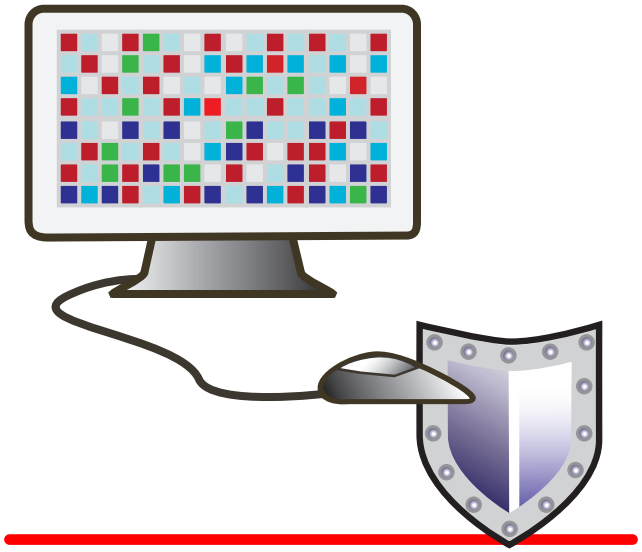
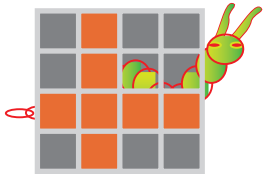
# КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ: дело каждого

**Преступники часто выбирают компьютеры и Интернет своей мишенью. Если компьютер не защищен, они могут получить доступ к информации в вашем компьютере и украсть номера кредитных карт, сведения о банковских счетах и другие конфиденциальные личные данные.**

**Каждый, кто пользуется компьютером, должен предпринять действия для того, чтобы повысить безопасность и снизить риск нанесения ущерба себе и своему компьютеру. Ниже приведены распространенные рекомендации по обеспечению компьютерной безопасности, которые вы можете использовать для своего компьютера.**



## Вирусы и черви



Компьютерный «вирус» внедряется в программы в вашем компьютере и причиняет вред программам, информации или оборудованию. Компьютерный «червь» делает то же самое и к тому же размножается. Вирусы и черви могут нанести вред вашему компьютеру, а также заразить другие компьютеры.

# ПРИМИТЕ МЕРЫ:

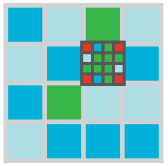
**вы можете предпринять эти действия безотлагательно, не тратя на это много времени и денег. Для некоторых требуется только изменить привычки.**

## Пароли


Пароли защищают данные, хранящиеся в вашем компьютере, включая конфиденциальные счета, документы и личные данные.

Наилучший способ не дать компьютерным взломщикам (хакерам) узнать ваш пароль, это использовать комбинацию букв, цифр и знаков (таких, как !, @, #, $, %). Самое важное, никогда не говорите никому свой пароль. Храните пароли в надежном месте и регулярно меняйте их.

## Пэтчи и обновления



Пэтч или обновление – это небольшая компьютерная программа, исправляющая известные проблемы программного обеспечения. Компании-разработчики программного обеспечения часто выпускают новые пэтчи и уведомляют вас о требующихся обновлениях по Интернету или по эл. почте, если вы зарегистрировали свой продукт.

Важно постоянно устанавливать новейшие пэтчи. Вы можете настроить свой компьютер делать это автоматически. Он будет связываться с компаниями-разработчиками программного обеспечения, чтобы исправлять вашу операционную систему, сетевой браузер и антивирусные программы.

## Брандмауэры и программы защиты против вирусов/ программ-шпионов

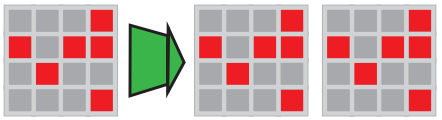
Брандмауэры (сетевые экраны) – это фильтрующие системы, контролирующие входящие и исходящие потоки информации между сетевыми компьютерными системами. Они защищают конфиденциальную информацию от несанкционированного доступа и не допускают попадание нежелательных программ в компьютер.

Программы антивирусной защиты или антивирусные программы пытаются определить, нейтрализовать или уничтожить вредоносные компьютерные программы. Антивирусные программы пытаются «почистить» («clean") или «дезинфицировать» ("disinfect") вирус, поместить его в «карантин» ("quarantine") или «разрушить»( "destroy") его, регулярно сканируя ваш компьютер.

Вы можете усилить настройки безопасности и блокировать всплывающую рекламу в своем сетевом браузере.

Есть бесплатные и несложные в пользовании брандмауэры и антивирусные программы. Информацию о них можно найти в Интернете по поисковым словам «брандмауэры (сетевые экраны)» или «антивирусные программы».

## Копии



Копировать важные файлы или документы, находящиеся в вашем компьютере, так же важно, как иметь копии вашего свидетельства о рождении или паспорта. Вы можете защитить свои документы или файлы, сохранив их на диск, флэш-диск USB, устройство сетевого хранения или другое устройство хранения информации. Делайте это регулярно.

## ПРОВЕРОЧНЫЙ СПИСОК

Ниже приводится проверочный список действий, которые пользователи домашних компьютеров могут предпринять для защиты своего компьютера. Он предоставлен координационным центром Computer Emergency Readiness Team (CERT). Более подробную информацию можно найти здесь: www.cert.org/tech_tips/home_networks.html.

- Пользуйтесь программами защиты
- Пользуйтесь брандмауэром (сетевым экраном).
- Не открывайте приложения к эл. сообщениям от неизвестного адресата.
- Не запускайте программы неизвестного происхождения.
- Блокируйте скрытые расширения названий файлов.
- Постоянно обновляйте все программы (включая операционную систему).
- Выключите компьютер или отключите Интернет, когда вы им не пользуетесь.

## Программы-шпионы и нежелательная реклама

Все хотят защитить свою конфиденциальную информацию. К сожалению, программы-шпионы (англ. название "spyware") и рекламные программы (англ. название "adware") могут проникнуть в ваш компьютер без вашего разрешения.

Вы можете неумышленно установить эти программы в свой компьютер, просматривая определенные веб-сайты, нажимая на ссылки, загружая файлы с Интернета или открывая приложения к сообщениям эл. почты.

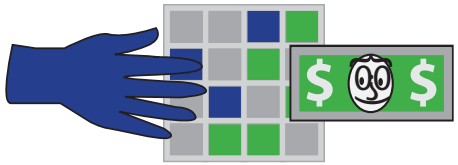
Программы-шпионы собирают личную информацию и посылают ее преступникам. Рекламные программы показывают нежелательную рекламу во всплывающих окнах или создают рекламную панель на экране вашего компьютера.

## Макулатурные сообщения эл. почты и махинации с целью выманивания денег:

**Не отвечайте на макулатурные эл. сообщения – удаляйте их!** Открывайте сообщения и нажимайте на ссылки, только если вы знаете авторов сообщений и доверяете им.

«Спам» - это непрошенное макулатурное сообщение эл. почты. Не отвечайте на него, просто удалите.

«Фишинг» (англ. название "Phishing") – это вид интернет-мошенничества, использующий спам или всплывающие сообщения, чтобы обманом побудить вас ввести личную информацию, номер социального обеспечения или пароли. Занимающиеся «фишингом» мошенники выдают свои электронные сообщения и веб-сайты за сообщения и сайты банков или других вызывающих доверие учреждений. Они пытаются обманом побудить вас предоставить им номера ваших счетов и пароли. Не отвечайте на эти сообщения и не нажимайте на ссылки, где вас просят предоставить личную информацию. Удаляйте их!



Также смотрите веб-сайт Сиэтла по безопасности информации по адресу: www.seattle.gov/informationsecurity.

Вы можете также посмотреть сайт компании Майкрософт по вопросам безопасности, где предоставлена информация на разных языках. Смотрите сайт по адресу: http://www.microsoft.com/protect и выберите нужный вам язык, нажав на "worldwide sites."

## ПОМОЩЬ

Печатные копии этой информации можно получить, позвонив по телефону (206) 233-7877 или написав нам по адресу: PO Box 94709, Seattle, WA, 98124-4709.

Районные библиотеки и технические центры также являются отличными источниками дополнительной информации. Смотрите: www.seattle.gov/tech/techmap

Помощь также можно получить в компаниях технической поддержки компьютеров и на сетевых форумах. Журнал «Consumer Reports», компьютерные журналы, компьютерные магазины, изготовители и компании-разработчики программного обеспечения также могут предоставить полезную информацию.

---

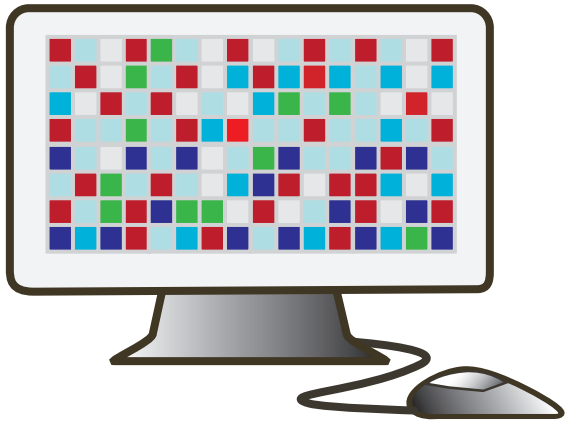
Эта брошюра подготовлена Технологической программой Отдела информационных технологий и Офисом информационной безопасности Городского совета Сиэтла.
www.seattle.gov/tech
www.seattle.gov/informationsecurity



Version 01/2010

City of Seattle
Department of Information Technology

# ЗАЩИЩЕН ЛИ ВАШ КОМПЬЮТЕР?



## Полезные советы для защиты вашего компьютера и ваших данных

City of Seattle
Department of Information Technology