новый, удовлетворяющий требованиям п. 4.1.

4.4 Никому передавайте и не разглашайте свои пароли.

4.5 Рекомендуется установить пароли на учётные записи пользователей операционной системы на компьютере.

4.6 Рекомендуется установить на телефон антивирусное ПО и своевременно его обновлять.

4.7 Рекомендуется включить блокировку экрана для мобильных устройств и отключить показ любых паролей при вводе.

4.8 Рекомендуется исключить возможность физического доступа посторонних лиц к компьютеру, с которого Вы осуществляете работу.

4.9 Рекомендуется применять на компьютере для работы специализированные программные и аппаратные средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п., обеспечить регулярное автоматическое обновление программного обеспечения этих средств.

4.10 На компьютере для работы необходимо исключить посещение WEBсайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п. Использование нелицензионного ПО повышает риск получения несанкционированного доступа злоумышленников с целью хищения информации.

4.11 Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ; старайтесь периодически просматривать журнал и реагировать на ошибки. Во избежание инцидентов, связанных с неправомерным использованием Вашей компьютерной техники, используемой для работы с информационными сервисами, убедительно просим Вас неукоснительно соблюдать рекомендуемые выше правила безопасности.

Только комплексное соблюдение описанных правил безопасности позволит Вам не стать жертвой мошенников и иных злоумышленников и поможет обеспечить защиту ВАШИХ ДАННЫХ.