

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой: <https://stuservis.ru/glava-diploma/69442>

Тип работы: Глава диплома

Предмет: Социальная психология

-

Парадокс в том, что мы часто говорим о том, что нас обманывает правительство, нас обманывает пресса, нас обманывают производители и торговцы. И мы действительно ожидаем этого обмана, поэтому ведем себя осторожно, когда общаемся с чиновником, продавцом на рынке или милиционером. Но почему-то, когда дело касается интернета, никто и не думает о том, что его могут обмануть, и это просто удивительно. возможна ситуация, когда вы разговариваете как будто бы со своим другом, которого знаете в реальной жизни, но за компьютером в этот раз сидит не он. Вдруг кто-нибудь взломал пароль, и общается теперь с вами под видом вашего друга, а вы как раз рассказываете что-нибудь очень личное и важное для вас? Или он просто отошел от компьютера, а кто-то сел на его место? Поэтому умные люди, как раньше делали разведчики, договариваются о пароле, то есть о некоем ключевом слове, которое используют в письме так, чтобы понять, что это точно тот самый человек, к которому они обращаются.

Сейчас есть возможность узнать, как выглядит ваш собеседник посредством веб-камеры, можно включить ее и посмотреть, тот это человек или не тот. Очень важна бдительность и понимание, что никогда нельзя давать никакой личной информации ни про себя, ни про других, тому, кого вы не знаете.

А некоторые безумцы еще и непрерывно указывают в соцсети свое местонахождение, порой даже с помощью GPS. Осталось только написать, сколько в ваших карманах денег, под каким ковриком лежат ключи от двери вашей квартиры, и где в ней вы прячете все ваши сбережения...

В психологическом отношении опасен уход от реальности, когда человек большую часть времени начинает думать в понятиях сети, информации в сети, игр в сети? Сейчас ведь очень многие в социальных сетях еще и играют, даже взрослые люди. Множество людей озабочены тем, чтобы вовремя полить виртуальную морковку, которую они никогда не попробуют. Действительно, наша лень приводит к тому, что мы тратим свою жизнь на игры.

Вот ты убивал, и убивал свое время, и вот оно кончилось, а дальше что? А что ты успел сделать? Вырастить две тонны виртуальной морковки? Собрать тысячу виртуальных друзей?

Ценность виртуального общения в том, что оно позволяет быть на связи людям, живущим в различных регионах. Кроме того виртуальное общение облегчает выполнение работы и облегчает жизнь в отпуске, вдали от офиса или дома, в этом есть определенное удобство, но, конечно, это примитив.

Какие ещё опасности таит жизнь в Интернете?

1. Во-первых, фишинг.

Фишинговыми письмами называют поддельные уведомления от имени администраторов, провайдеров и социальных сетей. Цель письма – побудить вас перейти по фальшивой ссылке на фальшивый сайт и ввести свои логин и пароль. Как правило эти фальшивые сайты и адреса имеют очень схожие с официальными и полностью копируют их дизайн и интерфейс.

Например:

<http://vkiontkate.ru/> вместо <http://vkontkate.ru/>

<http://odnoklasniki.ru> вместо <http://odnoklassniki.ru>

После ввода логина и пароля вас перенаправляют на официальный сайт, а ваши данные остаются в руках мошенников.

Защита простая, входите на официальный сайт напрямую, а не по предлагаемым ссылкам. Для защиты от взлома вашей странички тщательно продумывайте пароль и регулярно его сменяйте.

Есть несколько простых рекомендаций по созданию пароля:

- 1) пароль должен содержать от 7 до 20 символов;
- 2) пароль должен содержать буквы как нижнего так и верхнего регистра (т.е. и заглавные и прописные);
- 3) пароль должен содержать цифры и знаки пунктуации (1-9, !@#\$%);
- 4) пароль не должен совпадать с вашим логином (логин – это ваше имя пользователя).

1. Во-вторых, неправомерное использование фотографий.

Даже если свои фотоальбомы в социальных сетях вы блокируете для просмотра, они доступны для людей,

которые могут использовать их в своих интересах. В определённом возрасте некоторым девушкам хочется представляться более старшими и сексуальными и они выставляют на просмотр отдельным категориям альбомы с фотографиями в жанре «ню» (эротического характера). Эти фотографии потом могут появиться на сайтах эротической направленности.

Есть и вторая угроза – эти фотографии могут привлечь внимание людей с нарушенной психикой, что может привести к преследованию со стороны этих людей.

1. В-третьих, информация об отпусках и поездках может привлечь внимание криминал, специализирующийся на квартирных кражах.

2. Интернет-угрозы.

Кроме угроз жизни в социальных сетях существует множество угроз от обычной работы в Интернете.

1. Во-первых, компьютерные вирусы.

На сайтах, предлагающих аудио- или видеопroduкцию часто можно встретить предупреждение, что для прослушивания или просмотра контента необходимо обновить плеер, ссылка на который тут же прилагается. В итоге, вместо обновления плеера (или вместе с ним) вы получаете и вирусную программу, которая может либо блокировать работу вашего компьютера, пока вы по требованию не переведёте деньги и не получите код, или будет копировать всю информацию с вашего компьютера и пересылать ее своим разработчикам. Как быть? Поищите аудио- или видеопroduкцию в другом месте или, при необходимости, скачайте нужную программу на официальном сайте (возможно пробную версию).

Выводы.

В рамках одного урока рассмотреть все опасности, которые таит медиа-пространство, невозможно.

Если обобщить все угрозы, затронутые нами сегодня, то можно сделать вывод, что Интернет – это минное поле, где невнимательность и скоропалительность может привести к серьёзным проблемам, касающихся вас лично и ваше окружение.

Существует несколько простых правил, которые смогут если не обезопасить полностью, то значительно снизить угрозы:

1. Пользоваться антивирусом. Современный, регулярно обновляемый антивирус обеспечит надежной защитой от разнообразных интернет-угроз.

2. Регулярно загружать обновления: обновления программ закрывают уязвимости, которыми могут воспользоваться злоумышленники.

3. Не оставлять своих персональных данных на открытых ресурсах: данные, оставленные в интернете, собирают роботы злоумышленников, которые в дальнейшем могут использовать их в своих целях (например, присылать на ваш почтовый ящик больше спама).

4. Не загружать ничего со случайных сайтов: высока вероятность того, что вместе с загруженной программой/книгой/фильмом вы получите и вредоносную программу.

5. Не проходить по ссылкам в спамовых письмах: такие ссылки зачастую ведут на мошеннические, либо заражённые вредоносными программами сайты.

6. Не открывать приложения в письмах, если есть хоть какие-то сомнения в надёжности адресанта. Высока вероятность того, что в приложении содержится вредоносная программа (даже если это документ Word).

7. Не пытаться «отписаться» от спама (особенно в том случае, когда в спамерском письме есть соответствующая ссылка). Избавиться от спама это не поможет, скорее наоборот. Существуют два наиболее вероятных варианта развития событий: 1) спамеры регулярно запускают автоматическую проверку и чистку своих баз от несуществующих адресов; отвечая на письмо, вы подтверждаете, что ваш адрес (который, был, возможно, подобран автоматически) действительно существует, его действительно читают. Это побудит спамеров внести его в отдельные, «чистые» базы, вследствие чего вам будет приходить ещё больше спама; 2) пройдя по ссылке, вы попадете на заражённый сайт и получите вредоносную программу на свой компьютер.

8. Не откликаться на заманчивые предложения, особенно если они связаны с получением быстрых денег. Откликнувшись, вы или потеряете свои деньги, или, что гораздо хуже, окажетесь замешаны в преступные махинации.

2) Во-вторых, опасные сайты.

Существуют сайты, направленные на пробуждение в человеке низменных чувств, противопоставлению обществу и общественным нормам, ведущих человека в зависимость от разработчиков этих сайтов. Это порносайты, формирующие извращенное представление о сексуальных отношениях, ставящих плотское выше духовного).

Это онлайн-игровые сайты, ведущие к отрыву от реальности и социофобии.

Это экстремистские сайты, разжигающие ненависть и рознь. Подобные сайты через образ врага (виноватого во всем) предлагают поднять собственную

-

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой: <https://stuservis.ru/glava-diploma/69442>