

Безопасная работа в социальных сетях: общение, публикация материалов

"Презентация подготовлена для конкурса
"Интернешка" <http://interneshka.org/>".



- **Правила безопасной работы**
- Социальные сети, такие как Facebook, Одноклассники, ВКонтакте, пользуются большой популярностью. Это привлекает мошенников. Используя механизмы социальных сетей, злоумышленники распространяют вредоносное программное обеспечение, собирают персональные данные о пользователях.

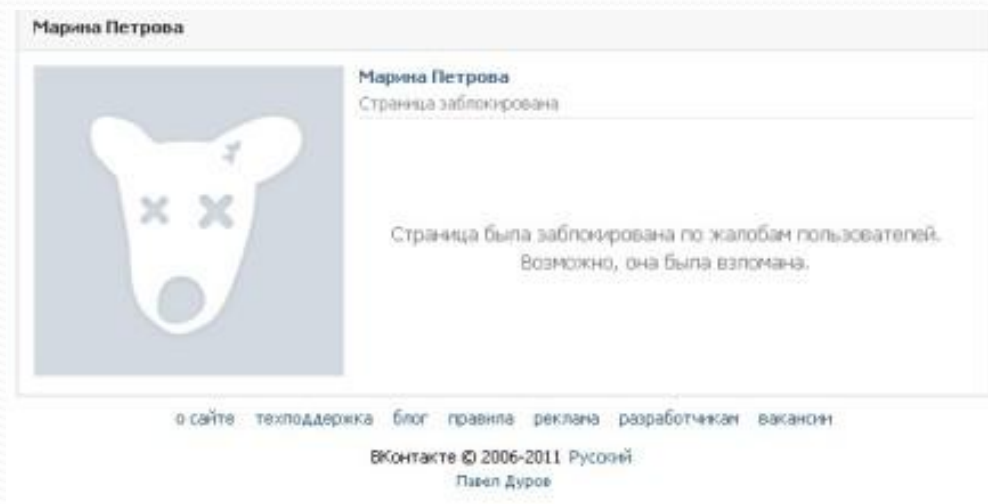


- Огромное количество пользователей – это как раз то, что нужно мошенникам. Ведь чем больше потенциальных жертв, тем скорее они получают заветную прибыль. А именно это является главной целью, которую преследуют все без исключения злоумышленники, орудующие на виртуальных просторах. Арсенал применяемых способов мошенничества все время расширяется. Однако можно выделить основные излюбленные методы обмана доверчивых пользователей.



Спам.

Через взломанные страницы мошенники рассылают ссылки на вредоносные сайты и зараженные файлы. Делается это при помощи личных сообщений или посредством публикации статусов, содержащих прямые или сокращенные ссылки на ресурсы, содержащие вирусы. Вы даже можете получать подобные сообщения от своих друзей с приписками дружеского характера. Это значит, что ваши знакомые, в свою очередь, стали жертвами интернет-мошенничества, и их аккаунты были взломаны.



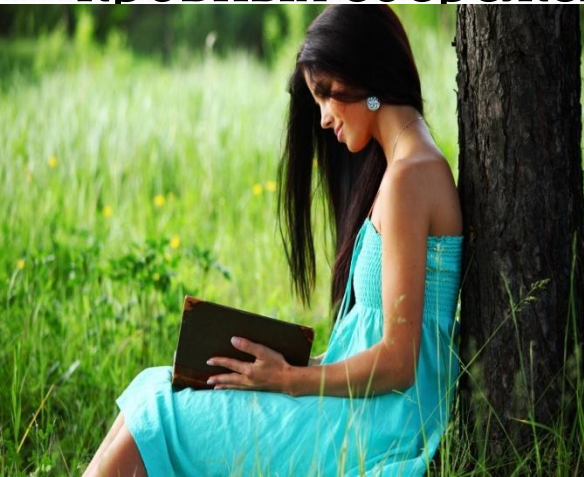
● Никогда не переходите по подозрительным ссылкам, а если такие сообщения присланы от имени ваших друзей, обязательно сообщите им об этом. Возможно, человек даже не подозревает, что его страница взломана.

Еще один способ, которым пользуются аферисты – рассылка сообщений от имени администрации ресурса с сообщением о том, что ваша страница заблокирована. Естественно, для разблокировки вас попросят отправить смс-сообщение, за которое с вас снимут определенную сумму денег.



● Виртуальные знакомства.

В социальных сетях люди часто знакомятся и продолжают общение уже в реальной жизни. Этим часто пользуются мошенники. Распространенная схема обмана заключается в том, что аферисты создают страницу в социальной сети, иллюстрируя её красочными фотографиями, и начинают активно знакомиться с потенциальными жертвами. Через какое-то время, заинтересованные поклонники начнут требовать встречи. Как раз этого и ждут авантюристы. Далее следует слезливая история о временных финансовых трудностях и просьбы помочь. Сердобольные, ничего неподозревающие, но уже влюбленные жертвы, легко ведутся на такой простой способ выманивания их кровных сбережений.



● Призывы о помощи.

Социальные сети переполнены различными просьбами о помощи. Люди просят собрать деньги на лечение, помочь бездомным животным и пр. Будьте осторожные, среди таких историй есть мошеннические. Как распознать по-настоящему человек просит помощи или же это просто способ заработать на милосердии других? Главное правило: проверяйте информацию. В мошеннических сообщениях её всегда крайне мало и кроме телефона нет никаких конкретных данных. Телефон и является способом получения незаконной прибыли. Позвонив по номеру, с вашего счета спишется определенная, зачастую довольно крупная, сумма, поскольку мошенники привязывают его к коротким premium-номерам.

Настоящие призывы о помощи содержат подробную информацию: фамилия, имя, отчество нуждающегося, его место жительства, информация о родственниках, лечебном учреждении, номера лицевого счета для помощи.



● Взлом аккаунта.

Выше мы говорили о том, что мошенники часто взламывают аккаунты для рассылки спама. Чтобы защитить свою страницу, старайтесь, чтобы ваш пароль был довольно сложным и не содержал явных комбинаций. Никогда не вводите свой пароль и логин от аккаунта в социальной сети по требованию сторонних ресурсов. Если на каком-то сайте, вас просят занести в анкету логин или пароль от личной странице, знайте, что этот сайт занимается мошенничеством.



Не привязывайте к своим аккаунтам номера кредитных карт.

Всегда помните, что вашу страницу могут взломать, поэтому старайтесь не размещать в социальных сетях сугубо личную информацию, не предназначенную для посторонних.

Помните, что многих проблем можно избежать, если проявлять элементарную осторожность и бдительность. Чтобы не стать жертвами мошенников, достаточно просто более ответственно подходит к вопросам конфиденциальности личной информации, и быть бдительными при общении с незнакомыми людьми.



Выполнила Антипова Валерия Вадимовна. Город
Смоленск Село Печерск.

Спасибо за внимание!

