Безопасная работа в социальных сетях: общение, публикация материалов

# Моя страничка – моя крепость!

Презентация подготовлена для конкурса

Выполнила: ученица 11 А класса
Смирнова Дарья

В XXI веке человек, не пользующийся социальными сетями – большая редкость. Личными страничками обзавелись люди всех возрастов: от совсем маленьки

Конечно, социальные сети – очень удобная вещь, но не стоит слишком

Ваша личная информация может стать оружием в руках мошенников против вас самих.

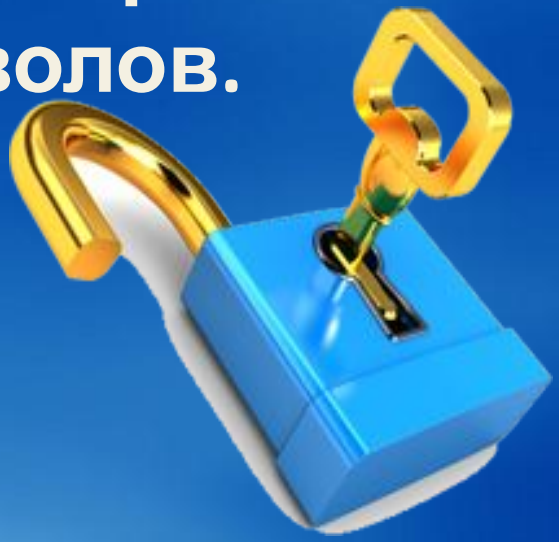
Чтобы не стать жертвой кибермошенников, нужно придерживаться нескольких правил…

1

# Используйте надежный пароль!

Рекомендуемая длина – 8 и более символов. Идеальный пароль – сочетание латинских букв разного регистра, цифр и спецсимволов.

Например: 6%d9QS~5f



Я убедилась в этом на личном опыте. Моим паролем была дата рождения, поэтому мошенники без труда взломали страницу и стали рассылать спам. Вскоре профиль был заморожен администратором, и я восстановила доступ.

# Никогда не используйте в качестве пароля:

- Дату рождения. Наверняка она указана в ваших личных данных
- Номер телефона
- Фамилию, имя , кличку животного
- Очевидные пароли, например, «qwerty», «12345», «пароль» и тому подобное

2

Если вам нужна **супербезопасность** – включите двухфакторную авторизацию. Кроме логина и пароля система требует ввода PIN-кода. Такой вариант может показаться не более безопасным.

3

# Контролируйте информацию о себе, которую вы размещаете.

Любой пользователь может сохранить себе ваши фотографии, видео, контакты и другие сведения.

Все чаще HR—рекрутеры пользуются соц. сетями, чтобы прояснить прошлое своих соискателей. Так что провокационные фото и видео могут лишить вас работы.

4

# *Меньше аккаунтов – меньше проблем*

**Многие пользователи создают свои странички где попало. Регистрируйтесь в социальных сетях, которыми точно будете пользоваться. Вы забудете о страничке, а информация останется ступной для мошен**

5

# Добавляйте в «друзья» тех, с кем лично знакомы.

## Неизвестных вам людеи оставьте в «подписчиках», за красивой аватаркой может скрываться кто угодно

Странно думать, но рабство до сих пор существует. Россиянину Максиму Р. друг по переписке в соц. сети предложил подработать в Узбекистане, пообещал оплатить все расходы. В итоге мужчина попал в трудовое рабство и через несколько месяцев чудом сбежал.

6

# Не переходите по неизвестным ссылкам.


Если возникает надпись: «Для получения подробной информации перейдите по ссылке…», задумайтесь. Ваш компьютер может быть заражен вирусом, как минимум.

7

# Пользуйтесь закладками

Существует множество сайтов – клонов, например «faceboook.com» вместо «facebook.com». Они вытягивают личную информацию из невнимательных пользователей.

8

**Будьте осторожны при установке приложений.**

**Любая соц. сеть предлагает пользователю богатый выбор дополнений, которые расширяют возможности вашей страницы. И передают информацию мошенникам.**

**Вы установили приложение «Мои гости» и надеетесь узнать, кто и когда посетил вашу страницу. Ничего подобного. Вас попросят отправить пару сообщений на указанный номер и будут регулярно снимать кругленькую сумму.**

**Часто мошенники пользуются неравнодушными людьми и простят перечислить на счет некоторую сумму денег.**

**В такой ситуации сразу обращайтесь в**

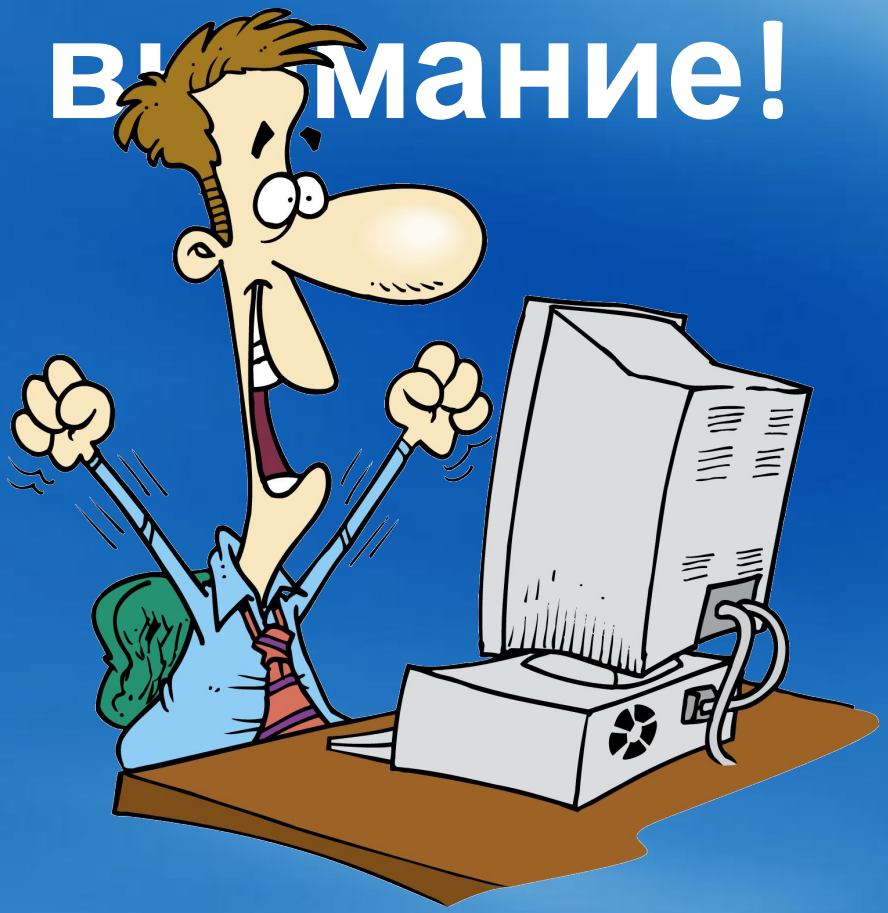


После трагедии с Airbus A321 злоумышленники создали в «Вконтакте» фейковую группу помощи близким погибших в авиакатастрофе. Они указали реквизиты для «Яндекс-деньги», номер кредитной карты и прочее, чтобы у жертв был выбор, как перечислить деньги мошенникам. Сейчас сообщество закрыто.

*«Осторожнее с тем, что вы постите на Facebook. Что бы это ни было, это еще всплывет когда-нибудь в вашей жизни»*

*«Все идет через сервера в США. Такова жизнь. Так она выстроена американцами. Все это возникло на заре интернета как спецпроект ЦРУ. Поэтому, для безопасности серверы крупных компаний должны быть*

# Спасибо за внимание!



Презентация подготовлена для конкурса «Интернешка» http://interneshka.org/