23. НЕБЕЗОПАСНЫЕ САЙТЫ И СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Карабаш К. А. студент гр.272302, Раптунович О.М., ассистент кафедры ЭИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ефремов А.А. – канд. эк. наук, доцент кафедры ЭИ

Аннотация. В наше время есть место, где можно найти любую информацию, называемое всемирной паутиной или интернетом. Поскольку не все люди знают и придерживаются правил безопасности в интернете, я хочу рассказать про интернет-мошенников, которые ищут для себя таких неосторожных пользователей и «крадут» личные данные или шантажируют и как следствие выманивают деньги. В этой работе я подробно рассмотрела самые популярные «ловушки» и рассказала, как обезопаситься от них, чтобы не попасть в руки аферистов.

Ключевые слова. Примеры самых распространенных «ловушек» в интернете, способы защиты от интернет-аферистов.

В современном мире очень сложно найти человека, который никогда не «заходил» во всемирную паутину. Логично, фактически в интернете можно найти абсолютно всё: обычные новостные сайты, работу с приложениями интернет-банкинга, использование развлекательных ресурсов, скачивание файлов (программ) и т.п.. С одной стороны эта возможность облегчает жизни большого количества людей, с другой даёт возможность мошенникам зарабатывать на неосторожных пользователях. Но вам не стоит бояться интернет-аферистов, ведь по итогам моей работы у вас появится информация на основе моих исследований о популярных сайтах, где люди попадают в «сети» мошенников, а «любое знание может быть оружием как нападения, так и обороны».

1. Фишинг.

Любой пользователь социальных сетей постоянно сталкивается с понятием фишинг, когда мошенники скидывают ссылку на сайт, похожий на оригинал, с целью получения необходимых данных для «угона» аккаунта. Звучит всё очень просто, но как же интернет-аферисты получают эти данные? Действуют мошенники очень просто и однообразно: создают сайт клон, похожий на какой-либо (например, ВКонтакте), далее делают масштабную рассылку пользователям оригинальной социальной сети ВКонтакте с предложением пройти какой-то опрос, узнать свою тайную любовь и т.п. Неосторожный пользователь переходит по ссылке и не замечает, что сайт «подменили», вводит свои личные данные при входе в свой аккаунт. В это время мошенникам автоматически приходит логин и пароль, который был введен на неоригинальном сайте, и они получают доступ к этому аккаунту. После следуют шантажи и/или рассылки разных форматов.

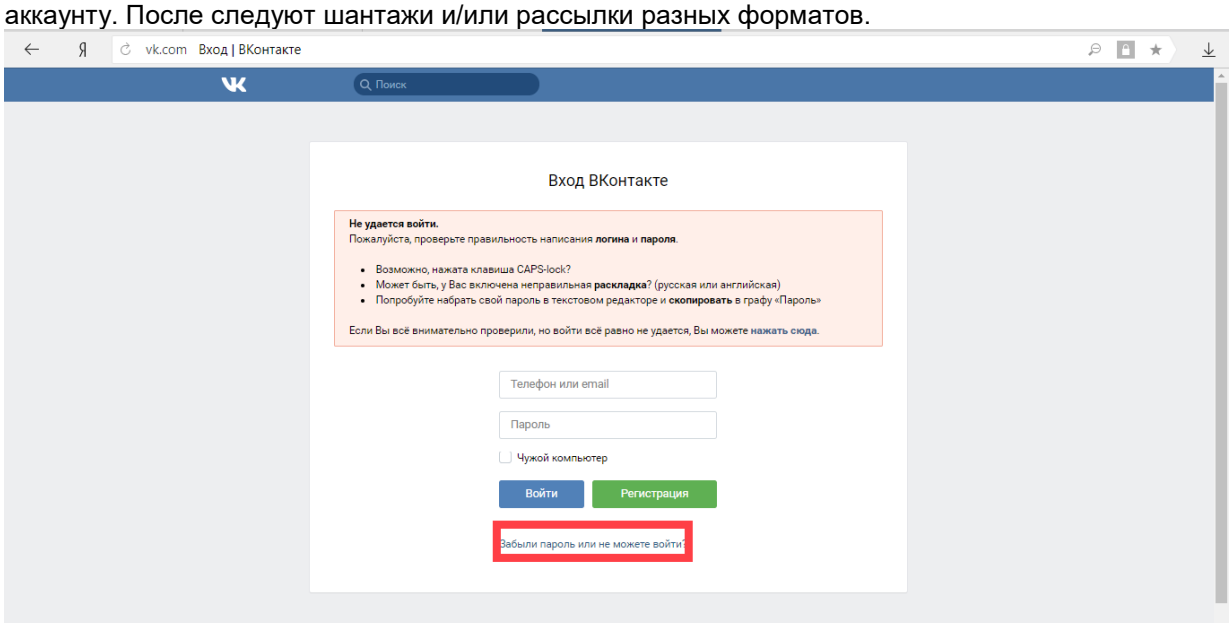

Рисунок 1 - Пример оригинального сайта ВКонтакте.

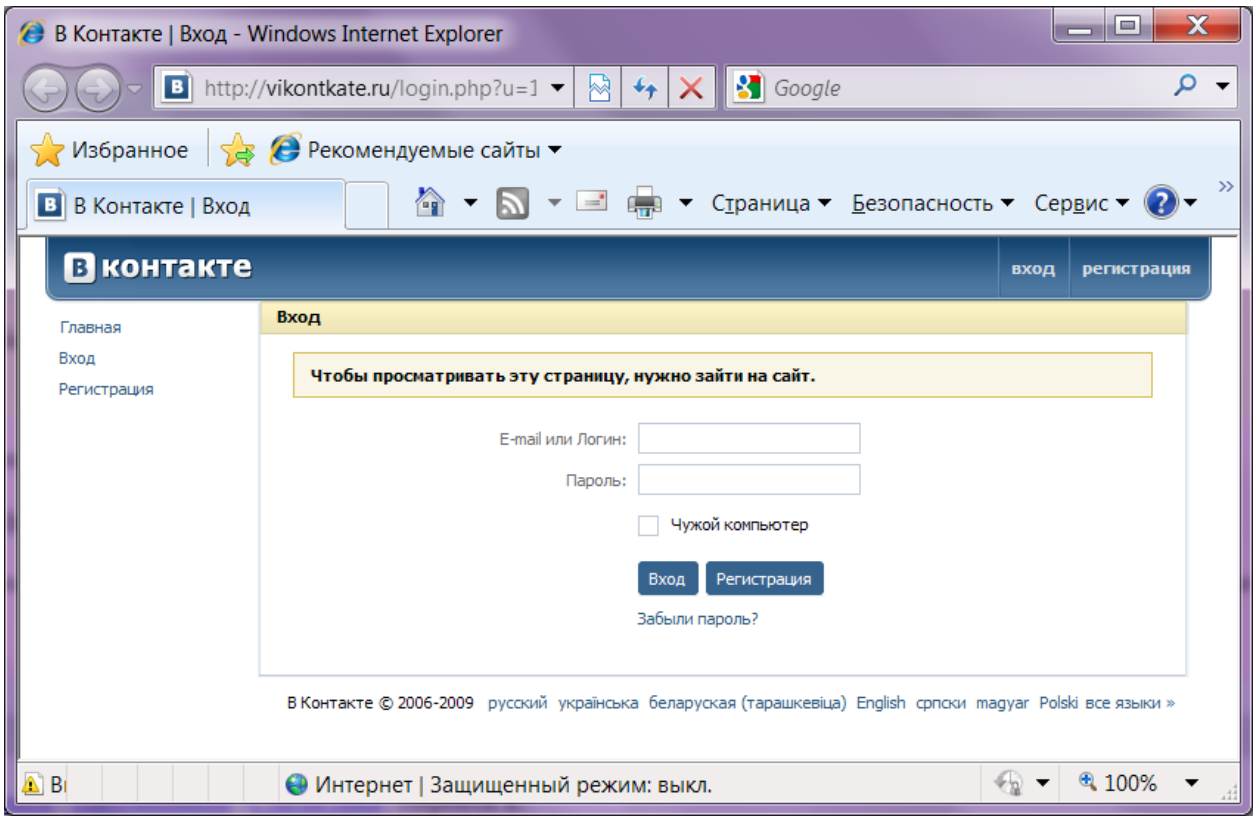

Рисунок 2 - Пример фишингового сайта ВКонтакте.

Способов обезопасить себя от различных фишинговых сайтов очень много. В основе пользования интернета лежит правило, связанное с ссылками от незнакомых пользователей. Так как первопричиной всех таких бед является переход по небезопасной ссылке, пользователям необходимо проверять их. Если вы уверены в человеке, то после попадание на какой-либо сайт по его ссылке, вам стоит посмотреть на адресную строку сайта (текстовое поле для ввода поискового запроса или для ввода адреса страницы в интернете) и сверить её с оригинальной. Друга также могли взломать злоумышленники, поэтому нельзя «слепо» переходить по всем ссылкам и вводить свои данные. Если вы ввели данные, а после заметили, что с сайтом что-то не так, следует немедленно сменить пароль на оригинальном сайте. В некоторых социальных сетях можно поставить двухэтапную аутентификацию.

Такие способы мошенничества могут быть не только в социальных сетях. Интернет-банки, аккаунты в играх, вообще любые интернет-аккаунты могут заинтересовать интернет-аферистов, которые постараются ими завладеть. Будьте бдительны!

2. Торрент.

Все люди любят экономить там, где это возможно. В интернете это делать очень просто, находя платный материал в разы дешевле или совершенно бесплатно. А если совсем не хватает времени на поиск, то можно использовать уже готовую технологию поиска – торрент. Кажется, что может произойти, если специальная технология будет искать что-то по моему запросу?

Принцип работы торрентов заключается в поиске файлов во всемирной паутине. Данные файлы не проверяются, таким образом человек сам даёт согласие на скачивание опасных вирусов на свой компьютер. С одной стороны, пользователь может проверять каждый файл на наличие в них вирусов, но смотря правде в глаза, сколько файлов он так проверит и проверит ли хотя бы один? При скачивании файлов из торрентов пользователю высвечивается предупреждение о том, что где-то, среди множества скачиваемых файлов есть вирус [3], но обычно человек просто игнорирует данное предупреждение, а после старается любыми способами спасти свой компьютер.

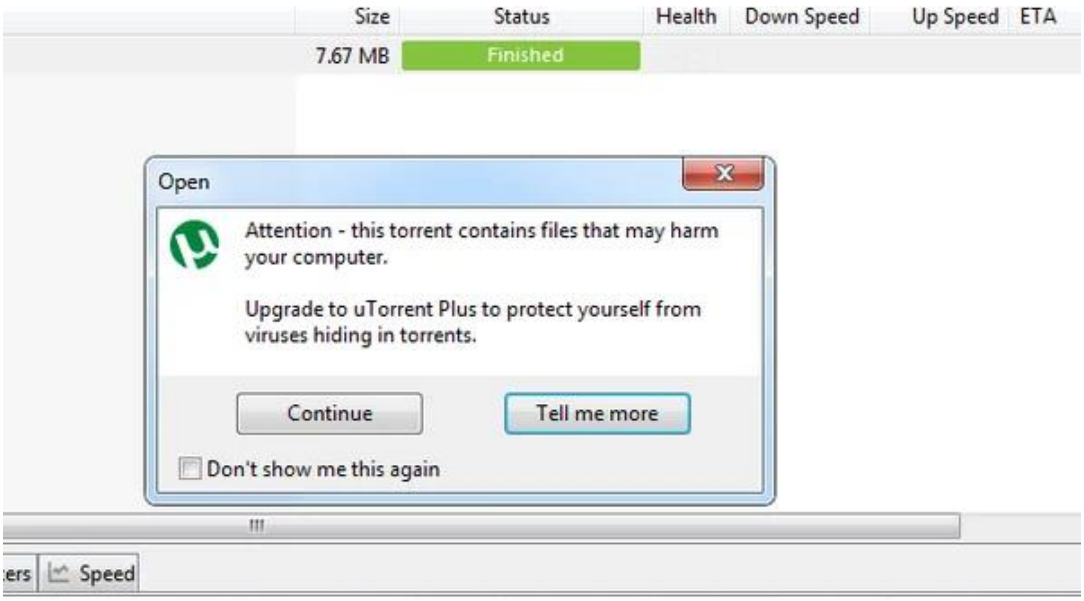

Рисунок 3 – Предупреждение о вредоносной программе внутри файла.

К сожалению, нет 100% способа обезопасить себя от таких вирусов, но есть рекомендации, которые смогут уменьшить риски до минимума. Первостепенно стоит использовать уже проверенные торрент-трекеры. Если вы хотите впервые ими воспользоваться, то стоить уделить время изучению этого сайта, прочтения большого количества комментариев и отзывов других пользователей. Если вы попали на какой-то непопулярный сайт, и он вас смущает – лучше не испытывать судьбу на себе, а найти более проверенный источник. В дополнение к вышесказанному, хочу подчеркнуть, что существует множество платных торрентов или продвинутых версий, которые сразу проверяют файлы на безопасность при помощи антивируса.

3. Файлообменники.

Представим ситуацию: у меня есть огромный файл, который надо скачать моему другу. Конечно, можно пойти сложным путем, где будет использоваться, к примеру, флешка, но проще скинуть этот файл куда-то в сеть и предоставить доступ своему другу при помощи ссылки. Данное действие будет выполнено при помощи файлообменника.

Интернет-аферисты знают про такие ссылки и способы загрузки данных в сеть и используют свои знания против неаккуратных пользователей. К примеру, была сделана большая рассылка, где мошенник получил доступ к такому хранилищу. Находясь «внутри», он мог загрузить туда вирусное приложение. Другие пользователи не будут даже догадываться, что с «облаком» знакомого что-то может быть не так и просто скачают. Страшнее, если пользователь скачивает софт, после чего компьютер вовсе отказывается работать.

Как же предостеречь себя от мошенников? Если сделать вывод с вышесказанного, то понятно, что сама угроза для пользователей заключается в вирусах. Нельзя предоставлять доступ к своему хранилищу малознакомым людям. Периодически обновлять ссылки на общие ресурсы и пароли доступа к разным интернет-ресурсам. Стоит использовать проверенные виртуальные хранилища и обращать внимание на расширение файлов. К примеру, скачивая обычный текст расширение *.bat будет наталкивать на мысль, что это системный файл, следовательно там скорее всего будут различного формата вирусы.

После проведения такого мини исследования, я могу сделать вывод: в интернете надо быть бдительным, всегда проверять сайты, на которых оставляете личные данные, минимально скачивать файлы и всегда их проверять.

Список использованных источников:
1. Какие сайты могут быть опасны и как их посещать | Блог «Электронного города» | Дзен (dzen.ru)
2. Фишинг — Википедия (wikipedia.org)
3. µTorrent — Википедия (wikipedia.org)
4. Как защитить аккаунт ВКонтакте от взлома и спама | Блог Касперского (kaspersky.ru)