

Опасные явления цифровой среды: вредоносные программы и приложения и их разновидности.
Правила кибергигиены, необходимые для предупреждения возникновения сложных и опасных ситуаций в цифровой среде.

Интернет — мир широких ВОЗМОЖНОСТЕЙ



Интернет позволяет вам:

- общаться с друзьями, семьей, коллегами;
- получать доступ к информации и развлечениям;
- учиться, встречаться с людьми и узнавать новое.

Защита и безопасность в Интернете

Защита. Необходимо защищать компьютеры при помощи современных технологий подобно тому, как мы защищаем двери в наших домах.

Безопасность. Наше поведение должно защищать от опасностей Интернета.



Основные угрозы безопасности компьютера



Вирусы и программы-черви

Программы, проникающие в компьютер для копирования, повреждения или уничтожения данных.



Программы-трояны

Вирусы, имитирующие полезные программы для уничтожения данных, повреждения компьютера и похищения личных сведений.



Программы-шпионы

Программы, отслеживающие ваши действия в Интернете или отображающие навязчивую рекламу.

Основные угрозы безопасности детей в Интернете



Киберхулиганы

И дети, и взрослые могут использовать Интернет, чтобы изводить или запугивать других людей.



Злоупотребление общим доступом к файлам

Несанкционированный обмен музыкой, видео и другими файлами может быть незаконным или повлечь загрузку вредоносных программ.



Неприличный контент

Если дети используют Интернет без присмотра, они могут столкнуться с изображениями или информацией, от которой их желательно оградить.



Вторжение в частную жизнь

Заполняя различные формы в Интернете, дети могут оставить конфиденциальные сведения о себе или своей семье.



Хищники

Эти люди используют Интернет для того, чтобы заманить детей на личную встречу.

Основные угрозы личной безопасности в Интернете



Кража идентификационных сведений

Преступление, связанное с похищением личных сведений и получением доступа к наличным деньгам или кредиту

Фишинг

Сообщения электронной почты, отправленные преступниками, чтобы обманом вынудить вас посетить поддельные веб-узлы и предоставить личные сведения



Мистификация

Сообщения электронной почты, отправленные, чтобы обманом вынудить пользователя отдать деньги



Нежелательная почта

Нежелательные сообщения электронной почты, мгновенные сообщения и другие виды коммуникации

Что вы можете предпринять



Ваш компьютер

- Включите интернет-брандмауэр Windows.
- Используйте Центр обновления Microsoft для автоматической загрузки новейших обновлений Windows.
- Установите и регулярно обновляйте антивирусное программное обеспечение.
- Установите и регулярно обновляйте Защитник Windows (Microsoft Windows Defender)



Ваша семья

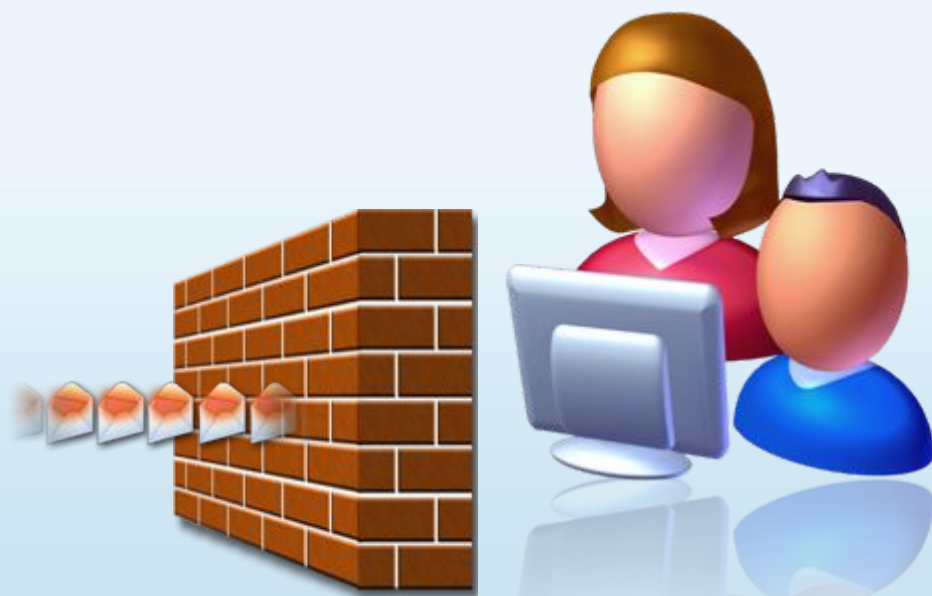
- Поговорите с детьми о том, что они делают в Интернете.
- Установите четкие правила использования Интернета.
- Держите личные сведения в секрете.
- Используйте настройки семейной безопасности в программном обеспечении Microsoft.



Вы сами

- Выработайте линию поведения в Интернете, снижающую риски.
- Аккуратно обращайтесь с личными сведениями.
- Используйте технологии антифишинга и защиты от нежелательной почты, встроенные в Windows Vista, Windows XP SP2, Windows Live и Microsoft Outlook.

Включите интернет-брандмауэр Windows



Интернет-брандмауэр
создает защитный
барьер между вашим
компьютером и
Интернетом

Используйте автоматическое обновление для загрузки новейших обновлений программного обеспечения

- Устанавливайте все обновления, как только они становятся доступны
- Автоматическое обновление обеспечивает наилучшую защиту



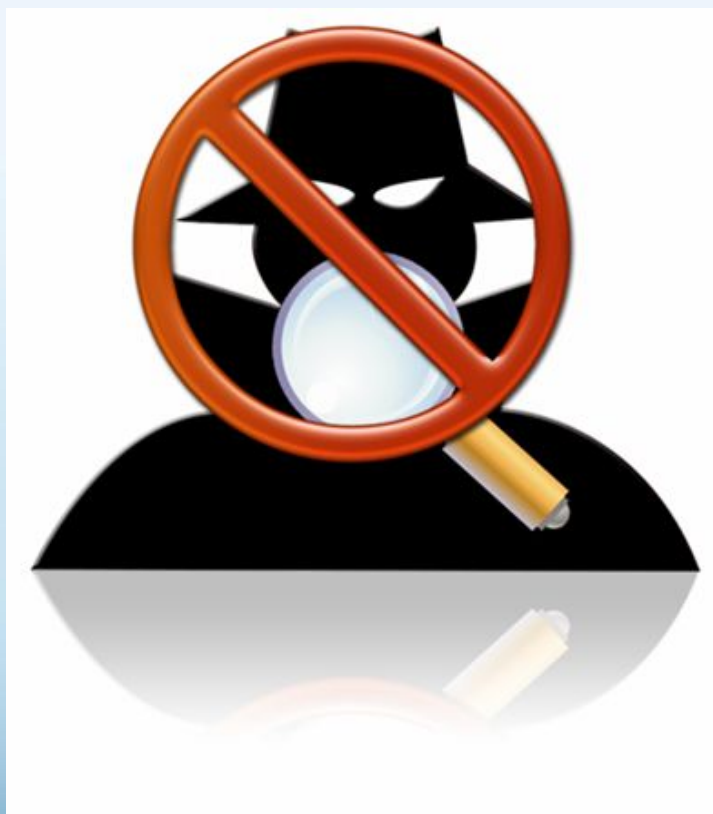
Установите и регулярно обновляйте антивирусное программное обеспечение



***Не позволяйте истечь
сроку его действия***

- Антивирусное программное обеспечение помогает обнаруживать и удалять компьютерные вирусы, прежде чем они смогут навредить.
- Для эффективности антивирусного программного обеспечения регулярно обновляйте его.

Установите и регулярно обновляйте антишпионское программное обеспечение



Используйте антишпионское программное обеспечение, такое как Защитник Windows (Microsoft Windows Defender), чтобы неизвестные программы не могли отслеживать ваши действия в сети и похищать ваши сведения.

Другие способы защиты компьютера



Архивируйте регулярно Ваши данные

Читайте заявления о конфиденциальности на веб-узлах

Закрывайте всплывающие окна при помощи красной кнопки «X»

Думайте, прежде чем щелкнуть по ссылке

Архивируйте свои файлы



- Сохраняйте их на компакт- или DVD-дисках, USB-накопителях или других внешних носителях
- Используйте веб-службы архивации

Думайте, прежде чем щелкнуть по ссылке

- Будьте осторожны с вложениями и ссылками в сообщениях электронной почты
- Загружайте файлы только с веб-узлов, которым доверяете



Изучайте заявления о конфиденциальности

Старайтесь понять,
на что Вы соглашаетесь,
прежде чем подтвердить
отправку или предоста-
вить личные сведения

Microsoft Online Privacy Notice Highlights

(Last updated January 2006)



Scope

This notice provides highlights of the full [Microsoft Online Privacy Statement](#). This notice and the full privacy statement apply to those Microsoft websites and services that display or link to this notice.

Personal Information

Additional Details

- When you register for certain Microsoft services, we will ask you to provide personal information.
- The information we collect may be combined with information obtained from other Microsoft services and other companies.
- We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.

Your Choices

Additional Details

- You can stop the delivery of promotional e-mail from a Microsoft site or service by following the instructions in the e-mail you receive.
- To make proactive choices about how we communicate with you, follow the instructions listed in the [Communication Preferences](#) of the full privacy statement.
- To view and edit your personal information, go to the [access section](#) of the full privacy statement.

Uses of Information

Additional Details

- We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
- We use your information to inform you of other products or services offered by Microsoft and its affiliates, and to send you relevant survey invitations related to Microsoft services.
- We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.

Important Information

- The full [Microsoft Online Privacy Statement](#) contains links to supplementary information about specific Microsoft sites or services.
- The sign in credentials (e-mail address and password) used to sign in to most Microsoft sites and services are part of the [Microsoft Passport Network](#).
- For more information on how to help protect your personal computer, your personal information and your family online, [visit our online safety resources](#).

How to Contact Us

For more information about our privacy practices, go to the full [Microsoft Online Privacy Statement](#). Or write us using our [Web ID](#).

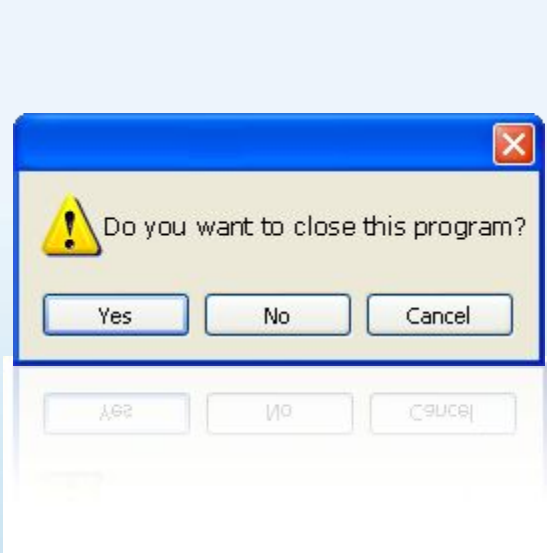
Microsoft is a TRUSTe licensee and you may [contact TRUSTe](#) if a privacy question is not properly addressed.

Microsoft Privacy

Microsoft Corporation

One Microsoft Way

Закрывайте всплывающие окна только щелчком по красной кнопке (X)



- Всегда используйте красную кнопку (X) в углу всплывающего окна.
- Никогда не нажимайте «Да», «Принять» и даже «Отмена», поскольку это может привести к установке программы на компьютер.

Установите четкие правила использования Интернета

- Не открывайте файлы для общего доступа и не открывайте вложения
- Не щелкайте по ссылкам в сообщениях электронной почты
- Относитесь к другим так, как хотите, чтобы относились к вам
- Защищайте себя
- Уважайте собственность других людей
- Никогда не отправляйтесь на личную встречу с «другом» из Интернета



Действия, которые помогут защитить *ваши личные сведения*

- 1** **Выработайте** линию поведения в Интернете, снижающую риски для вашей безопасности
- 2** **Обращайтесь** с личными сведениями аккуратно
- 3** **Используйте** технологии для снижения рисков и при необходимости поднимайте тревогу

Выработайте линию поведения в Интернете, снижающую риски для вашей безопасности



- Удаляйте нежелательную почту, не открывая ее
- Остерегайтесь мошенничества в Интернете
- Используйте надежные пароли

Осторожно обращайтесь с ЛИЧНЫМИ СВЕДЕНИЯМИ



- Никогда не сообщайте личные сведения в мгновенных сообщениях или электронной почте
- Пользуйтесь только безопасными и надежными веб-узлами
- Убедитесь, что Вы попали именно туда, куда намеревались: веб-узлы могут быть поддельными
- Избегайте финансовых операций по беспроводным сетям
- В публичном месте сохраняйте конфиденциальность

Пользуйтесь технологиями антифишинга и защиты от нежелательной почты

- Множество поставщиков электронной почты, а также такие программы, как Windows Live Hotmail® и Microsoft Outlook®, отфильтровывают большинство сообщений с нежелательной почтой
- Антифишинг в Internet Explorer® блокирует и предупреждает о подозрительных веб-узлах



Если Ваши идентификационные сведения похищены

- Сообщите об этом
- Ведите записи
- Измените все пароли
- Заявите о мошенничестве в кредитных отчетах

Получите копию **кредитного отчета** и убедитесь, что ваш счет отмечен записями «Мошенничество» и «Заявление пострадавшего»

Основные рекомендации по защите персональных данных

PRO PERM.RU

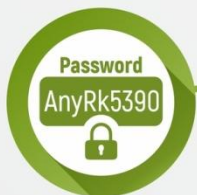
Не открывайте подозрительные файлы из электронных писем, не переходите по непроверенным ссылкам из sms и сообщений в соцсетях, не устанавливайте пиратский софт



Установите антивирус, опираясь на рейтинг Роскачества



Составляйте только сложные пароли из букв разного регистра, символов и цифр. Где возможно, используйте двухфакторную аутентификацию



Ни при каких обстоятельствах не вводите данные своих учетных записей (логин и пароль) на подозрительных сайтах



Используйте разные пароли на разных интернет-ресурсах



Отходя от компьютера, не забывайте включать спящий режим



Регулярно делайте резервные копии важной информации на внешнем USB-носителе.

Пройдите тест

- <https://cyberpolygon.com/ru/cyber-hygiene-test/>