Файзуллин Рамазан Рустамович
студент 3 курс, Институт истории и государственного управления
Башкирский государственный университет
Россия, г.Уфа
Байрушин Федор Тимофеевич
доцент кафедры «Управления информационной безопасностью»
Институт истории и государственного управления
Башкирский государственный университет
Россия, г.Уфа

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

Аннотация: *Мы живем в XXI веке. Многие люди уже не представляют свою жизнь без Интернета. К числу этих «многих людей» относятся Интернет - мошенники, которые стремятся украсть у ни в чем неповинного пользователя его данные, деньги и многое другое, тот, кто не знает, что делать, обязательно попадется на удочку злоумышленников.*

Ключевые слова: *социальная сеть, угроза, информационная безопасность, метод, интернет.*

Annotation*: We live in the XXI century. Many people no longer imagine their lives without the Internet. Among these "many people" are Internet scammers who seek to steal from anything innocent user his data, money and much more, one who does not know what to do will necessarily fall for the bait of intruders.*

Keywords: *social network, threat, information security, method, Internet.*

Социальная сеть (Интернет) - платформа, онлайн-сервис и веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений в Интернете. Исходя из этого определения, сделаем вывод, что интересны будут персональные данные, которые предоставляются самими пользователями. Большая часть пользовательских данных настоящая, потому что мы ищем друзей, соседей и так далее. Пользователи чаще всего

вносят данные: имя, фамилия, отчество, адрес, интересы, места отдыха, работы.

По исследованиям массачусетского университета флористики среднему хакеру для взлома пароля требуется 30-60 минут. Простые пароли хакеры могут взломать без применения специальных программ. Сложные же пароли взламываются при помощи специальных программ-взломщиков. Эти программы содержат словари с паролями. Остается только подобрать пароль. Даже , самый первый червь, написанный в 1988 году уже умел подбирать пароли по словарю. Недавний виновник глобальной эпидемии kido (conficker) имел обширный словарик с паролями. Социальные сети на данный момент времени остаются очень популярными среди аудитории, которая принадлежит разным возрастным группам. Вместе с тем, наиболее уязвимой является группа школьного возраста, что связано не только с желанием самовыражения, но и с недостатком жизненного опыта, пренебрежение опасностью, недооценивание возможных рисков.

Вопрос, интересующий многих - чем же грозит утеря пароля от аккаунта? Это почти стопроцентная рассылка спама Вашим друзьям и близким (плюс еще дивизия незнакомых Вам людей).Если Ваш аккаунт взломали, и Вы потеряли над ним контроль, есть большая вероятность, что взломают все почтовые ящики, которые будут там указаны.

Cookies — небольшой фрагмент служебной информации, помещаемый веб-сервером на компьютер пользователя. Применяется для сохранения данных, специфичных для данного пользователя и используемых веб-сервером для различных целей. Они могут сохранять любые пользовательские настройки, например, ключ сессии (без пароля), зашифрованный пароль, комбинацию из зашифрованного пароля и логина. Именно поэтому они могут представлять определенную ценность для злоумышленников.

1. Cookies можно украсть. Проще всего это сделать, имея доступ к пользовательскому компьютеру. Через Интернет-соединение уже сложнее. Кража cookies через Интернет-соединение называется взломом сессии. Хакер, произведший взлом сессии и перехвативший cookies, легко сможет ими воспользоваться, даже не сомневайтесь в этом.

2. Cookies можно подменить. Подменой cookies называется изменение его содержимого (например, количества пересылаемых в Интернет-магазин средств). Подмена cookies происходит непосредственно перед отправкой их на сервер.

Проще всего cookies украсть в местах, наименее защищенных и наиболее массовых (например, кафе с доступом к wi-fi). Самую серьезную защиту Ваших cookies предоставляют защищенные каналы (HTTPS-сессия плюс атрибут «SECURE» у самих cookies).

Фи́шинг (англ. phishing, от fishing - рыбная ловля, выуживание) - вид интернет- мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям. Фишинг можно охарактеризовать как тип компьютерного мошенничества, который использует принципы социальной инженерии с целью получения от жертвы конфиденциальной информации. Киберпреступники обычно осуществляют свои действия при помощи электронной почты, сервисов мгновенных сообщений или SMS, посылая фишинговое сообщение, в котором напрямую просят пользователя предоставить информацию (путем ввода учетных данных в поля сайта-подделки, скачивания вредоносного ПО при нажатии ссылки и т.д.), благодаря чему злоумышленники получают всю нужную для них информацию.

Еще один тип угроз, который мигрировал в социальные сети из систем интернет-банкинга - это программы для кражи паролей. Они внедряют части своего кода в ваш браузер (в основном, в Internet Explorer и иногда в Firefox)

для того, чтобы похитить ваши регистрационные данные до того, как они будут отправлены на сервер.

Если злоумышленнику удастся заполучить ваши регистрационные данные, то, скорее всего, он станет отправлять ссылки, устанавливающие программу для кражи паролей на компьютеры ваших друзей. В результате количество компьютеров-жертв будет расти как снежный ком.

Существует еще один фид угроз- Фарминг, который еще более опасен, чем фишинг. Сначала появился фишинг, а потом (в результате эволюции) - фарминг. Фарминг (от англ. pharming, farming – сельское хозяйство) - это замаскированное перенаправление пользователя - жертвы на ложный IP-адрес. Является более опасным способом мошенничества, чем фишинг.

Для обеспечения информационной безопасности в социальных сетях нужно соблюдать некоторые простые принципы, которые помогут защитить аккаунт:

- используйте защищенный доступ;

- при регистрации используйте сложный пароль;

- при завершении работы в социальной сети выполняйте процедуру выхода;

- не переходите по ссылкам, отправленным в сообщениях, если вы не уверены в безопасности ссылок;

- с осторожностью устанавливайте приложения, ориентированные на работу с социальными сетями;

- осуществляйте смену паролей раз в пол года.

Таким образом, перечислены только самые популярные методы безопасности в известных социальных сетях. Тем не менее, вполне очевидно, как много можно узнать о любом из нас, не отходя от компьютера.

Использованные источники:

1.Виды защиты информации в социальных сетях / [Электронный ресурс] – Режим доступа: https://sites.google.com/site/socialnyeseti94 (Дата обращения: 02.01.2018)

2. Безопасность в социальных сетях / [Электронный ресурс] – Режим доступа: https://whoer.net/blog/bezopasnost-v-socialnyx-setyax/ (Дата обращения: 02.01.2018)