Основные опасности в интернете

Пользователи интернета подвергаются целому ряду потенциальных угроз. Ландшафт угроз постоянно меняется, а киберпреступники изобретают новые способы атак на интернет-пользователей. Вот лишь основной список опасностей при использовании интернета:

Кража идентификационных данных
Утечки данных
Вредоносные программы и вирусы
Фишинговые и мошеннические электронные письма
Поддельные сайты
Интернет-мошенничество
Мошенничество на сайтах и в приложениях для знакомств
Неприемлемый контент
Кибербуллинг
Неверные настройки конфиденциальности

Основные рекомендации по безопасности в интернете

Чтобы избежать перечисленных опасностей, важно знать и соблюдать основные правила работы в интернете:

№1. Убедитесь, что ваше интернет-соединение защищено

При использовании общедоступного Wi-Fi для выхода в сеть в общественном месте у вас отсутствует контроль над его безопасностью. Использование общедоступного Wi-Fi не всегда безопасно, однако может оказаться неизбежным, если вы находитесь вне дома. Если вы используете общедоступный Wi-Fi, избегайте выполнения таких операций как онлайн-банкинг и онлайн-покупки.

Если эти операции необходимы, используйте виртуальную частную сеть (VPN). VPN обеспечивает безопасность данных, передаваемых по незащищенной сети. Если вы не используете VPN, воздержитесь от совершения личных транзакций до момента, когда появится возможность надежного подключения к интернету.

№2. Используйте надежные пароли

Пароли – одно из самых слабых мест в системе кибербезопасности. Пользователи часто создают пароли, которые легко запомнить а, следовательно, злоумышленникам не составит труда их подобрать. Кроме того, опасно использовать один и тот же пароль для нескольких сайтов, поскольку, получив учетные данные с одного сайта, злоумышленники могут получить доступ к другим сайтам, на которых используются эти же учетные данные.

Выбирайте надежные пароли, подбор которых вызовет сложности у киберпреступников. Надежный пароль обладает следующими свойствами:

Длинный: минимум 12 символов, в идеале, даже больше.
Содержит заглавные и строчные буквы, а также специальные символы и цифры.
Не очевидный: в пароле не используются комбинации последовательных цифр (1234) и личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного.
Не содержит запоминающихся сочетаний клавиш.
В этом случае может оказаться полезным использование менеджера паролей. Менеджеры паролей помогают создавать надежные пароли, хранить их в цифровом хранилище, защищенном единым мастер-паролем, и получать их при входе в учетные записи.

№3. По возможности включите многофакторную аутентификацию

Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используются два или более метода проверки. Например, вместо простого запроса имени пользователя или пароля, при многофакторной аутентификации запрашивается дополнительная информация:
Дополнительный одноразовый пароль, который серверы аутентификации веб-сайта отправляют на телефон или электронную почту.
Ответы на личные вопросы безопасности.
Отпечаток пальца или другая биометрическая информация, например, голосовые данные или распознавание лица.
Многофакторная аутентификация снижает вероятность кибератаки. Чтобы защитить онлайн-аккаунты, рекомендуется по возможности использовать многофакторную аутентификацию. Для обеспечения безопасности в интернете можно также применять сторонние приложения проверки подлинности, такие как Google Authenticator и Authy.

№4. Поддерживайте программное обеспечение и операционные системы в актуальном состоянии

Поддерживайте актуальное состояние всех используемых операционных систем и приложений. Разработчики постоянно работают над безопасностью продуктов, отслеживая последние угрозы и выпуская исправления безопасности в случае обнаружения уязвимостей. Использование последних версий операционных систем и приложений позволяет применять последние исправления безопасности. Это особенно важно для приложений, содержащих платежные данные, информацию о состоянии здоровья и прочую конфиденциальную информацию.

№5. Убедитесь, что веб-сайты выглядят и работают надежно

Надежность – важный атрибут всех посещаемых веб-сайтов, особенно тех, на которых осуществляются транзакции, таких как сайты электронной коммерции. Следует обратить внимание, имеется ли у сайта актуальный сертификат безопасности. Убедитесь, что веб-адрес сайта

начинается с HTTPS, а не с HTTP (S означает «безопасный»), и что в адресной строке отображается значок замка. Другие признаки надежности сайта включают:

Грамматически правильный текст без орфографических и пунктуационных ошибок. Авторитетные бренды прикладывают значительные усилия для обеспечения надлежащего качества своих веб-сайтов.

Качественные изображения, соответствующие ширине экрана.

Объявления, органично вписанные в структуру сайта и не перегружающие его.

№6. Оцените и ознакомьтесь с параметрами и политиками конфиденциальности

Маркетологи, как и злоумышленники, хотят знать о вас все. Они могут получить эту информацию из истории поисковых запросов и социальных сетей. Но вы можете контролировать доступную им информацию. В веб-браузерах и мобильных операционных системах предусмотрены параметры для обеспечения конфиденциальности в интернете. На сайтах социальных сетей, таких как Facebook, Twitter, Instagram, LinkedIn и прочих, предусмотрены параметры для повышения конфиденциальности. Потратив некоторое время на детальное изучение параметров конфиденциальности, установите их на комфортном для вас уровне.

Многие из нас принимают политики конфиденциальности, не читая. Однако огромное количество данных обрабатывается в маркетинговых и рекламных целях, поэтому рекомендуется ознакомиться с политиками конфиденциальности используемых веб-сайтов и приложений и понять, как собираются и используются данные. Но даже если вы установили частные параметры конфиденциальности, не следует забывать, что ничего в интернете не является полностью конфиденциальным. Злоумышленники, администраторы веб-сайтов и правоохранительные органы могут иметь доступ к информации, которую вы считаете частной.

№7. Следите, по каким ссылкам вы переходите

Один неосторожный переход по ссылке – и ваши личные данные попали к злоумышленникам или устройство заразилось вредоносной программой. Поэтому важно внимательно переходить по ссылкам и избегать определенных типов контента: ссылок из ненадежных источников, спам-сообщений, онлайн-викторин, кликбейтных заголовков, «бесплатных» предложений и нежелательной рекламы.

При получении электронного письма, в подлинности которого вы сомневаетесь, не переходите по содержащимся в нем ссылкам и не открывайте вложения.

Рекомендуется вообще не открывать такие сообщения. Если вы не уверены в подлинности электронного письма, обратитесь непосредственно к отправителю. Например, позвоните в банк и спросите, является ли полученное сообщение подлинным.

При просмотре сайта, убедитесь, что переход по ссылкам осуществляется на страницы со связанным или ожидаемым содержимым. Например, если вы переходите по ссылке, которая, как вам кажется, ведет на описание сафари в

Африке, но вместо этого попадете на кликбейтную страницу о том, как похудели знаменитости или на статью с заголовком «Где они сейчас?», немедленно покиньте эту страницу.

№8. Обеспечьте защиту устройств

По данным одного из отчетов, почти треть пользователей смартфонов не использует пароли, блокировку экрана и другие функции безопасности для защиты телефонов. Рекомендуется использовать пароли, секретные коды и другие средства безопасности, такие как считывание отпечатков пальцев или технологию распознавания лица на всех устройствах: телефонах, компьютерах, планшетах, умных часах, умных телевизорах и других устройствах.

№9. Регулярно выполняйте резервное копирование

Следует иметь резервные копии важной личной информации на внешних жестких дисках и регулярно создавать новые резервные копии. Программы-вымогатели – это тип вредоносных программ, блокирующих компьютер и не позволяющих получить доступ к важным файлам. Резервное копирование данных помогает минимизировать негативные последствия атак программ-вымогателей.

№10. Удаляйте неиспользуемые учетные записи

У многих есть устаревшие неиспользуемые учетные записи. Их наличие может стать источником уязвимостей при использовании интернета. Старые учетные записи с большей вероятностью имеют более слабые пароли, а сайты, на которых они использовались, могут иметь ненадежную политику защиты данных. Кроме того, по данным в старых профилях социальных сетей киберпреступники могут собрать о вас различные данные, например, дату рождения и местонахождение, и составить базовое представление.

№11. Будьте осторожны с загружаемыми из интернета объектами

Основная цель киберпреступников – обманным путем заставить пользователя загрузить вредоносные программы. Вредоносные программы могут быть замаскированы под различные приложения, от популярных игр до приложений для проверки трафика или погоды, или скрыты на подготовленных злоумышленниками веб-сайтах, с которых предпринимается попытка установить вредоносные программы на устройство.

Вредоносные программы наносят ущерб: нарушают работу устройства, крадут личные данные, предоставляют несанкционированный доступ к компьютеру. Обычно для загрузки вредоносных программ требуется ряд действия со стороны пользователя, но встречается также заражение путем скрытой загрузки, когда веб-сайт пытается установить вредоносные программы на компьютер, не спрашивая предварительного разрешения. Будьте осторожны при загрузке объектов на устройство, загружайте контент только из надежных или официальных источников.

№12. Будьте осторожны с информацией, публикуемой в интернете

В интернете нет возможности удаления опубликованной информации. Все опубликованные комментарии и изображения могут навсегда остаться в сети, поскольку при удалении оригинала не происходит удаление копий, которые могли сделать другие пользователи. После публикации комментария уже нет возможности «взять свои слова обратно», также невозможно удалить опубликованное компрометирующее изображение. Если вы не хотели бы, чтобы вашу публикацию увидели родители или потенциальный работодатель, не стоит публиковать этот материал.

Так же будьте осторожны, публикуя личную информацию в интернете: не указывайте адрес и дату рождения в биографических данных социальных сетей. В реальной жизни вы бы не сообщали личные данные незнакомцам, аналогично не следует публиковать их в интернете и делать доступными миллионам пользователей.

Соблюдайте осторожность при предоставлении адреса электронной почты. Полезно иметь дополнительную временную учетную запись электронной почты, используемую исключительно для регистрации и подписки. Она должна отличаться от рабочей и от используемой для переписки с друзьями и близкими.

№13: Будьте осторожны при знакомствах в интернете

Ваши интернет-знакомые не всегда являются теми, за кого себя выдают. Они могут даже не являться реальными людьми. Используя поддельные профили в социальных сетях, злоумышленники охотятся за неосторожными пользователями с целью кражи их средств. К социальной жизни в интернете стоит относиться с такой же осторожностью, как и к социальной жизни в реальном мире. Это особенно важно в связи с возросшим в последние годы количеством случаев мошенничества в сфере онлайн-знакомств.

№14. Перепроверяйте найденную в интернете информацию

К сожалению, в интернете присутствует большое количество поддельных новостей и ложных сведений. В потоке получаемой ежедневно информации легко потеряться. Если вы сомневаетесь в достоверности прочитанной информации, проведите собственное исследование и установите реальные факты. На надежных веб-сайтах, как правило, приводятся ссылки на первоисточники, а на подозрительных страницах вообще не приведено никаких ссылок. Вы можете ознакомиться с рекомендациями по выявлению фейковых новостей.

№ 15. Используйте надежное антивирусное решение и регулярно обновляйте его

Помимо соблюдения рекомендаций по обеспечению безопасности в интернете, важно использовать надежное антивирусное решение. Программное обеспечение для безопасности в интернете защищает устройства и данные и блокирует не только распространенные угрозы, такие как вирусы и вредоносные программы, но и комплексные атаки с использованием приложений-шпионов, шифровальщиков и межсайтового скриптинга. Аналогично операционным системам и приложениям, также важно регулярно обновлять антивирус для защиты от новейших киберугроз.