Основные правила безопасности в сети Интернет

- Будьте аккуратны со ссылками, содержащимися в электронных посланиях. Они могут вести совсем не туда, куда указывает текстовая информация.
- Не отправляйте конфиденциальную личную или финансовую информацию, если только она не зашифрована (при работе на защищенном веб-сайте). Обычные письма по электронной почте не шифруются.
- Будьте внимательны! Фальшивые, похожие на сайты крупных компаний веб-сайты, предназначены для обмана клиентов и сбора их личной информации. Убедитесь, что веб-сайты, с которыми Вы работаете, содержат заявления о соблюдении конфиденциальности и безопасности, и внимательно их изучите. Убедитесь, что необходимый вам URL появляется в поле «адрес» или «узел» вашего браузера. Некоторые веб-сайты могут казаться похожими на необходимый Вам, но в действительности быть фальсифицированными. Потратьте несколько лишних секунд и напечатайте URL лично.
- При передаче конфиденциальной информации ищите символ замка в правом нижнем углу веб-страницы. Этот символ указывает на то, что сайт работает в защищенном режиме. Вы должны увидеть его ПРЕЖДЕ, чем Вы введете конфиденциальную информацию.
- Используйте надежные пароли или ПИНы для Ваших счетов в Интернете. Выбирайте слова, которые другим будет трудно угадать, и используйте разный пароль для каждого Вашего счета. Используйте буквы и цифры, а также сочетание заглавных и строчных букв, если пароли или ПИНы различают строчные и заглавные буквы.
- При выходе из программы делайте это в соответствии с установленными процедурами. Не закрывайте браузер просто так! Выполняйте инструкции по выходу из безопасной зоны для обеспечения Вашей безопасности.
- Избегайте осуществления любых банковских операций в местах, где услуги Интернет являются общедоступными, например в Интернет-кафе. Очень трудно определить, отсутствуют ли на таких компьютерах хакерские программы, которые фиксируют Вашу личную информацию и сведения о счете. Если Вам необходимо осуществить операцию с компьютера общего пользования, измените Ваш ПИН с Вашего компьютера после того, как Вы пользовались компьютером общего доступа. Это имеет большое значение, так как существует риск фиксирования нажатий клавиш (включая номера банковской карты и кредитной карты, а также ПИНа) при помощи специальных программ, встроенных в компьютер общего доступа, без Вашего ведома.

1. Логин и Пароль

Логин - это Ваш уникальный идентификатор, «имя», дающее возможность защитить ваш подключенный к Сети компьютер от несанкционированного входа в сеть другим лицом. При регистрации в нашей сети вы указываете свой логин и вводите пароль, известный только Вам.

Основные правила обращения с Логином и Паролем

- Пожалуйста не сообщайте Ваш пароль другим лицам!
- Не отвечайте на послания по электронной почте с запросами о Ваших личных данных!
- Относитесь с подозрением к любой компании или лицу, запрашивающим Ваш пароль, номер

паспорта или другую конфиденциальную информацию. Сотрудники компании NetByNet никогда не запрашивает информацию такого рода по электронной почте.
- Периодически проверяйте свой компьютер антивирусной программой на отсутствие программ-шпионов, крадущих пароли и личные данные.
- Помните что все действия совершенные под Вашими логином/паролем юридически считаются совершенными Вами.

2. Вирусы

Компьютерный вирус - это программа, нарушающая целостность информации на вашем компьютере, в отдельных случаях приводящая также к отказу оборудования, входящего в состав вашего компьютера. В современных условиях компьютерные вирусы являются неотъемлемой частью информации, содержащейся в локальных и глобальных (Интернет) сетях, однако, влияние вирусов на работу Вашего компьютера можно нейтрализовать, придерживаясь следующих правил.

Основные правила антивирусной безопасности.

- Устанавливайте зарекомендовавшие себя антивирусные программы
- Несмотря на большой выбор антивирусных систем, следует использовать только безусловно зарекомендовавшие себя на нашем рынке пакеты. Вы можете обратиться к нам за рекомендациями по антивирусному программному обеспечению. Следует также отдавать предпочтение хорошо поддерживаемым продуктам именно нашего региона, поскольку, несмотря на глобальность сети, большая часть вирусов присуща именно Рунету (русскоязычному Интернету).
- Периодически обновляйте Вашу антивирусную программу
- Антивирусные сканеры способны защищать только от тех компьютерных вирусов, данные которой содержатся в антивирусной базе. Этого недостаточно для гарантии абсолютной защиты - хотя бы потому, что появляются новые виды вирусных программ. Поэтому обновлять антивирусные базы надо регулярно. Чем чаще выполняется эта несложная операция, тем более защищенным будет рабочее место.
- Будьте осторожны с файлами в письмах электронной почты. Никогда не открывайте подозрительные файлы, пришедшие от незнакомых Вам людей.
- Никогда не запускайте программы, присланные неизвестным лицом! Это правило является общеизвестным и не нуждается в пояснениях. Однако файлы, полученные от «надежных» корреспондентов (знакомых, коллег, друзей), также могут быть инфицированы. Ваши знакомые могут не знать, что с их компьютера несанкционированно отправляются письма: вирус способен осуществлять отправку от чужого имени незаметно для владельца компьютера! Перед открытием любого файла необходимо проверить его антивирусными средствами. Естественно, хорошие антивирусные пакеты производят проверку автоматически.
- Ограничьте круг лиц, пользующихся Вашим компьютером
- Идеальным вариантом является ситуация, когда никто, кроме вас, не имеет доступа к вашему компьютеру. Однако, если это невозможно, необходимо четко разграничить права доступа и определить круг разрешенных действий для других лиц. В первую очередь это касается работы с дискетами и CD, Интернетом и электронной почтой.
- Делайте регулярное резервное копирование
- Выполняя это правило, Вы сможете сохранить данные не только при поражении компьютера каким-либо вирусом, но и в случае серьезной поломки в аппаратной части компьютера.
- Не паникуйте!

Мы ни в коем случае не хотим создать среди пользователей впечатление, что вирусы - это

неисправимая катастрофа. Вирусы являются такими же программами, как, допустим, калькулятор или записная книжка Windows. Их отличительная черта в том, что вирусы способны размножаться (т.е. создавать свои копии), интегрироваться в другие файлы или загрузочные секторы, а также производить другие несанкционированные действия. Гораздо больший вред способны нанести необдуманные действия, направленные на нейтрализацию вируса. При работе в корпоративной сети следует немедленно обратиться к системному администратору. Если Вы просто домашний пользователь, то свяжитесь с компанией, у которой Вы приобрели антивирусную программу. Предоставьте возможность профессионалам позаботиться о безопасности вашего компьютера, в противном случае Вы можете навсегда потерять информацию, хранившеюся на Вашем компьютере.

В заключение следует добавить, что вредоносные программы могут не быть вирусами как таковыми, но безусловно создавать трудности при работе на компьютере. Это могут быть, например, программы навязчивой рекламной направленности, заносящие адрес своей страницы в систему как стартовую при просмотре Интернет, и не дающие возможность ее изменить в дальнейшем. Поэтому, кроме антивирусного программного обеспечения, неплохо установить программы AdAware, защищающие от таких вредоносных программ.

3. Работа через радиомодемы WiFi

У беспроводных сетей очень много общего с проводными, но есть и различия. Для того, чтобы проникнуть в проводную сеть, хакеру необходимо физически к ней подключиться. В варианте Wi-Fi ему достаточно установить антенну в ближайшей подворотне в зоне действия сети.

Что же теоретически может получить злоумышленник в беспроводной сети, настройке которой не было уделено должного внимания?

Вот стандартный список:

- доступ к ресурсам и дискам пользователей Wi-Fi-сети, а через неё - и к ресурсам LAN;
- подслушивание трафика, извлечение из него конфиденциальной информации;
- искажение проходящей в сети информации;
- воровство интернет-траффика;
- атака на ПК пользователей и серверы сети (например, Denial of Service или даже глушение радиосвязи);
- внедрение поддельной точки доступа;
- рассылка спама, противоправная деятельность от Вашего имени.

В сети NetByNet разрешена установка клиентами бытового оборудования wi-fi в целях личного использования и организации внутренней wi-fi сети для подключения нескольких компьютеров в пределах квартиры. Но мы настоятельно просим уделять должное внимание вопросам безопасности Вашего wi-fi оборудования.

Основные же правила при организации и настройке частной Wi-Fi-сети (если нет задачи сделать её общедоступной) таковы:

- Перед покупкой сетевых устройств внимательно ознакомьтесь с документацией. Узнайте, какие протоколы или технологии шифрования ими поддерживаются. Проверьте, поддерживает ли эти технологии шифрования ваша ОС. Если нет, то скачайте апдейты на сайте разработчика. Если ряд технологий не поддерживается со стороны ОС, то это должно поддерживаться на уровне драйверов;
- Обратите внимание на устройства, использующие WPA2 и 802.11i, поскольку в этом

стандарте для обеспечения безопасности используется новый Advanced Encryption Standard (AES);

- Если точка доступа позволяет запрещать доступ к своим настройкам с помощью беспроводного подключения, то используйте эту возможность. Настраивайте AP только по проводам. Не используйте по радио протокол SNMP, web-интерфейс и telnet;
- Если точка доступа позволяет управлять доступом клиентов по MAC-адресам (Media Access Control, в настройках может называться Access List), используйте эту возможность. Хотя MAC-адрес и можно подменить, тем не менее это дополнительный барьер на пути злоумышленника;
- Если оборудование позволяет запретить трансляцию в эфир идентификатора SSID, используйте эту возможность (опция может называться "closed network"), но и в этом случае SSID может быть перехвачен при подключении легитимного клиента;
- Запретите доступ для клиентов с SSID по умолчанию "ANY", если оборудование позволяет это делать. Не используйте в своих сетях простые SSID - придумайте что-нибудь уникальное, не завязанное на название вашей организации и отсутствующее в словарях. Впрочем, SSID не шифруется и может быть легко перехвачен (или подсмотрен на ПК клиента);
- Располагайте антенны как можно дальше от окон, внешних стен здания, а также ограничивайте мощность радиоизлучения, чтобы снизить вероятность подключения «с улицы». Используйте направленные антенны, не используйте радиоканал по умолчанию;
- Если при установке драйверов сетевых устройств предлагается выбор между технологиями шифрования WEP, WEP/WPA (средний вариант), WPA, выбирайте WPA (в малых сетях можно использовать режим Pre-Shared Key (PSK)). Если устройства не поддерживают WPA, то обязательно включайте хотя бы WEP. При выборе устройства никогда не приобретайте то, что не поддерживает даже 128bit WEP.
- Всегда используйте максимально длинные ключи. 128-бит - это минимум (но если в сети есть карты 40/64 бит, то в этом случае с ними вы не сможете соединиться). Никогда не прописывайте в настройках простые, «дефолтные» или очевидные ключи и пароли (день рождения, 12345), периодически их меняйте (в настройках обычно имеется удобный выбор из четырёх заранее заданных ключей - сообщите клиентам о том, в какой день недели какой ключ используется).
- Не давайте никому информации о том, каким образом и с какими паролями вы подключаетесь (если используются пароли). Искажение данных или их воровство, а также прослушивание трафика путем внедрения в передаваемый поток - очень трудоемкая задача при условиях, что применяются длинные динамически изменяющиеся ключи. Поэтому хакерам проще использовать человеческий фактор;
- Если Вы используете статические ключи и пароли, позаботьтесь об их частой смене. Делать это лучше одному человеку - администратору;
  если в настройках устройства предлагается выбор между методами WEP-аутентификации "Shared Key" и "Open System", выбирайте "Shared Key". Если AP не поддерживает фильтрацию по MAC-адресам, то для входа в "Open System" достаточно знать SSID, в случае же "Shared Key" клиент должен знать WEP-ключ (www.proxim.com/ support/ all/ harmony/ technotes/ tn2001-08-10c.html). Впрочем, в случае "Shared Key" возможен перехват ключа, и при этом ключ доступа одинаков для всех клиентов. В связи с этим многие источники рекомендуют "Open System";
- Обязательно используйте сложный пароль для доступа к настройкам точки доступа. Если точка доступа не позволяет ограничивать доступ паролем, её место на свалке;
- Если для генерации ключа предлагается ввести ключевую фразу, то используйте набор букв и цифр без пробелов. При ручном вводе ключа WEP вводите значения для всех полей ключа (при шестнадцатеричной записи вводить можно цифры 0-9 и буквы a-f).
- По возможности не используйте в беспроводных сетях протокол TCP/IP для организации папок, файлов и принтеров общего доступа. Организация разделяемых ресурсов средствами

NetBEUI в данном случае безопаснее. Не разрешайте гостевой доступ к ресурсам общего доступа, используйте длинные сложные пароли;

- По возможности не используйте в беспроводной сети DHCP - вручную распределить статические IP-адреса между легитимными клиентами безопаснее;
- На всех ПК внутри беспроводной сети установите файерволлы, старайтесь не устанавливать точку доступа вне брандмауэра, используйте минимум протоколов внутри WLAN (например, только HTTP и SMTP). Дело в том, что в корпоративных сетях файерволл стоит обычно один - на выходе в интернет, взломщик же, получивший доступ через Wi-Fi, может попасть в LAN, минуя корпоративный файерволл;
- Регулярно исследуйте уязвимости своей сети с помощью специализированных сканеров безопасности (в том числе хакерских типа NetStumbler), обновляйте прошивки и драйвера устройств, устанавливайте заплатки для Windows.

Пожалуйста помните, что при компрометации Вашей wi-fi сети и совершении злоумышленником противоправных действий в Сети от Вашего имени, доказать Вашу непричастность очень сложно.