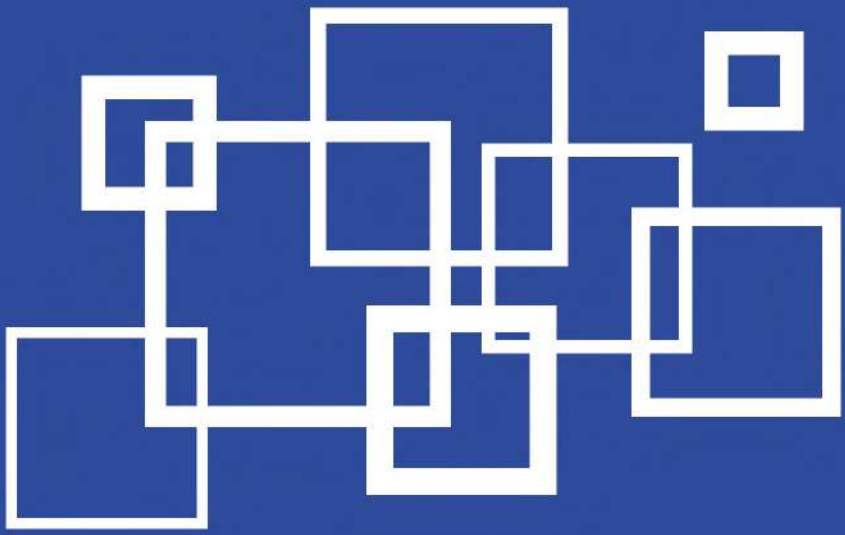
РЕКОМЕНДАЦИИ

по безопасному использованию
сети Интернет



ВВЕДЕНИЕ

Современный мир характеризуется стремительным развитием информационно-коммуникационных технологий и активным внедрением глобальных коммуникационных сетей, в частности сети Интернет, практически во все сферы деятельности человека и общества.

Люди доверяют компьютеру личную информацию, не зная или не задумываясь о связанных с этим рисках. Персональные данные, данные онлайн-банкинга – всё это является целью злоумышленников, поэтому каждый пользователь может стать потенциальной жертвой. Чтобы этого не случилось, каждому человеку необходимо обеспечивать личную информационную безопасность.

В данном сборнике описываются актуальные угрозы информационной безопасности и приводятся общие рекомендации, которые помогут Вам избежать возможных рисков, возникающих при работе в сети Интернет. Описание конкретных шагов по настройке программного обеспечения в соответсвии с приведёнными рекомендациями можете посмотреть на сайте www.safe-surf.ru.

В сборнике представлены четыре раздела:

– актуальные угрозы;

– рекомендации по обеспечению базового уровня защиты персонального компьютера;

– правила работы в сети Интернет;

– безопасное использование современных технологий.

СОДЕРЖАНИЕ

1 РАЗДЕЛ

АКТУАЛЬНЫЕ УГРОЗЫ

Целью большинства современных компьютерных атак является получение финансовой выгоды злоумышленником. Исходя из этого, компьютер обычного пользователя может быть использован злоумышленником при шантаже (заражение вредоносной программой-вымогателем) или незаметно для пользователя включен в бот-сеть для реализации масштабных компьютерных атак на различные цели.

Методы, которые злоумышленники используют в ходе проведения компьютерных атак, можно условно разделить на технические и социальные.

К техническим методам относятся: использование вредоносного программного обеспечения, эксплуатация уязвимостей и другие средства, с помощью которых происходит заражение компьютера и похищение пользовательской информации.

Социальным методом проведения компьютерных атак является социальная инженерия, применяя которую злоумышленники обманными путями могут получить информацию или заставить пользователя совершить необходимые им действия.

Вредоносные программы

В основе практически любой компьютерной атаки лежит вредоносная программа.

На компьютер пользователя такая программа может попасть одним из следующих способов:

– через USB-флешки и другие съёмные носители;

– через электронную почту и системы обмена мгновенными сообщениями;

– через заражённые веб-страницы.

Рекомендации

1. Используйте средства антивирусной защиты.
2. Регулярно обновляйте базы данных антивируса.
3. Регулярно обновляйте программное обеспечение.
4. Работайте под учётной записью с ограниченными правами.
5. Отключайте автозапуск подключённых устройств.
6. Используйте межсетевой экран (firewall).
7. Используйте спам-фильтры.
8. Регулярно создавайте резервные копии.

Социальная инженерия

Этот термин обозначает способ получить нужную злоумышленнику информацию или заставить пользователя совершить необходимые действия не используя технические средства, а только применяя психологические методы воздействия на людей: при помощи убеждения, внушения и хитрости.

Стоит отметить, что любой пользователь сети Интернет уязвим к методам социальной инженерии.

Основные пути воздействия на пользователя — это электронная почта, социальные сети, сервисы мгновенного обмена сообщениями и телефон.

В результате действий злоумышленника пользователи добровольно выдают свои данные и совершают действия, зачастую не подозревая, что их обманули.

Рекомендации

1. Не отвечайте на письма от неизвестных отправителей.
2. Не переходите по ссылкам, содержащимся в письмах от неизвестных отправителей.
3. Не сообщайте приватную информацию, запрашиваемую в письмах, приходящих по электронной почте и сообщениях в электронных мессенджерах.

Фишинг

Цель фишинга — получение злоумышленником данных банковской карты пользователя или информации об учётной записи (логине и пароле) на каком-либо ресурсе в сети Интернет.

Инструмент фишинга — поддельная страница сайта с формой для ввода данных или письмо, отправленное якобы от лица администрации или службы поддержки этого онлайн-ресурса, содержащее ссылку на поддельную страницу.

Дизайн формы для ввода данных или поддельного сайта может быть довольно точной копией настоящего ресурса.

Рекомендации

1. Не переходите по ссылкам и не открывайте вложения из писем от неизвестных Вам адресатов.
2. Не сообщайте никому свои логины и пароли учётных записей, а также данные банковских карт.
3. Обращайте внимание на URL-адреса страниц, на которых Вы вводите учётные данные.
4. Проверяйте наличие https-соединения для сайтов, на которых Вы собираетесь ввести учётные данные.
5. Проверяйте реальные адреса гиперссылок, наводя на них курсор. Адрес, куда ведёт эта ссылка, будет отображён в левой нижней части браузера.

Выманивание денег с помощью электронной почты и социальных сетей

С распространением электронной почты и социальных сетей выманивание у жертвы денег с их помощью приняло масштабные формы.

Содержание сообщений может быть самым разным. Расчёт делается только на методы социальной инженерии. В данном виде мошенничества не используются технические средства.

Примером распространённой схемы мошенничества является сбор денег «на лечение ребенка», когда злоумышленники делают рассылки писем якобы от лица благотворительных организаций с просьбами о пожертвованиях.

Рекомендации

1. Не отвечайте на письма от неизвестных адресатов.
2. Проверяйте личность отправителя (организации) письма через поисковые системы или официальные сайты.
3. Если письмо с просьбой о переводе денег пришло от знакомого Вам человека, перезвоните ему и спросите, действительно ли он это отправлял.

Поддельные антивирусы

Поддельные антивирусы могут быть как бесполезной утилитой, приобретенной пользователем за деньги, так и вредоносным программным обеспечением, похищающим данные с компьютера.

Фальшивый антивирус можно получить различными способами. Например, скачав с сомнительного сайта бесплатный антивирус, гарантирующий стопроцентную защиту от всех видов вредоносных программ. Кроме того, поддельные антивирусы распространяются как вложения электронной почты, могут загружаться на уже зараженный компьютер специальным вирусом-загрузчиком.

Рекомендации

1. Используйте только лицензионные антивирусные средства.
2. Скачивайте антивирус только с официального сайта разработчика.
3. Регулярно обновляйте антивирус (обновления должны также загружаться из официальных источников).

Фальшивая техподдержка

Фальшивая техподдержка является одним из методов социальной инженерии. Обычно это звонки по телефону якобы от сотрудников банка или технических специалистов какой-нибудь крупной компании, занимающейся разработкой программного обеспечения.

Злоумышленники заявляют об обнаружении вирусов на компьютере жертвы и, используя непонятные большинству пользователей технические термины, пытаются убедить собеседника предоставить им удалённый доступ к компьютеру или сообщить пароли от учётных записей.

Рекомендации

1. Если Вы получили письмо на электронную почту якобы от сотрудника компании Microsoft или Apple, не сообщайте ему логины и пароли от Ваших учётных записей и не предоставляйте ему удалённый доступ к Вашему компьютеру.

2. Помните, что сотрудники банка не имеют права требовать сообщить им пин-код или CVV/CVC-код Вашей карты.

Контрафактное программное обеспечение

Скачивая пиратское программное обеспечение, пользователь рискует безопасностью компьютера и своих данных, а также подвергает опасности взлома устройства других пользователей.

Использование контрафактного программного обеспечения может привести к следующим последствиям:

– кража личных данных из компьютера;

– использование компьютера как элемента бот-сети;

– потеря данных (выход компьютера из строя);

– нарушение работы другого лицензионного программного обеспечения.

Рекомендации

1. Используйте лицензионное программное обеспечение.
2. Используйте программное обеспечение с открытым исходным кодом (open source).
3. Избегайте передачи личных данных с компьютера, на котором установлено контрафактное программное обеспечение.
4. Регулярно обновляйте антивирусные базы данных и операционную систему.

2 РАЗДЕЛ

БАЗОВЫЙ УРОВЕНЬ ЗАЩИТЫ

Любое современное устройство требует настройки. Это справедливо как для традиционных устройств: компьютеров, телефонов, домашних маршрутизаторов, так и для бытовой техники, всё чаще использующей сеть Интернет и являющейся частью, так называемого, Интернета-вещей.

Обеспечение защиты устройств — это процесс, который сочетает в себе применение и последующее совершенствование технических, организационных и поведенческих мер.

Недостаточно один раз просто установить антивирус, необходимо убедиться, что он регулярно обновляется, обеспечивая защиту от новейших угроз.

Кроме того, необходимо иметь определённый набор знаний и умений, который позволит обеспечить базовый уровень защиты компьютера.

В этом разделе внимание акцентируется на базовых настройках и принципах использования компьютера или другого устройства, использующего сеть Интернет, которые необходимо соблюдать сразу после его покупки.

Учётные записи в операционной системе

Учётная запись — это набор данных, сообщающих операционной системе о том, к каким папкам и файлам пользователь имеет доступ, какие он может делать изменения в работе компьютера, а также о персональных настройках пользователя.

Для пользователя учётная запись — это своего рода ключ к личной информации и персональным данным, хранящимся на компьютере. И этот ключ также нуждается в защите, обеспечить которую помогут следующие рекомендации.

Рекомендации

1. Создавайте отдельные учётные записи пользователя и администратора.
2. Используйте надёжный пароль для каждой учётной записи.
3. Работайте под учётной записью пользователя (с ограниченными правами).
4. При использовании компьютера посторонними людьми создайте гостевую учётную запись с минимальными правами.
5. Ограничьте количество попыток ввода пароля.

Использование паролей

Пароль является средством первой необходимости и первым рубежом защиты персональной информации пользователя.

Современные реалии требуют использование пароля для входа в операционную систему, электронную почту, социальные сети, системы Интернет-банкинга и другие сайты, где хранится чувствительная информация пользователя.

Пароль, как важное средство защиты личных данных, должен быть надёжным, уникальным и хорошо спрятанным. В противном случае утечка данных с какого-либо недостаточно защищенного ресурса или кража пароля позволят злоумышленнику получить доступ ко всем остальным учётным записям пользователя, включая системы Интернет-банкинга.

Рекомендации

1. Используйте уникальный пароль для каждого Интернет-ресурса, сервиса или устройства.
2. Используйте надёжные пароли.
3. Изменяйте пароль, предлагаемый Интернет-сайтом или используемый в устройствах по умолчанию.
4. Изменяйте существующие пароли не реже одного раза в квартал.
5. Избегайте хранения паролей в открытом виде.
6. Используйте менеджер паролей.

Создание надёжных паролей

От качества созданного пользователем пароля напрямую зависит безопасность его данных или денежных средств.

Надёжный пароль — это пароль, который сложно подобрать. Чтобы создать такой пароль, достаточно следовать рекомендациям о минимальной длине, используемом наборе символов и исключить наиболее распространённые комбинации.

Но идеальный пароль — это пароль, который обладает характеристиками надёжного и который можно легко запомнить. Чтобы создать такой пароль, нужно ассоциировать его с конкретным ресурсом.

Например, хорошим паролем для условного сайта www.mail.ru будет — L12i!9A@1m13[1]. В нём буквы соответствуют слову mail набранному в обратной последовательности с меняющимся регистром, цифры — порядковый номер буквы по алфавиту, а специальные знаки « ! » и « @ » ассоциируются с буквами i и A.

1 Использовать приведённый пароль бессмысленно, так как он всем известен. Здесь указана лишь логика создания паролей.

Рекомендации

1. Используйте сочетания символов верхнего и нижнего регистров, цифр и специальных символов.
2. Используйте длинные пароли, более 8 символов.
3. Избегайте использования в паролях дат, имён, номеров телефонов и другой персональной информации, которая может быть угадана или найдена в открытых источниках.
4. Изменяйте существующие пароли не реже одного раза в квартал.
5. Избегайте повторения использованых ранее паролей.
6. Используйте менеджер паролей.

Хранение паролей

Со временем у активного пользователя сети Интернет набирается большое количество надёжных паролей и возникает вопрос об их хранении.

Кто-то считает безопасным записать пароль на бумажке или в заметки на телефоне, кто-то их запоминает, но оптимальным вариантом будет использование специального сервиса или программы — менеджера паролей.

Такая программа позволяет хранить все используемые пароли, независимо от их длины и сложности, в одном файле в зашифрованном виде. К тому же она позволяет автоматически генерировать новые пароли, каталогизировать, осуществлять поиск и управлять существующими паролями. Единственное, что пользователю необходимо будет помнить — это мастер-пароль к зашифрованной базе данных с остальными паролями.

Рекомендации

1. Избегайте хранения Ваших паролей в местах, доступных для посторонних.
2. Избегайте хранения паролей в открытом виде.
3. Регулярно осуществляйте резервное копирование всех паролей.
4. Изменяйте пароль, предлагаемый Интернет-сайтом или используемый в устройствах по умолчанию.
5. Изменяйте существующие пароли не реже одного раза в квартал.
6. Используйте менеджер паролей.

Обновление операционной системы и программного обеспечения

Злоумышленники регулярно находят новые способы и средства внедрения вредоносного программного обеспечения на компьютеры пользователей, используя для этого уязвимости операционных систем и программного обеспечения. В свою очередь разработчики стараются как можно оперативнее устранять обнаруженные уязвимости. Поэтому регулярно выпускают обновленные версии программного обеспечения – более безопасные и защищённые.

Пользователю необходимо поддерживать программное обеспечение, имеющееся на его устройствах, в актуальном состоянии. Проще всего это сделать, включив функцию автоматической установки обновлений, которая присутствует в большинстве современных программ.

Рекомендации

1. Включите функцию автоматической установки критических обновлений для операционной системы.
2. Включите функцию автоматической установки обновления для программного обеспечения.
3. Регулярно проверяйте на сайте производителя появление обновлений для программ, не имеющих функции автоматического обновления, например, для плагинов браузеров.
4. Проверяйте источники, из которых скачиваются обновления для программного обеспечения.
5. Устанавливайте обновления только с официальных сайтов разработчиков.

Резервное копирование данных

Чтобы избежать случайного или несанкционированного удаления информации с компьютера, существует специальная процедура, которая позволяет дублировать важные данные — резервное копирование.

Возможность резервного копирования имеется во всех современных операционных системах, однако, данные сервисы могут иметь ограничения, например, отсутствовие функции экспорта копии на внешний носитель.

Старайтесь регулярно делать копии важных документов, фотографий и другой информации на съёмные носители

Рекомендации

1. Определите, какие файлы представляют для Вас ценность, периодически выполняйте их резервное копирование.
2. Определите период проведения резервного копирования, исходя из степени важности сохраняемых данных.
3. Храните резервные копии на отдельном носителе информации или в облачном хранилище.
4. Используйте шифрование для важных данных.

Антивирусные средства

Антивирусные средства выполняют сканирование наиболее уязвимых областей операционной системы и контролируют возможные пути заражения вирусами, такие как вложения электронной почты и потенциально опасные веб-сайты.

Антивирус должен быть всегда включён.

Современные антивирусные программы, как правило, производят обновление антивирусных баз автоматически. Если автоматическое обновление баз данных по каким-либо причинам невозможно, необходимо осуществлять его в ручном режиме, скачивая архивы обновлений с веб-сайта разработчика и устанавливая их на компьютере.

Рекомендуется периодически проводить полное сканирование системы при помощи антивируса, а также всегда проверять на наличие вирусов все съёмные носители.

Рекомендации

1. Используйте только лицензионные антивирусные средства.
2. Скачивайте антивирус только с официального сайта разработчика.
3. Настройте автоматическое обновление антивируса.
4. Регулярно, не реже одного раза в неделю, обновляйте антивирусные базы вручную, если устройство не имеет выхода в сеть Интернет.

Персональный межсетевой экран

Задача межсетевого экрана — защищать от несанкционированного доступа к компьютеру по сети.

Персональный межсетевой экран — программное обеспечение, которое часто входит в состав наиболее популярных операционных систем или антивирусных приложений.

Особенностью персонального межсетевого экрана является возможность контролировать приложения, которые устанавливают сетевые соединения.

Рекомендации

1. Запретите всем программам доступ к сети по умолчанию.
2. Обращайте внимание на то, каким приложениям Вы разрешаете доступ в сеть.

Работа с браузером

Браузер — это программа, которая позволяет просматривать веб-страницы. По умолчанию браузер хранит всю информацию, которую вводит пользователь: адреса сайтов, имена загружаемых файлов, пароли, включая персональные данные и реквизиты для совершения финансовых операций.

Для сохранения приватности этих данных важно настроить браузер.

Рекомендации

1. Настройте автоматическое обновление браузера.
2. Настройте автоматическое удаление cookie-файлов после завершения каждого сеанса работы или периодически удаляйте их вручную.
3. Отключите функцию запоминания паролей.
4. Отключите функцию синхронизации между компьютерами.
5. Отключите отслеживание местоположения.
6. Отключите поддержку JavaScript.
7. Удалите все неиспользуемые расширения.
8. Включите блокировку всплывающих окон.
9. Включите защиту от фишинга
10. Включите запрос на разрешение запуска плагинов.
11. Используйте для совершения финансовых операций и операций с персональными данными в сети Интернет браузер в режиме «приватного просмотра».

Файлы cookies

Файлы cookies представляют собой текстовые файлы, сохраняющие некоторую информацию о посещении пользователем сайтов. Их основное назначение — сделать использование сети Интернет удобным: позволить сайтам «узнавать» пользователя при его повторном посещении или позволить совершать покупку нескольких товаров в онлайн-магазине.

Опасность приёма и хранения cookie-файлов со всех сайтов заключается в возможности отследить перемещение пользователя по сайтам, а также составить представление об его интересах.

Кроме того, перехватив cookie-файл, злоумышленники могут получить доступ к какому-либо сайту, не имея аутентификационных данных пользователя: логина и пароля.

Рекомендации

1. Настроите хранение cookie-файлов только в течение одного сеанса и их удаление при закрытии браузера.
2. Отключите приём cookie-файлов со сторонних сайтов.
3. Используйте специальные приложения или расширения для браузеров, позволяющие анализировать и управлять сохранёнными cookie-файлами.

Расширения браузера

Механизм расширений в браузере позволяет дополнить стандартный функционал браузера, добавив, например, средства по анализу цен в интернет-магазинах, блокировку рекламы и т.д.

Однако стоит помнить, что расширения — это отдельное программное обеспечение, запускаемое от имени пользователя и имеющее свои собственные уязвимости. А главное, расширения могут получать доступ к любой информации, вводимой пользователем в браузере, и передавать её третьим лицам для обработки.

Рекомендации

1. Устанавливайте расширения только из официального магазина приложений.
2. Удалите все неиспользуемые расширения.
3. Используйте для совершения финансовых операций и операций с персональными данными в сети Интернет браузер без расширений, либо включайте режим «приватного просмотра».
4. Регулярно обновляйте расширения браузеров вручную.
5. Обращайте внимание, на доступ к какой информации расширение запрашивает разрешение.

3 РАЗДЕЛ

ПРАВИЛА РАБОТЫ В СЕТИ ИНТЕРНЕТ

Сеть Интернет предоставляет пользователю множество возможностей — это и получение необходимой информации, и общение, и совершение покупок, и проведение онлайн-платежей.

Наряду со всеми своими преимуществами сеть Интернет является небезопасной средой, в которой пользователя подстерегают риски заражения компьютера вредоносными программами, кражи персональных данных, учётных записей и денежных средств.

Как и в обычной жизни в виртуальном пространстве нужно следовать определённым правилам безопасности, избегать рисков, чтобы не стать жертвой злоумышленников.

Структура URL адресов

Все страницы, размещённые в сети Интернет, имеют уникальный адрес, который представляет собой определённую последовательность цифр.

Для удобства пользователей была введена символьная интерпретация для адресов сайтов в сети Интернет, которая получила название URL — универсальный указатель ресурса.

Обманные приемы, используемые мошенниками, следующие:

– создание сайта с URL, похожим на URL уже существующего сайта;

– использование ссылок с сокращённой формой представления URL;

– использование цифрового представления адреса сайта;

– подделка гиперссылок.

Рекомендации

1. Включите в настройках браузера полное отображение URL адреса.
2. Оценивайте URL: если кажется, что использован один из обманных приёмов, лучше по этой ссылке не переходить.
3. Проверяйте URL адрес незнакомой страницы при помощи поисковых систем.
4. Проверяйте реальные адреса гиперссылок, скрытых за текстом или изображением.
5. Используйте сервисы проверки безопасности Интернет-страниц.

Определение степени доверия к сайтам

Когда большинство источников информации и услуг, включая государственные, размещено в сети Интернет, возникает вопрос о способах определения степени доверия к сайтам. Нередки случаи, когда страницы создаются мошенниками для выманивания денежных средств или персональных данных пользователей.

Рекомендации

1. Включите в настройках браузера полное отображение URL-адреса сайта.
2. Оценивайте URL: если кажется, что использован один из обманных приёмов, лучше по этой ссылке не переходить.
3. Оценивайте внешний вид сайта, качество его материалов и наличие контактов обратной связи.
4. Проверяйте наличие https-соединения (значок замка в строке URL-адреса) у сайтов, работающих с персональными данными или тех, где совершаются денежные операции.
5. Проверяйте наличие и содержание политики конфиденциальности персональных данных для сайтов, где требуется их ввод.
6. Используйте подтверждение совершения платежей через одноразовые пароли или SMS-код.
7. Проверяйте сайты через ресурсы по проверке подлинности сайтов.

Безопасное использование электронной почты

Многие сервисы в сети Интернет используют адрес электронной почты в качестве логина для осуществления аутентификации пользователя, или инструмента восстановления пароля. В том числе сервисы, совершающие финансовые операции.

Получив доступ к Вашей электронной почте, злоумышленник сможет не только прочитать личную переписку, но и получить доступ к Интернет-ресурсам, где данный адрес использовался для регистрации. Исходя из этого, защита электронной почты становится одной из основных и приоритетных задач для пользователя.

Не стоит забывать, что по электронной почте могут приходить не только «полезные» письма, но и письма фишинговой и спам рассылок.

Рекомендации

1. Используйте шифрование при доступе к электронной почте: https-соединение через браузер, и протокол SSL для почтовых программ.
2. Используйте двухфакторную авторизацию для доступа к электронной почте и номер телефона для восстановления её пароля.
3. Создавайте надёжные пароли для доступа к электронной почте и меняйте их не реже, чем раз в квартал.
4. Избегайте использования для контрольного вопроса информации, которую можно угадать или получить из социальных сетей.
5. Используйте шифрование при доступе к электронной почте через общественные Wi-Fi-сети.
6. Игнорируйте вложения и не переходите по ссылкам из писем, полученных от неизвестных отправителей.
7. Используйте разные адреса электронной почты для деловой переписки, совершения финансовых операций и регистрации в различных социальных сетях и сайтах.
8. Установите на компьютер средство антивирусной защиты и регулярно обновляйте антивирусные базы.
9. Регулярно обновляйте операционную систему и программное обеспечение.

Безопасный поиск в сети Интернет

Практически все пользователи сети Интернет, когда-нибудь использовали поисковые системы, не подозревая о возможных угрозах, связанных с ними.

Сайты, полученные в поисковой выдаче, могут содержать некорректную, недостоверную или ложную информацию, а также стать причиной проникновения на компьютер пользователя вредоносной программы.

Кроме этого, поисковые системы составляют «профиль» пользователя, собирая и объединяя любую доступную им информацию, будь то предмет и история поиска, профиль социальной сети или отметка местоположения пользователя через смартфон. Всё, что когда-либо было опубликовано человеком в сети, будет найдено и сохранено.

Рекомендации

1. Оценивайте URL-адреса сайтов, выдаваемых поисковыми системами, прежде, чем перейти на них.
2. Используйте антивирусные средства защиты и регулярно обновляйте их.
3. Проверяйте достоверность информации, полученной из сети Интернет, с помощью нескольких источников информации.
4. Проверяйте информацию, которую поисковые системы выдают о Вас.
5. Следите за тем, какие данные Вы оставляете при регистрации на том или ином ресурсе.
6. Избегайте размещения избыточной информации о себе.
7. Ознакомьтесь с политикой конфиденциальности ресурса, где оставляете персональные данные.

Интернет-платежи

Электронные платежи стали неотъемлемой частью нашей повседневной жизни. Это быстро и удобно, однако платой за удобство становится повышенное внимание со стороны злоумышленников. Учитывая, что получение финансовой выгоды — это их основная цель, важно знать методы мошенников, а также уметь от них защититься и быть бдительным при совершении покупок.

Рекомендации

1. Оценивайте URL и внешний вид сайта, качество его материалов и наличие контактов обратной связи.
2. Проверяйте наличие https-соединения у сайтов, на которых Вы собираетесь вводить персональные данные и реквизиты банковских карт.
3. Используйте двухфакторную авторизацию: одноразовые пароли или подтверждение с помощью SMS-кода.
4. Избегайте использования компьютеров в общественных местах, а также общественных точек доступа к Wi-Fi-сети для осуществления Интернет-платежей.
5. Используйте браузер без расширений либо включайте в браузере режим «приватного просмотра».
6. Используйте надёжные пароли.

Социальные сети

Социальные сети предоставляют уникальную возможность поддерживать и заводить новые дружеские и деловые связи по всему миру.

В то же время социальные сети являются удобной площадкой для распространения спама, мошеннических сообщений и вредоносных программ, а также сбора персональных данных.

Пользователи склонны больше доверять тем, кто входит в список их «друзей» в социальной сети, публикуя чувствительную информацию, при этом забывая, что размещают её в открытом доступе, а под «друзьями» могут скрываться совсем незнакомые люди.

Рекомендации

1. Избегайте добавления в друзья в социальных сетях всех подряд, контролируйте, к какой информации Вы даёте доступ новому контакту.
2. Ограничьте количество личной информации, размещаемой в социальных сетях, сделайте её доступной только для группы близких друзей.
3. Уточните с помощью другого средства связи, действительно ли человек отправлял Вам просьбу, даже если она пришла от знакомого Вам человека.
4. Избегайте переходов по ссылкам, полученным в социальных сетях.
5. Старайтесь не принимать файлы в социальных сетях, если Вы не обговорили это заранее.
6. Проявляйте осторожность при установке приложений или дополнений для социальных сетей.

4 РАЗДЕЛ

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ

Развитие современных технологий, упрощает многие сферы деятельности человека. Наибольшей популярностью пользуются устройства, имеющие выход в сеть Интернет. Благодаря им пользователь всегда может быть в курсе последних новостей, просматривать медиа-контент, связываться с другими пользователями, совершать финансовые операции и управлять бытовой техникой у себя дома.

Но наряду с достоинствами присутствуют и угрозы, которым могут быть подвержены данные устройства при недостаточной степени их защиты. Безопасное использование современных технологий позволит не только защитить свои устройства от взлома, но и сохранить личную информацию и денежные средства.

Безопасность домашней Wi-Fi-сети

Большинство людей пользуется преимуществом беспроводных технологий дома. На данный момент домашние Wi-Fi-сети широко распространены, так как они позволяют подключить личные устройства к сети Интернет с помощью беспроводного соединения.

Однако немногие уделяют внимание настройке сердца этой системы — домашнего Wi-Fi-роутера, указывая только параметры, необходимые для подключения к сети провайдера, и оставляя другие настройки по умолчанию. В этом случае, не обеспечивается надлежащая безопасность, и доступ к устройству могут получить злоумышленники.

Рекомендации

1. Перед первым использованием смените пароль и логин доступа к интерфейсу роутера, установленные по умолчанию.
2. Настройте шифрование с использованием современных алгоритмов (WPA2) и надёжный пароль на подключение к сети.
3. Скройте название домашней сети (SSID).
4. Ограничьте число устройств с доступом в сеть Интернет.
5. Настройте межсетевой экран роутера.
6. Уменьшите радиус действия Wi-Fi-сети, если такая опция поддерживается Вашим роутером.
7. Запретите доступ к настройкам точки доступа или роутера через беспроводную сеть.

Общественная Wi-Fi-сеть

В настоящее время к беспроводным Wi-Fi-сетям можно подключиться в общественном транспорте, кафе, магазинах.

При всех своих достоинствах беспроводная связь более опасна по сравнению с проводной. Для перехвата информации в открытых беспроводных сетях злоумышленнику достаточно просто подключиться к ней.

Рекомендации

1. Проверяйте наличие https-соединения у сайтов, на которых Вы собираетесь вводить персональные данные.
2. Используйте двухфакторную авторизацию: одноразовые пароли или подтверждение с помощью SMS-кода.
3. Выбирайте точки доступа с включенным шифрованием (на подключение к которым установлен пароль). Пароль можно уточнить у владельца общественной точки доступа
4. Избегайте подключения к открытым Wi-Fi-сетям для передачи конфиденциальной информации.

Безопасность мобильных устройств

Доверяя всё больше личной информации смартфонам и планшетам, их владельцы часто забывают о соблюдении элементарных правил безопасности. Между тем, количество преступлений, связанных с похищением персональных данных, растёт с каждым днём.

Особый интерес для мошенников представляют данные для входа в различные финансовые системы, доступа к сайтам, почтовым ящикам, онлайн-играм, а также найденные на устройстве адреса электронной почты и номера телефонов.

Рекомендации

1. Не оставляйте устройство без присмотра.
2. Настройте автоматическую блокировку устройства.
3. Выходите из всех аккаунтов, когда прекращаете работу с устройством.
4. Используйте шифрование данных и выполняйте резервное копирование.
5. Устанавливайте программное обеспечение только из магазина приложений.
6. Регулярно обновляйте программное обеспечение и операционную систему.
7. Установите лицензионное антивирусное ПО.
8. Используйте защищенные точки доступа к Wi-Fi-сети.
9. Отключайте Wi-Fi и Bluetooth, если в данный момент они не используются.
10. Не открывайте вложения и ссылки, поступившие от неизвестных адресатов.
11. При переходе через QR-код по распознанной ссылке убедитесь, что она привела именно на ожидаемый сайт.

Интернет вещей

Интернет вещей — система взаимодействия электронных устройств, имеющих выход в сеть для выполнения определённых функций. Всевозможные устройства: автомобили и бытовые приборы, системы безопасности и личные вещи, то есть, практически все окружающие нас вещи, могут быть со временем подключены к беспроводной сети.

В то же время у большинства устройств Интернета вещей беспроводной трафик не шифруется, а веб-интерфейс имеет небезопасную организацию доступа.

По факту, устройства Интернета вещей осуществляют сбор персональных данных, отслеживают перемещения своих хозяев, получают информацию об их привычках, следят через камеры в бытовых устройствах. Получив доступ к подобной информации, злоумышленник может не только следить за жертвой, но и вторгаться в её личную жизнь.

Рекомендации

1. Перед принятием решения о приобритении устройства ознакомьтесь на официальном сайте с производителя с пользовательским соглашением.
2. Перед началом использования измените настройки авторизации, заданные по умолчанию.
3. Используйте надёжные пароли для подключения.
4. Устанавливайте на устройства последние обновления безопасности и новейшие версии прошивок.
5. При возможности используйте шифрование каналов связи.
6. Разделяйте домашние сети: для Интернета вещей и для личного использования.
7. Скройте беспроводную сеть.
8. Отключайте удаленный доступ, если он не требуется.
9. Контролируйте к какой информации устройство запрашивает доступ.

Сборник «Рекомендации по безопаному использованию сети Интернет» подготовлен на основе материалов сайта «Безопасность пользователей в сети Интренет» (www.safe-surf.ru).