**Несколько советов по безопасности в сети «Интернет».**

Современную жизнь трудно представить себе без сети «Интернет». Современные компьютерные технологии стремительно развиваются и занимают все больше места в жизни каждого человека.

Вместе с тем интернет-технологии активно используют преступники и правонарушители. Такая ситуация сформировала понятие об интернет-угрозах и необходимость их распознавать и им противостоять.

Социальные сети сегодня стали для нас больше, чем просто среда общения и обмена фотографиями. Простота работы со своими страничками со смартфонов и планшетов, недорогие тарифы для подключения мобильного

интернета и доступный wi-fi, позволяют быть on-line всегда и везде, а социальные сети превращаются в устойчивую привычку, без которой мы уже не можем представить современную жизнь. Но легкая доступность сетей создает новые возможности и новые угрозы, как для активных пользователей, так и для тех, кто проверяет свои «странички» один раз в день или даже реже.

 Страничка в социальных сетях – это мощный инструмент формирования имиджа человека, поэтому так необходимо внимательно относиться к тому, как она выглядит. Но как найти эту грань между излишней скрытностью и чрезмерным хвастовством? Ведь сегодня принято встречать человека по аватарке, а провожать по контенту страницы. Медиамир стал настолько реальным, что мы воспринимаем страницу человека, как его самого. Смотрим на записи и делаем выводы. Если у Вас «открытые» аккаунты в

социальных сетях, то нужно понимать, что информацию в них может увидеть любой пользователь. В связи с этим, важной проблемой становится эмоциональная зависимость от социальных сетей и излишняя откровенность.

Большинству пользователей зачастую трудно удержаться от соблазна рассказать о приобретении машины, квартиры, повышении на работе, путешествии или утреннем кофе. Контент страницы – личная информация,

контакты, фотографии, геолокация – позволяет узнать Ваше окружение, интересы и виды активности. Визуальный контент обычно проходит внутреннюю модерацию, позволяет оценить уровень уверенности, смелости и адекватности. Мы не призываем Вас оставлять аккаунты пустыми, но не стоит забывать о настройках приватности. При этом важно заметить, что быть и казаться – разные понятия. То, что демонстрируется в социальных сетях, не всегда соответствует реальности. Нельзя забывать, что в современном мире социальные сети – это ваше лицо. И если Вы хотите произвести хорошее впечатление, оставляйте все самое личное «под замком».

Не стоит использовать чужую фотографию в качестве аватарки для своей странички. Герой «украденного» кадра может пожаловаться в администрацию соц.сети, и Ваш аккаунт заблокируют. Указывайте настоящее имя. «Псевдонимы» могут негативно характеризовать Вас в глазах коллег и будущих работодателей. Не размещайте персональные данные, которые могут Вас скомпрометировать или стать причиной для излишнего

беспокойства. Уделяйте значение тому, о чем Вы пишете на странице, и тем репостам, которые делаете из пабликов и со страниц своих друзей. Они также

работают на Ваш имидж.

 Пользователи социальных сетей все чаще сталкиваются с кибермоббингом. Кибермоббинг - это использование средств электронной коммуникации для унижения и оскорбления других людей. Иначе говоря, кибермоббинг – это социальное давление, перенесенное в плоскость электронного общения. Кибермоббинг осуществляется посредством электронной почты, социальных сетей, программ для мгновенного обмена сообщениями, размещения на порталах, а также посредством мобильного телефона, через SMS-сообщения.

**Чтобы не стать жертвой кибермоббинга, воспользуйтесь следующими правилами:**

- не выкладывайте в сеть лишнюю информацию или медиафайлы, которые могут компрометировать Вас или Ваших знакомых. Также не стоит отправлять такую информацию людям, которые не вызывают доверия,

- не вступайте в словесные перепалки в комментариях, на форумах, в беседах. У комментаторов может появиться желание мести,

- игнорируйте сообщения, в которых Вас оскорбляют, унижают или угрожают. Также стоит уведомить о таких сообщениях администрацию сайта или сервиса,

- не угрожайте хулигану «найти и наказать». Это лишь спровоцирует его на продолжение социального давления и усугубит ситуацию.

- удалите злоумышленника из социальных сетей, заблокируйте доступ к Вашей странице, добавьте в черный список,

- не присоединяйтесь, если Ваши друзья дразнят кого-то в сети. Попросите их остановиться, предупредите о вредных последствиях кибермоббинга.

- чаще меняйте пароли в социальных сетях, так как злоумышленники могут писать от Вашего имени.

**Как распознавать спам:**

- если Вы считаете, что получили письмо содержащее спам в папку **Входящие,** выделите нужное письмо и нажмите кнопку **Это спам!** — письмо

будет перемещено в папку **Спам,** а необходимая информация будет отправлена в Спамоборону. Изучение нежелательных рассылок позволяет

улучшать алгоритмы фильтрации для новых видов спама.

- если письмо попало в папку **Спам** по ошибке, нажмите кнопку **Не спам!** — новые письма из рассылки будут приходить в папку **Входящие.**

- спамооборона учитывает как общие, так и «персональные» правила фильтрации, которые действуют для отдельного почтового ящика. Если вы считаете письма рассылки нежелательными, а пользователь другого почтового ящика — полезными, в вашем ящике они будут попадать в папку

**Спам,** а в ящике другого пользователя в папку **Входящие.**

**Несколько правил безопасности Интернет-транзакций:**

 Если Вы решили проверить баланс своей кредитной карты онлайн, оплатить счета, перевести деньги кому-либо, купить или продать что-нибудь в интернете, то эти простые правила помогут Вам не потерять деньги.

1. **Защити свой компьютер.**

- Своевременно проверяйте обновления Программного обеспечения. Обязательно установите антивирусное и антишпионское ПО. Никогда не отключайте firewall. Защитите свой wi-fi роутер паролем и используйте usb-накопители с осторожностью.

 **2.** **Используйте только сложные пароли.**

- Самые эффективные пароли – написать какое-нибудь русское словосочетание в английской раскладке клавиатуры. Вам в любом случае будет намного проще и главное безопаснее создать свой сложный пароль, чем злоумышленникам такой пароль разгадать. Пароль «Denis1986» взламывается очень просто, поэтому мы советуем Вам придумать 2 вида паролей: 1) длинные и сложные пароли для платежных систем; 2) простые и легко запоминающееся для форумов и других, не представляющих опасности для ваших денег. Храните свои пароли в секрете. Не отправляйте их по SMS, e-mail или в социальных сетях.

 **3. Не переходите по ссылкам. Набирайте адрес сайта самостоятельно.**

- При переходе по ссылке из сомнительных источников (e-mail,форумы, сообщения в соц.сетях, всплывающие окна), Вы рискуете попасть на «фишинговый сайт» (Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям, номерам кредитных карт, электронной почте и т.д.). Суть заключается в том, что мошенник создает интернет-страницу, идентичную настоящей, на которой у пользователя запрашивается конфиденциальная информация с целью ее получения мошенником. В первую очередь при переходе на сайт обращайте внимание на адресную строку. Зачастую мошенники подменяют одну или несколько букв в названии сайта (пример: http://www.sberbank.ru/ - http://www.sbenbank.ru/).

 **4. Всегда проверяйте, установлено ли защищенное соединение.**

- В сети Интернет используется в основном два протокола: HTTP и Secure HTTP. Перед тем как ввести свою конфиденциальную информацию (пароли, номера кредиток, номер телефона, паспортные данные), обратите внимание на адресную строку, убедитесь, что имя протокола имеет вид https://, а не http (“s” – значит secure. англ. «защищенный»). Сертификаты подлинности получают только законопослушные компании, проверенные специалистами.

Также о защищенности интернет-соединения свидетельствует значок амбарного замка на зеленом фоне рядом с адресной строкой.

 **5. Совершайте транзакции только на домашнем компьютере.**

- Никогда не оплачивайте счета, не проверяйте баланс личного счета, не совершайте покупки и другие операции с банковскими картами или электронными деньгами на компьютерах с общим доступом, а также на других мобильных устройствах (планшетах, телефонах), подключенных к публичным точкам доступа WiFi.

 **6. Придерживайтесь здравого смысла.**

- Чтобы защитить себя от мошенников, тщательно изучите эти простые советы. Внимательно относитесь к оповещениям из своего «банка». Часто злоумышленники присылают сообщения, в которых написано, что Ваш счет будет заблокирован, если Вы не предпримите немедленных действий, связанных с переводом денег, или представляются вашими родственниками и требуют денег на операцию. Не доверяйте сообщениям такого характера, и с

Вашими деньгами все будет в порядке.