Правила безопасности в сети интернет

Информационная безопасность в сети интернет становится темой уроков в школах. Вирус легко подхватить со спамом, даже на проверенных сайтах, поэтому опытные юзеры рекомендуют установить надежный файрволл и антивирусное программное обеспечение, с автоматическим обновлением. Существует несколько правил:

1. Удалять неизвестные письма и файлы от неизвестных адресатов.
2. Не читая, бросать в спам предложения легкого заработка.
3. Никому не показывать свои пароли.
4. Не пользоваться подозрительными ссылками.
5. Работать с платежными системами через приложения.
6. Отслеживать интернет-траффик, если он вдруг сильно возрос, возможна вирусная атака.

Безопасность в социальных сетях

Небрежность к вопросу «безопасность в интернете» может создать немало проблем. Одним из основных источников опасности являются социальные сети, поэтому рекомендуется соблюдать меры безопасности в сети интернет и никогда не сообщать:

1. Дату дня рождения свою или членов семьи.
2. Семейное положение. Особенно это касается женщин, которые легко могут стать жертвами аферистов.
3. Место жительства или данные об отъезде. Многие люди, уезжая на отдых, сообщают об этом в социальных сетях друзьям и знакомым. Безопаснее позвонить, поскольку эта информация может послужить наводкой для воров.
4. Личную информацию о себе или сплетни о сотрудниках, с упоминанием имен или фамилий.
5. Подробные данные о детях, с упоминанием имени и даты рождения. Этой информацией могут воспользоваться мошенники.

Безопасность платежей в интернете

В наше время большинство финансовых операций проводится через интернет, кабинеты онлайн удобны, но тоже требуют учитывать меры безопасности в сети интернет:

- никогда не сообщать данные карты;
- завести вторую карту для выплат, если работодатели окажутся мошенниками, то потери будут минимальными.
- игнорировать запросы банков о проверке пароля, они их не рассылают.

Людям, которые ведут торговлю через интернет, стоит обратить внимание на такие аспекты:

1. Рассчитываться за покупки лучше дебетовой картой, а не кредитной.
2. Установить на основной карте лимит доступных денег или пополнять счет перед покупками.
3. Позаботиться об СМС-информировании, это поможет вовремя заблокировать доступ к карте.
4. Пользоваться проверенными сервисами.
5. Отказываться от автоплатежей, они могут «посадить» пользователя на обременительные выплаты.

Безопасность интернет банкинга поможет обеспечить:

- SSL-шифрование данных, передаваемых от компьютера пользователя в систему банка и назад;
- полученные в банках одноразовые пароли;
- разовые СМС-пароли;
- электронная цифровая подпись;
- внешний электронный ключ;

Безопасность покупок в интернете

Покупки в интернет-магазинах очень удобны, но повышается риск потерять деньги на махинациях аферистов. Специалисты разработали для покупок такие меры безопасности в интернете:

1. Приобретать товары в крупных маркетах.
2. Проверять, соответствует ли информация на сайте онлайн-магазина действительности, должен быть указан адрес и телефон для контактов.
3. Уточнять, как давно на рынке интернет-услуг работает торговая точка через дату регистрации домена. Если магазин открылся недавно, лучше не рисковать, сайты-однодневки часто используют мошенники.
4. Использовать защищенное соединение.
5. Заранее ознакомиться с отзывами об интернет-магазине или товаре на форумах.

Немного советов, для безопасности пользования Интернетом...

Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но в тоже время, Сеть таит в себе много опасностей. Помните, что Ваша безопасность в Интернете, на 90% зависит от Вас.

Совет №1.

Не ходите по подозрительным ссылкам.
Если вам пришло письмо с предложением обновить пароль или с сайта «Одноклассники.ру» поступило уведомление о новом сообщении, не торопитесь открывать предлагаемые ссылки.
Вместо настоящего сайта вполне можно увидеть совсем не то, что есть на самом деле, разница всего в одной букве, и многие этого даже не замечают. Если вы проследуете по этой ссылке, то в худшем случае можете подцепить серьезный вирус, а в лучшем – просто лишитесь своего аккаунта на сайте.

Совет № 2.

Установите систему антивирусной защиты.
Не экономьте на этих системах и не забывайте регулярно обновлять антивирусные базы.

Совет № 3.

Не верьте предложениям прочитать чужие SMS или посмотреть на «шокирующее видео», например, с Семенович.

Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, «Программы, позволяющие заходить в чужие страницы». В общем, фантазия мошенников безгранична. Когда спадет волна SMS, придет что-нибудь другое.
Общее у всех этих фальшивок одно – вам предлагается нечто, нарушающее чье-то личное пространство якобы под большим секретом. Люди любопытны и доверчивы, и именно излишняя доверчивость иногда приводит к большим бедам. В лучшем случае, захотев прочитать чужие SMS, можно лишиться 300-500 рублей на счету телефона (если нужно будет отправить сообщение на короткий номер для оплаты), в худшем – на компьютере поселится злобный вирус с такого сайта.
Запомните одну простую вещь: ***«Бесплатный сыр - только в мышеловке!»***

Совет № 4.

Пользуйтесь лицензионным программным обеспечением (ПО).

Совет № 5.

Делайте покупки только в проверенных интернет-магазинах.

Совет № 6.

Регулярно устанавливайте обновления программ. Своевременная установка обновлений касается любых программ.

Совет № 7.

С осторожностью относитесь к скачиваемым в Интернете файлам. Никто не гарантирует, что, скачивая программу даже на известном и уважаемом сайте, вы не подцепите очередной вирус. Новые вирусы выходят быстрее, чем защита от них, и антивирусное ПО сайтов вполне может «проморгать» очередной хитрый вирус. Совет один – обязательно сканируйте все новые файлы вашим антивирусом.

Совет № 8.

Не верьте всему, что говорят и пишут в Интернете.

Совет № 9.

Фильтруйте электронные письма. Никогда не открывайте «подозрительные письма» и тем более никогда на них не отвечайте.

Совет №10.

Не разглашайте в Интернете личную информацию.

Безопасность работы в интернете

Чтобы безопасность в сети интернет была надежной, необходимо придерживаться нескольких правил:

1. Отслеживать адреса ссылок. Если предлагается посетить по переходу другой сайт, лучше не проверять, куда этот «клубочек» приведет.
2. Внимательно читать строчки браузера. Вместо Одноклассники. ру может прийти похожая - Одноклассники. ру. ком, это уже совсем иная рассылка, опасная для компьютера.
3. Не пользоваться незнакомыми ссылками или файлами, даже если они пришли от друзей. Лучше уточнить у приятеля, присылал ли он ее, нередко через взломанный аккаунт рассылается вредный спам.
4. Проверять материалы, которые скачиваете через файлообменник.

Безопасность общения в интернете

Многие пользователи находят друзей в соцсетях, но нужно помнить, что при общении не стоит игнорировать правила безопасности в интернете. Чем больше круг, тем выше риск получить неприятности от малознакомых людей. Правила очень простые:

1. Не выкладывать сканы документов и данные банковских карт, иначе рискуете стать заемщиком крупной суммы или потерять свои кровные.
2. Не указывать адрес и место работы.
3. Не соглашаться на встречи в реале, если новый знакомый предлагает сомнительное или малолюдное место.
4. На форумах общаться уважительно.

Безопасность детей в интернете

Современные дети сегодня – самая большая зона риска, поскольку безоговорочно доверяют онлайн-друзьям, под ником которых могут скрываться недобрые взрослые. Безопасность детей в сети интернет – забота родителей. Можно установить программу, которая блокирует посещение опасных сайтов. Объясните подростку, что ради своей же безопасности необходимо:

- не писать свои настоящие данные, адрес и номер школы, поскольку ими могут воспользоваться аферисты;
- не устанавливать неизвестные программы;
- не доверять безоговорочно всему, что пишут в сети;
- сообщать родителям, если появились подозрительные знакомые, настойчиво предлагающие повидаться в реале.

Безопасность в интернете - «группы смерти»

Огромный ажиотаж вызвала деятельность «групп смерти», подталкивающие молодежь к самоубийству. Безопасность в сети стала иллюзорной, для не желающих расставаться с жизнью в ход шли угрозы. Если ребенок стал замкнутым и запуганным, не исключено, что причиной этого является такая секта. Короткий инструктаж для взрослых, как построить сложную беседу:

1. Объяснить, что для тех, кто толкает на смерть, это способ заработать, чем больше таких случаев, тем больше рекламы сайту.

2. Аргументировать, что организаторы таких сект – неадекватные люди, и нельзя умирать, чтобы доставить удовольствие психопатам.
3. Подыскать написанные медиками материалы о том, как болезненны любые способы самоубийства.
4. Заверить, что угрозы тем, кто не хочет подчиняться – надуманные, в реальности причинить вред организаторы не осмелятся. Если же подобные звонки все же имели место, необходимо обратиться в правоохранительные органы.