ОБУЧЕНИЕ – НЕОБХОДИМОЕ УСЛОВИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПЕРИОД ЦИФРОВИЗАЦИИ

Власова Г.А., Войтехович С.А.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Беларусь, gvlas@tut.by

Abstract. The consequence of the fast digitalization of society is that people that don't have technical education, become users of information technology. Low-level education of users in the sphere of information safety leads to vulnerability of networks and systems. Recommendations for protection of users against threats are considered.

Вместе с технологиями и техникой развивается и киберпреступность. Взлом почты, кража паролей, получение доступа к персональным данным, в том числе к личной информации и банковским аккаунтам – те из немногих проблем, которые могут принести мошенники.

Быстрая цифровизация общества приводит к тому, что пользователями информационных технологий становятся люди, не имеющего технического образования или вовсе не осведомлённые о принципах защиты собственной информации в цифровом обществе.

Недостаточная осведомлённость пользователей в вопросах информационной безопасности приводит к уязвимости сетей и систем. Например, уязвимости появляются из-за недостаточной проверки данных, вводимых пользователем, и позволяют вставить в интерпретируемый код произвольные команды (SQL-инъекция, XSS, SiXSS); загрузки сомнительных программ из сети; использования открытых Wi-Fi сетей без применения каких – либо средств защиты и так далее [1].

Для того, чтобы не стать «жертвой» киберпреступников в современном мире, каждый пользователь должен знать и применять следующие правила:

– ставить пароли на устройства, причем пароль не должен содержать данные, которые легко найти в открытом доступе – девичья фамилия матери, любимая команда, номер телефона и так далее;

– не использовать секретные вопросы для восстановления пароля, поскольку подобрать ответ для профессионала – вопрос времени;

– использовать разные пароли для аккаунтов;

– не вводить пароли под камерами, в общественных местах, где его может увидеть злоумышленник;

– помимо пароля использовать двухфакторную аутентификацию через google authentificator, не использовать и не привязывать номер телефона к аккаунтам – злоумышленники могут перехватить смс, либо продублировать номер сим-карты;

– применять полное шифрование данных [2], iphone уже делает это, в большинстве телефонов android можно включить опцию; для компьютеров под macos и windows professional есть встроенные инструменты, в остальных случаях помогут бесплатные шифровщики;

– использовать надежные сервисы для хранения и переписки;

– включать pgp-шифрование для электронной почты;

– обмениваться сообщениями в современных мессенджерах, шифрующих данные, например, telegram, signal, whatsapp; даже facebook messenger усложнит доступ к переписке;

– не забывать удалять сообщения и чистить историю;

– осторожно работать с открытыми wi-fi сетями, с их помощью злоумышленники способны перехватить данные; если нужно подключиться к сети в общественном месте – использовать vpn;

– обращать внимание на интерфейсы устанавливаемых программ и посещаемых сайтов: мошенники умеют подделывать их, чтобы завладеть логинами-паролями невнимательных пользователей;

– не переходить по сомнительным ссылкам;

– устанавливать приложения только из достоверных источников; всегда проверять, какую именно информацию хочет использовать новое приложение, и если вы не доверяете разработчикам, то лучше не рисковать, предоставляя доступ;

– для подписок, рассылок и регистраций на сайтах завести отдельную почту, никак не связанную с основной; либо пользоваться сервисами генерации временных адресов;

– отключать опцию сбора геолокации во всех программах, где она не нужна.

Необходимость соблюдения данных правил очевидна для специалистов в области информационной безопасности. Однако пользуются информационными ресурсами не только они, но и люди без специального образования, которые, тем не менее, предполагают, что их данные защищены. При этом защита информации невозможна без правильного поведения каждого пользователя. Поэтому обучение основам информационной безопасности необходимо донести до каждого пользователя устройств, имеющих доступ в сеть Internet.

Из изложенного выше следует, что решить проблему информационной безопасности сетей и систем невозможно без знаний и обучения пользователей, в противном случае это приведет к неминуемой краже данных или их утрате.

Литература

1. IoT Goes Nuclear: Creating a ZigBee Chain Reaction [Электронный ресурс]. – Режим доступа: http://iotworm.eyalro.net.

2. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. Выпуск №1 (9), 2015. – с. 26-43.