Автор: **Заренок Н. В.** Студент 1 курса Академии маркетинга и социально-информационных технологий – ИМСИТ (Краснодар)

Соавтор: **Стафеев А. В.** Студент 1 курса Краснодарского информационного технологического техникума - КИТТ «Банковское дело»

НЕОБХОДИМОСТЬ ИНТЕРНЕТ-БЕЗОПАСНОСТИ

Актуальность: данная проблема распространяется абсолютно на всех пользователей сети- Интернет. В связи с тем, что все пользователи сети-Интернет являются разных возрастных групп, стоит обратить большую часть внимания на пользователей-несовершеннолетнего возраста и на людей старших возрастов, так как они подвергаются большей угрозе или не подозревают о ней как таковой. В связи с чем он подвергается стрессу, в следствии чего может возникнуть эмоциональное или же психическое расстройство, что повлечёт угрозу здоровью. Не всё общество подозревает о том, что незнание закона не освобождает нас от ответственности, что может повлечь за собой нарушение закона по незнанию.

Ключевые слова: защита, здоровье, угроза, данные, сеть-Интернет, несовершеннолетние, общество, люди, пользователи, психическое расстройство, стресс, злоумышленники, эмоциональное расстройство, закон, ответственность, преступление, хакер, информация.

В наше время «атаке» злоумышленников подвергаются чаще всего несовершеннолетние и люди старших возрастных групп. Хакеры и злоумышленники пользуются незащищенностью интернет-данных пользователей, а также их наивностью и глупостью. Они могут представиться в виде представителей работников банка, различными организациями, фирмами, компаниями и другими учреждениями, используя при этом рассылку вредоносных сообщений, спама, ссылок, а также пользуясь уязвимостью

некоторых программ, заполучить личные данные интернет-пользователей и причинить вред технике с помощью вирусов.

Существует очень много способов защиты данных с помощью паролей, антивирусов, кодировок и т. п., но нет ни одной безопасной системы. Вследствие чего происходит хищение данных. Из-за этого человек может испытывать стресс, эмоциональные расстройства или же психические, которые могут причинить ущерб здоровью и привести к различным заболеваниям. Человек может как подвергаться физическому насилию, а также проявлять агрессию по отношению к другим и может пойти на необузданные поступки о совершении которых может пожалеть. Человек может совершить преступное деяние сам не зная этого или же совершить это намеренно, например, взломав чью-то страницу или же опубликовав фотографию другого человека, который был против этого, на эмоциях мог взломать сайт какой-нибудь организации и украсть данные, помочь преступникам и так далее. Хакеры или злоумышленники могут взломать вас, или же украсть ваши данные и использовать их в своих намерениях.

В случаях, когда человек подвергается стрессу, эмоциональному или психическому расстройству, ему сложнее справляться со своими ежедневными задачами, своей работой и с адаптацией в обществе, а так же люди становятся легкой добычей для мошенников, готовых прибегнуть к шантажу. При использовании сети Интернет люди ежедневно сталкиваются с информационными проблемами, по этому людям стоит обдумать и изучить то, с чем они могут столкнуться, чтобы в будущем, они могли использовать свои знания и защитить себя от каких-либо угроз. Особенное внимание изучения интернет материала стоит уделить малолетним пользователям и пользователям старших возрастных групп, если заранее хоть как то подготовиться, можно избежать множество проблем или справиться с имеющейся угрозой.

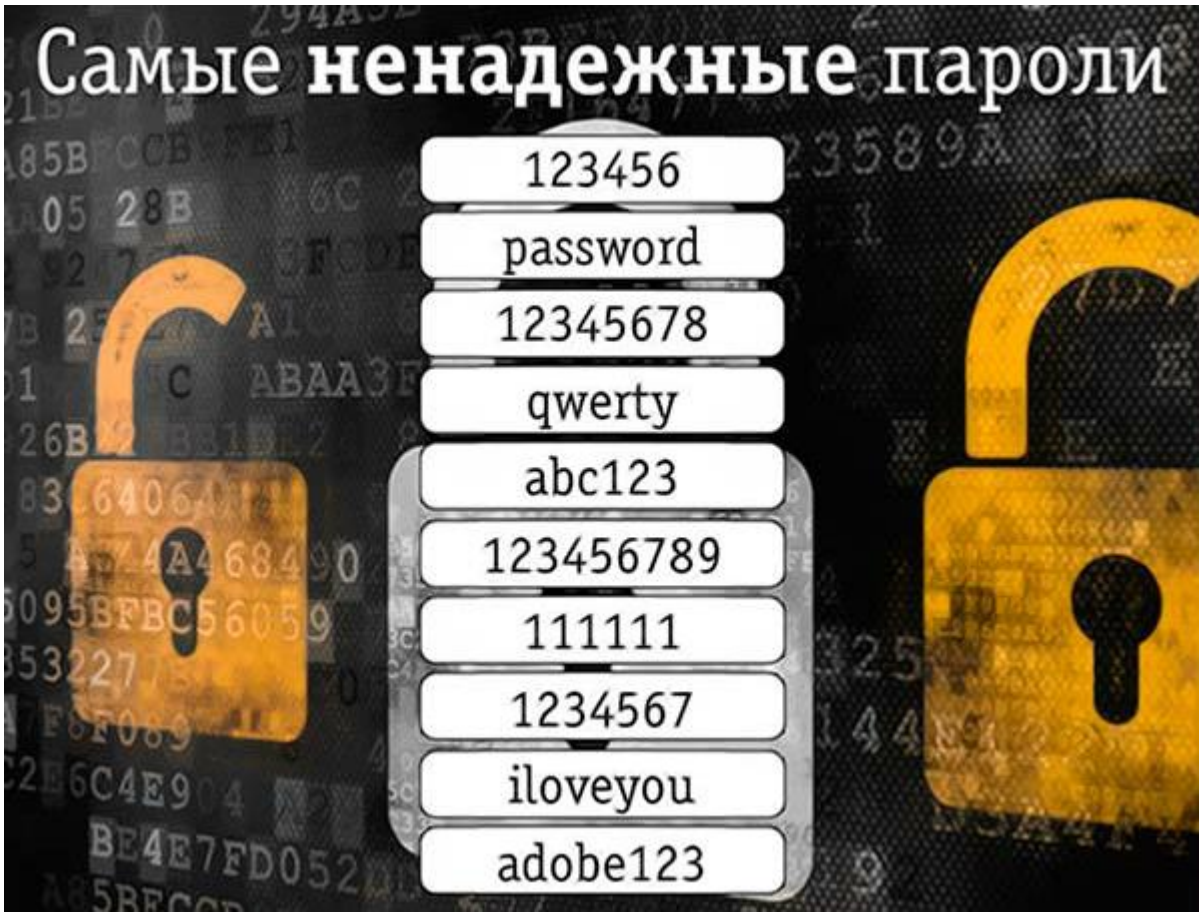
Приведем несколько примеров:

1. **Взлом страницы социальной сети, кража и использование личной информации пользователя.**

Открыв социальную сеть «ВКонтакте», во вкладке «сообщения» вы заметили новое сообщение от неизвестного вам пользователя, содержащее ссылку на неизвестный вам сайт. По незнанию, а может в связи со своей любопытностью вы перешли по этой ссылке и угодили в ловушку злоумышленников, в следствие чего, последние получили доступ к вашим личным данным и управлению учетной записью. В таком случае ваша информация скорее всего будет использована во вред вам и вашим близким, для получения злоумышленниками материальной выгоды. Информация может быть как маловажной, так и более ценной.

Для того, чтобы не попасть в данную ситуацию, нужно:

1) Не сообщать свои пароли никому и ни в коем случае.
2) Не переходить по незнакомым вам ссылкам.
3) Не предоставлять свою информацию незнакомым, или малознакомым людям.
4) Использовать только надежные, или сложные пароли.
5) Не подключаться к подозрительным сетям.



И тому подобное

Что делать, если вас все же взломали? В таком случае нет ничего сложного, нужно лишь:

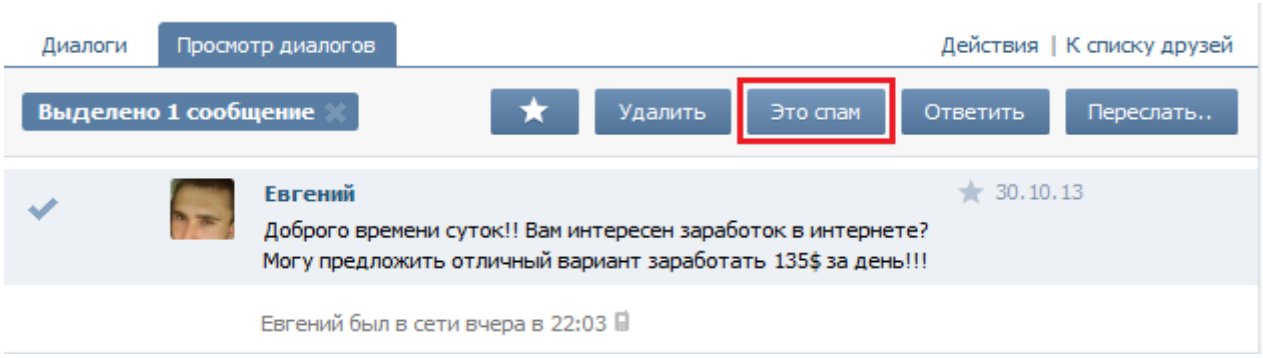
1) Временно удалить свою страницу, так злоумышленники не смогут воспользоваться информацией, содержащейся на ней.

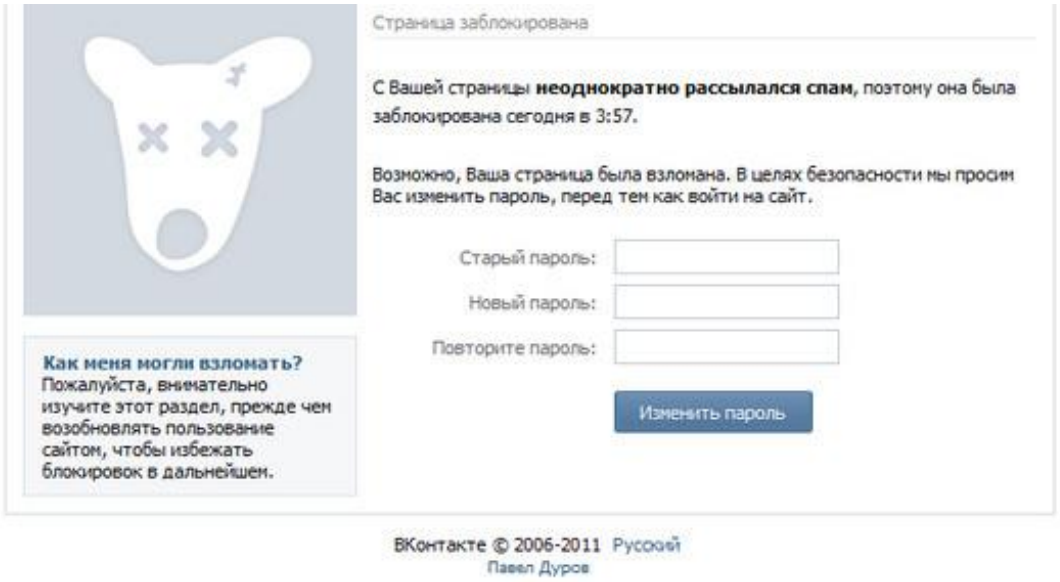
2) Восстановить свою страницу с заменой пароля.

3) В случае возникновения каких-либо сложностей, обратиться в службу поддержки данной социальной сети.

4) Проверить свои данные после восстановления страницы.

5) Проверить диалоги на наличие вредоносных, либо спам рассылок пользователям, иначе вас могут повторно заблокировать.





2. Хищение особо ценной информации, такой как: банковские счета, документация в электронном виде и т. п.

В поисках нужной информации вы перешли на сайт и случайно скачали файл, содержащий вредоносное Программное Обеспечение, после чего, злоумышленник получил доступ к информации, содержащейся на вашем компьютере, либо гаджете. Среди этой информации, большей угрозе подвергаются банковские счета; документация, содержащаяся в электронном виде; пароли. С помощью этих данных, злоумышленник может снять с вашего счета деньги, оплатить что-либо, воспользоваться вашими документами для

получения собственной выгоды.

Для того, чтобы не попасть в данную ситуацию, нужно:

1) обзавестись защитным Программным Обеспечением, таким как антивирус.

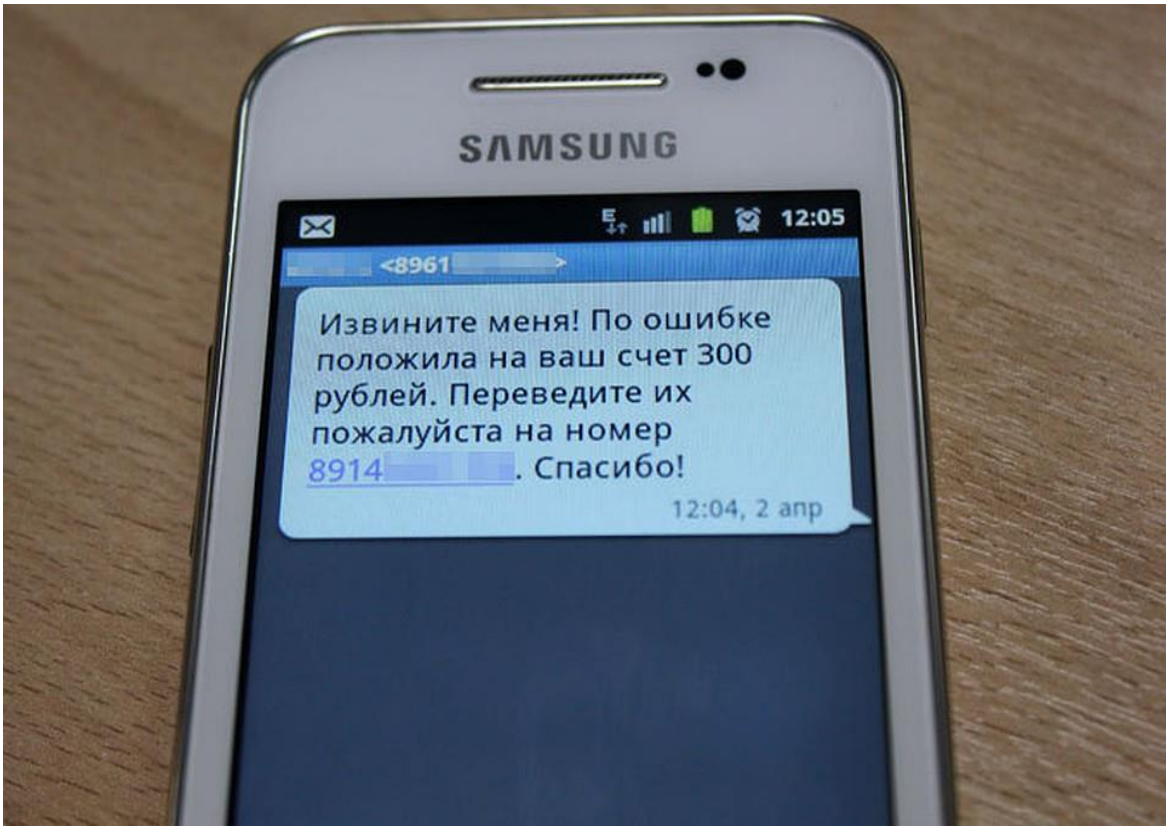
2) Не скачивать подозрительные файлы, с подозрительных сайтов.

3) Всегда читать условия соглашения использования ПО.

4) Не отвечать на подозрительные сообщения с неизвестных номеров.

5) Не предоставлять важную личную информацию людям, представляющимся сотрудниками каких-либо организаций или социальных служб.

6) Никому не предоставлять информацию о своей карте, ни ее номер, ни CCV.



Что делать в случае кражи особо важной информации?

Здесь уже сложнее, чем в случае взлома аккаунта социальной сети.

1) Связаться с банком, заблокировать карту.

2) Посетить банк, чтобы получить детализацию счета, копию заявления на блокировку карты и копию договора с банком.

3) Обратиться в полицию, предоставить полученные в банке документы и все возможные доказательства.

4) Если банковский счет попал в руки злоумышленников по вашей вине, или же банк не признает данные махинации мошенничеством, готовьтесь к судебному разбирательству.

3. **Кража личной информации в целях выманивания денежных средств путем шантажа.**

Злоумышленник завладел материалами интимного характера с вашим участием, и грозится распространить этот материал, пустив его в свободный доступ, если вы не переведете ему указанную сумму денег.

Для того, чтобы обезопасить себя от данной ситуации, необходимо:

1) Держать важные личные данные под надежной защитой, используя многоуровневые пароли.

2) По возможности, не хранить важную, либо личную информацию, которой злоумышленник может воспользоваться для шантажа, в облаке, или подобных онлайн хранилищах, либо на незащищенных устройствах.

3) Не предоставлять важную личную информацию никому, без исключений.

Что делать, если вы все же подверглись шантажу:

1) Не поддаваться панике.

2) Спокойно реагировать на угрозы шантажиста, не идти у него на поводу, чтобы он подумал, что данная информация не имеет для вас ценности и тогда, он возможно, отступит.

3) Сохранить любые доказательства шантажа, будь то переписки, либо звонки.

4) Обратится в полицию со всеми доказательствами шантажа.

5) Приготовиться к судебному разбирательству в случае необходимости

В следующей статье, те же авторы раскроют тему работы различных специализированных служб в информационной области и кибербезопасности.

Информация, фото-видео материал для подготовки статьи взяты из открытых источников в сети Интернет, СМИ, социальных сетей.

Статья отражает мнение авторов.
Цель проинформировать молодежь о безопасном использовании интернета, соблюдение законодательства и этических норм, а так же предупреждение и профилактика негативных явлений, киберпреступности с использованием компьютерных технологий и интернета.

Возрастная категория статьи 16+