БЕЗОПАСТНОСТЬ В ИНТЕРНЕТЕ

Учащегося 114
гр.
Герасимова
Алексея
КСиПТ

ОПРЕДЕЛЕНИЕ

- Интернет-безопасность — это отрасль компьютерной безопасности, связанная специальным образом не только с Интернетом, но и с сетевой безопасностью, поскольку она применяется к другим приложениям или операционным системам в целом.

ЗАЩИТА ОТ ХАКЕРОВ

- Как отмечает Inc., пользователи часто попадаются на удочку «странных» сайтов через виртуальное «сарафанное радио», при скачивании музыки или просмотре бесплатных фотографий.
- Нажав на сомнительную ссылку, вы можете запустить в свою систему вредоносное ПО, которое затем предо**1) Переход по сомнительным ссылкам**
- ставит злоумышленникам доступ к вашей личной информации, включая банковские счета и номера кредитных карт.
- Чтобы не подвергаться риску, старайтесь заходить на сайты с хорошей репутацией. Как правило, наиболее безопасные ссылки отображаются в верху списка результатов любого поискового запроса Google, но если вы все-таки сомневаетесь, не нажимайте на ссылку.

Вредоносные программы

- Вирус, иначе вредоносная программа — это любое программное обеспечение, используемое для получения несанкционированного доступа к информации или ресурсам компьютера с целью хищения, удаления, искажения или подмены данных. Вирусы делятся на группы по типу заражаемых объектов, методам заражения и жертвам. Заразить компьютер вирусом можно разными способами: от использования съемного носителя до посещения вредоносного сайта. Благодаря антивирусным компаниям в наше время вирусы встречаются довольно редко.
- Ботнет — компьютерная сеть, состоящая из запущенных ботов. Зачастую бот — специальная программа, устанавливаемая на компьютер пользователя без его согласия, которая позволяет злоумышленнику выполнять некие действия, такие как рассылка спама, переборка паролей и т. д.
- Компьютерный вирус — это программы, которые создают копии самих себя с целью внедрения в коды других программ и системные области памяти, а также распространения самих себя по различным каналам связи. Чаще всего используются для захвата информации на компьютере. Компьютерные виды делятся на группы по поражаемым объектам, методам их заражения, поражаемым операционным системам и т. д.
- Сетевые черви в некотором роде являются вирусами, так как тоже способны копировать самих себя, но не могут нанести вред существующим файлам. Вместо этого они создают дополнительную нагрузку на компьютер за счет интенсивного распространения. Черви классифицируются по способу распространения и месту заражения.
- Вирус-вымогатель блокирует доступ к компьютеру или возможность считывания данных, а затем требует выкуп для восстановления исходного состояния. Вирусы этого типа могут шифровать данные, блокировать или препятствовать работе в системе или браузере.
- Лжеантивирус создает видимость работающего антивируса, что позволяет осуществить внедрение дополнительного заражения. Также может предлагать дополнительные услуги при введении пользовательских данных: кредитная карта, номер телефона и т. д.
- Программа-шпион — это программа, тайно отслеживающая активность пользователя и сообщающая о ней другим пользователям. Данный вид программ имеет широкий спектр возможностей: от сбора информации о посещаемых сайтах до удаленного управления компьютером или смартфоном.
- Кейлогер — программное обеспечение, регистрирующее нажатия клавиш на клавиатуре и мыши, а также дату и время этих действий.
- Троян — вредоносная программа, проникающая на компьютер под видом легального программного обеспечения с целью выполнения действий, нужных злоумышленникам. Свое название вирус получил благодаря сходству по принципу действию с деревянным конем, погубившим Трою. Существует 5 основных типов троянов: удаленный доступ, уничтожение данных, загрузчик, деактиватор программ безопасности и сервер.

Токен (авторизации)

- Некоторые онлайн-сайты предлагают клиентам возможность использовать шестизначный код, который случайным образом изменяется каждые 30-60 секунд на токене безопасности. Клавиши маркера безопасности встроены в математические вычисления и манипулируют числами на основе текущего времени, встроенного в устройство. Это означает, что каждые тридцать секунд существует только определённый массив чисел, который будет правильным для проверки доступа к онлайн-учетной записи. Веб-сайт, на котором пользователь регистрируется, будет уведомлен о серийном номере этого устройства и будет знать вычисления и правильное время, встроенные в устройство, чтобы убедиться, что указанное число действительно является одним из немногих шестизначных чисел, которое работает в этом при 30-60-секундном цикле. Через 30-60 секунд устройство представит новое случайное шестизначное число, которое мож

Продукты интернет-безопасности

- Антивирусы
- Антивирусное программное обеспечение и программы обеспечения безопасности в Интернете помогут защитить устройство от атак путем обнаружения и устранения вредоносных программ.

- Менеджер паролей
- Менеджер паролей — это программное приложение, которое помогает пользователю хранить и организовывать пароли. Менеджеры паролей обычно хранят пароли в зашифрованном виде, требуя от пользователя создания главного пароля, открывающего доступ к базе всех паролей.

- Комплекты безопасности
- Так называемые комплекты безопасности были впервые предложены для продажи в 2003 году (McAfee) и содержат набор брандмауэров, антивирусных, антишпионских программ и т. д.[18] Они также предлагают защиту от краж, проверку безопасности переносного хранилища, частный интернет-просмотр, облачный антиспам, измельчитель файлов или принятие решений, связанных с безопасностью (ответы на всплывающие окна), а несколько из них бесплатны.


КОНЕЦ...