Перечень рекомендаций по обеспечению информационной безопасности персональных данных в части открытия сайтов, ссылок на интернет-ресурсы, чатах, порядка регистрации, формирования сложных паролей, ввода персональных данных

При регистрации на интернет-ресурсах пользователю предлагается заполнить текстовые поля, содержащие его персональные данные, с помощью которых пользователь опознается в системе как конкретное физическое лицо. К данным, которые пользователь предоставляет могут относиться: ФИО, номер телефона, адрес электронной почты, адрес проживания, дата рождения, паспортные данные, фотографии, ИНН, сведения о работе, ссылки на профили в социальных сетях и мессенджерах.

На сайтах, осуществляющих сбор и обработку персональных данных, должна быть размещена политика конфиденциальности с описанием того, какие именно персональные данные собираются сайтом и с какой целью, а также условия их хранения и передачи. Кроме того, в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», интернет-ресурс имеет право собирать и обрабатывать персональные данные пользователя только при предоставлении согласия на обработку персональных данных пользователя. Для этих целей в большинстве случаев после формы заполнения данных сайтом размещается уведомление об ознакомлении пользователя с политикой конфиденциальности, а также о согласии пользователя на обработку его персональных данных. Соответственно, интернет-ресурсы, на которых отсутствуют вышеуказанные пункты может быть ненадежным, а переданные пользователем персональные данные могут быть переданы третьим лицам, в том числе иностранным организациям.

Одним из распространенных видов мошенничества в Интернет-пространстве является фишинг, при котором злоумышленник создает точную копию хорошо известного сайта с идентичной стилистикой и оформлением, которую трудно отличить от оригинала. При переходе пользователя по ссылке на этот сайт злоумышленник может получить данные (логин, пароль) от учетной записи пользователя и получить к ней прямой доступ. В данном случае, все введенные пользователем данные попадают владельцу поддельного сайта, коим и является злоумышленник. Итоговой целью злоумышленника зачастую является шантаж в случае если доступ был получен к учетной записи социальный сетей или мессенджеров, либо кража денежных средств в случае, если в результате фишинга был получен доступ к банковскому счету.

Для того, чтобы сохранить свои данные под защитой и не передать злоумышленнику случайным образом, необходимо следовать некоторым правилам:

- внимательно проверять правильность написания адреса сайта, на котором осуществляется ввод данных. Для максимальной правдоподобности некоторые символы в адресе сайта могут быть заменены на схожие по написанию. То же относится и к адресам электронной почты, с которых может прийти письмо со ссылкой или прикрепленными файлами;

- «надежность» сайта возможно определить по наличию значка «замок» в начале адресной строки, либо слов «Соединение защищено», «Надежный» или подобным. При отсутствии такого значка, либо если ссылка на сайт отображается красным цветом или предупреждающим символом, стоит открыть необходимый сайт обычным способом, введя адрес вручную и авторизоваться стандартным путем. Во многих случаях, браузер оценивает надежность сайта, в том числе, по указанному протоколу «http» либо «hhtps». Протокол «http» считается ненадежным, так как данные на таком сайте передается в открытом, незашифрованном виде, в котором их могут перехватить третьи лица. Однако, несмотря на то, что сайты с протоколом «https» передают информацию в зашифрованном виде, такие сайты не всегда являются гарантией безопасного соединения;

- ссылки на конкретные сайты с целью удобства возможно сокращать с помощью определенных сервисов, поэтому прежде чем переходить по сокращенной ссылке стоит понять, на какой именно сайт она ведёт. Для этого необходимо воспользоваться одним из сервисов по дешифрованию коротких ссылок (https://ciox.ru/check_short_url, https://seolik.ru/short-link-checking или иные) либо просто введя поисковый запрос «куда ведет сокращенная ссылка»;

- избегать посещения сайтов сомнительной репутации и скачивания с них каких-либо файлов и программного обеспечения, а также подключения неизвестных съемных носителей информации (флеш-карт, внешних жестких дисков) к автоматизированным рабочим местам;

- проводить регулярную антивирусную проверку рабочего места и подключаемых к нему носителей информации лицензированными средствами антивирусной защиты.

При регистрации на различных интернет-ресурсах и социальных сетях следует уделять особое внимание данным которые пользователь использует при авторизации. Если при авторизации для поля «имя пользователя» или «логин» зачастую используется адрес электронной почты, номер телефона или собственный логин, то пароль к нему придумывает сам пользователь.

Чем сложнее придуманный пароль, тем сложнее становится процедура его подбора или взлома для злоумышленника. Пароль должен быть длиной не менее восьми символов и состоять из цифр и букв как в верхнем, так и нижнем регистрах. Рекомендуется также включаться в пароль специальные символы и знаки. Запрещается записывать пароли на бумаге и размещать в общедоступных местах, а также передавать другим работникам и третьим лицам. В случае, если интернет-сайтом предусмотрена возможность многофакторной аутентификации, например, с подтверждением авторизации через смс-сообщение либо почтовое сообщение, то использование данный функции позволит обеспечить дополнительную защиту учетной записи. При этом код подтверждения либо ссылка, которые приходят на электронную почту в целях подтверждения входа, не должны передаваться третьим лицам. В случае утери или подозрения на компрометацию логинов и паролей необходимо оперативно произвести их смену.

Вышеуказанные меры защиты информации позволят пользователю интернет-ресурсов сохранить свои персональные данные под защитой, а также предотвратить возможность попадания личных данных в руки злоумышленников.