Безопасное использование социальных сетей

Что нужно знать:

- Поменьше активности в Интернете. Если же что-то разместить или написать очень хочется, то важно, чтобы это не касалось демонстрации или одобрения фашизма, нацизма, радикальных религиозных течений, сект; унижения или агрессии к любым людям по национальности, расе, вере, полу, социальной группе.

Осторожнее в обсуждениях политики!

В Интернете вы не у себя дома, а посреди Красной площади в толпе людей.

Почти все крупные сайты зарегистрированы как СМИ, а значит, любой ваш комментарий на таком сайте будет оцениваться как доступный для всех, что будет учтено при его оценке органами.

- «Лайк» песни или видео, репост того, что понравилось на свою страницу - это уже распространение. Рекомендуем всем повторно изучить свою страницу, и если нужно - почистить. Если не уверены в законности того, что у вас размещено, смело удаляйте!

«ВКонтакте» активно сотрудничает с правоохранительными органами.

Закрытая страница - не спасение

Были случаи возбуждения дела из-за картинок, пропагандирующих насилие, фашизм, наркотики , фейковую информацию, в альбоме «только для своих»

ОБЪЯСНЯЕМ.РФ

ПРЕДУПРЕЖДАЕМ,
что за создание и распространение фейковых новостей предусмотрена
УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ!

Не поддавайтесь на провокации

Вы – наше будущее!
Будьте сильными!
Берегите себя.!
Помните, что мы живем в великой стране, с великой историей и великой культурой!

В помощь тем, кто хочет получать достоверную информацию, в России запустили сайт «Объясняем.РФ». Сообщения только проверенные, никаких слухов. Также на портале отвечают на самые горячие вопросы, которые волнуют россиян. И главное — разоблачают фейки, которые сейчас активно распространяют через интернет под видом правды.

ОБЪЯСНЯЕМ.РФ
Достоверно и наглядно о том, что важно прямо сейчас

http://serp-koll.ru

Министерство образования Московской области

Профессиональное образование Московской области

ГБПОУ МО "Серпуховский колледж"

СТОП ЛЖЕНОВОСТИ

Безопасное использование социальных сетей

http://serp-koll.ru

Безопасное использование социальных сетей

Интернет и социальные сети стали частью нашей жизни. Важно помнить, что Интернет - общественное место, в котором есть правила поведения, которые нужно соблюдать.

Последние несколько дней российские пользователи соцсетей столкнулись с самым настоящим психическим террором.

Обращаемся к вам с просьбой: быть максимально внимательными и не верить новостям в соцсетях. Вполне вероятно, что то, что вас напугало — это продукт фабрики фейков.

В связи с расширением фронтов информационной и кибервойны предлагаем вам небольшую памятку-ликбез по цифровой безопасности и основным векторам атаки на пользователей интернета.

БОТЫ. Прямой взлом аккаунта

БОТЫ

Самая безобидная, на первый взгляд, угроза в списке. С ботами мы сталкиваемся каждый день - их используют для накрутки рекламных постов, оставления положительных или негативных отзывов. Сейчас боты используются для распространения пропаганды и фейков.

В данном случае следует применять базовые принципы цифровой гигиены:

1)проверять источники любой информации (смотрите на ссылки на источники и наличие подобной информации в поиске гугл/яндекс);

2) проверять автора сообщения. Обычно боты - это либо новореги, либо аккаунты с крайне низкой активностью, которые используют стоковые фотографии на аватарках, легко ищущиеся поиском и принадлежащие аккаунтам с другими именами.

При столкновении с ними стоит оставить жалобу на аккаунт и добавить в чёрный список.

Прямой взлом аккаунта

Чтобы обезопасить себя следует:

1)задуматься над более сложным паролем.

2) поставьте, наконец, двухфакторную авторизацию!

3) не авторизуйтесь с помощью учётной записи соцсетей на сомнительных ресурсах. Злоумышленники могут перехватить токен авторизации и воспользоваться им для входа в ваш аккаунт.

ФИШИНГ

Фишинг часто идёт рука об руку с ботами.

Например, распространяемый украинцами сайт для проверки попал ли ваш родственник в плен, на самом деле являлся фишинговым и собирал всю введённую информацию для дальнейшего спама и шантажа.

Но чаще фишинг используется для получения ваших учётных данных или данных банковской карты.

НЕ ОТКРЫВАЙТЕ ССЫЛКИ ИЛИ ВЛОЖЕНИЯ В ЭЛЕКТРОННОЙ ПЕРЕПИСКЕ ОТ НЕИЗВЕСТНЫХ АДРЕСАТОВ.

НЕ ПЕРЕХОДИТЕ ПО НЕИЗВЕСТНЫМ ССЫЛКАМ.

НЕ ВВОДИТЕ НИКАКИЕ ЛИЧНЫЕ ДАННЫЕ НА САЙТАХ, ПРО КОТОРЫЕ ВЫ В ПЕРВЫЙ РАЗ СЛЫШИТЕ.

ДАЖЕ ЕСЛИ ВАМ ПИШЕТ ЗНАКОМЫЙ, УБЕДИТЕСЬ, ЧТО ЕГО НЕ ВЗЛОМАЛИ.

Эти правила должны быть выучены буквально всеми, т.к. большая часть взломов осуществляется с помощью фишинга.