Title: Безопасность в интернет-сети: важные рекомендации

Description: Важность обеспечения личной безопасности при использовании интернета. Правила создания паролей. Опасность вирусных программ. Атаки по электронной почте и в соцсетях. Как защититься от злоумышленников?

Безопасность в интернете H1

Население цивилизованных стран с каждым годом все больше времени проводит в интернете. Работаете вы удаленно, отвечаете на электронные письма, ищете информацию в Google или общаетесь с друзьями в социальных сетях — вы подключены к интернету.

Более 30% населения планеты ежедневно пользуются интернетом. Параллельно тому как число пользователей интернета увеличивается и приближается к 2 миллиардам, необходимость серьезного отношения к безопасности в интернете становится все более очевидной.

Правила безопасности в интернете H2

Когда дело доходит до компьютерной безопасности мы часто ведем себя безрассудно. Жертвы киберпреступников самостоятельно отдают злоумышленникам свои личные данные, открывают подозрительные ссылки и совершают прочие необдуманные действия.

Компьютеры, не защищенные антивирусами, становятся легкой добычей для вредоносных программ. А пользователи соцсетей размещают в публичном доступе информацию, необходимую мошенникам для доступа к банковским счетам.

Умение защищать конфиденциальные данные в интернете — это навык, необходимый каждому пользователю. Для того чтобы обеспечить собственную безопасность, достаточно использовать несколько простых инструментов и следовать простейшим правилам безопасности в интернет-пространстве.

Используйте надежные пароли H3

Одна из основных опасностей, которая грозит каждому пользователю — это взлом учетных записей. Пользуясь вашей неосторожностью злоумышленники могут добыть банковские реквизиты и конфиденциальную личную информацию.

Предотвратить это можно, руководствуясь рекомендациями по составлению надежных паролей для защиты данных. Список этих рекомендаций довольно короткий:

- пароль должен содержать не менее 8-ми символов;

- в нем должны быть цифры, латински буквы верхнего и нижнего регистра и символы;
- для каждого аккаунта необходимо создавать новый пароль.

Таким образом вы обезопасите себя от большинства тактик, используемых злоумышленниками для получения личных данных.

Избегайте вирусов H3

Будьте осторожны с файлами и ссылками, которые находите на подозрительных ресурсах. Киберпреступники могут использовать их, для заражения вашего устройства вредоносными программами.

Необходимо с осторожностью относиться к подозрительным источникам. Если 10 лет назад злоумышленники отправляли сообщения с вирусами случайным пользователям, то сейчас большинство из них использует гораздо более хитрые методы.

Киберпреступник может написать вам с поддельного профиля знаменитости, или знакомого вам человека. Кроме того, он может взломать аккаунты обычных пользователей и использовать их для распространения вредоносного программного обеспечения (ПО).

Для своевременного обнаружения и удаления вредоносных программ с вашего устройства, необходимо установить качественный антивирус. Данное программное обеспечение будет уведомлять вас о подозрительных веб-сайтах и файлах.

Будьте осторожны с подозрительными письмами H3

E-mail рассылки — еще один популярный инструмент, часто используемых хакерами для распространения вредоносных программ. Вы можете получить письмо с заманчивым рекламным предложением, которое будет содержать ссылку на скачивание вредоносного ПО.

Часто пользователи даже не осознают, что скачали зараженный файл. Загрузка начинается автоматически и длится всего несколько секунд. А обнаружить подобный файл в системе может только антивирусная программа.

Письма злоумышленников также могут содержать ссылки на сайты, копирующие популярные ресурсы. Никогда не вводите свои личные данные, переходя по таким ссылкам, иначе ними сразу завладеют преступники.

Защититься от атак по электронной почте проще чем от любых других угроз. Достаточно просто не открывать подозрительные письма и, самое главное, не переходить по ссылкам, которые в них содержатся.

Проверяйте контакты в социальных сетях H3

Социальные сети, похоже, являются главной мишенью в наши дни. Обманывать людей, используя уже взломанный аккаунт в Facebook и запуская функцию

"Доверенный контакт" — один из наиболее распространенных способов кражи личных данных.

Лучший способ защититься от мошенничества с "Доверенным контактом" в Facebook — связаться с другом напрямую. Не по электронной почте или в SMS, а лично или по телефону.

Подключите двухфакторную аутентификацию H3

Двухфакторная аутентификация — отличный способ дополнительно повысить уровень безопасности. Вместо того чтобы просто войти в аккаунт с помощью имени пользователя и пароля, вам необходимо будет подтвердить свою личность через второй источник.

К примеру, для входа в аккаунт Facebook необходимо будет ввести в соответствующем поле код из SMS. Таким образом, даже заполучив ваш логин и пароль, преступник не сможет получить доступ к учетной записи.

Безопасность в интернете для детей H2

Дети с раннего возраста начинают пользоваться устройствами, с доступом к интернету. Неважно, будет ли это смартфон, планшет или компьютер, вы должны убедиться, что ребенок сможет безопасно использовать интернет ресурсы.

Поэтому важно обучить его основам интернет-безопасности и установить на устройстве родительский контроль. Так вы гарантируете, что юный пользователь не посетит нежелательные ресурсы.

Важно понимать, что установка средств контроля не обеспечит абсолютной безопасности. Серия воспитательных бесед будет гораздо эффективнее любых электронных защитных средств.

Современные дети и подростки воспринимают девайсы и Интернет, как неотъемлемую часть собственной жизни. Они также склонны размещать большое количество личной информации в социальных сетях.

Злоумышленники могут использовать эти данные для подбора паролей или ответов на общие вопросы безопасности. Поэтому очень важно проводить с детьми беседы на следующие темы:

- ответственное использование личных данных;
- правила поведения в Интернете;
- принципы общения с пользователями.

Эти меры предосторожности сведут к минимуму риск того, что ваш ребенок попадется на удочку мошенников.

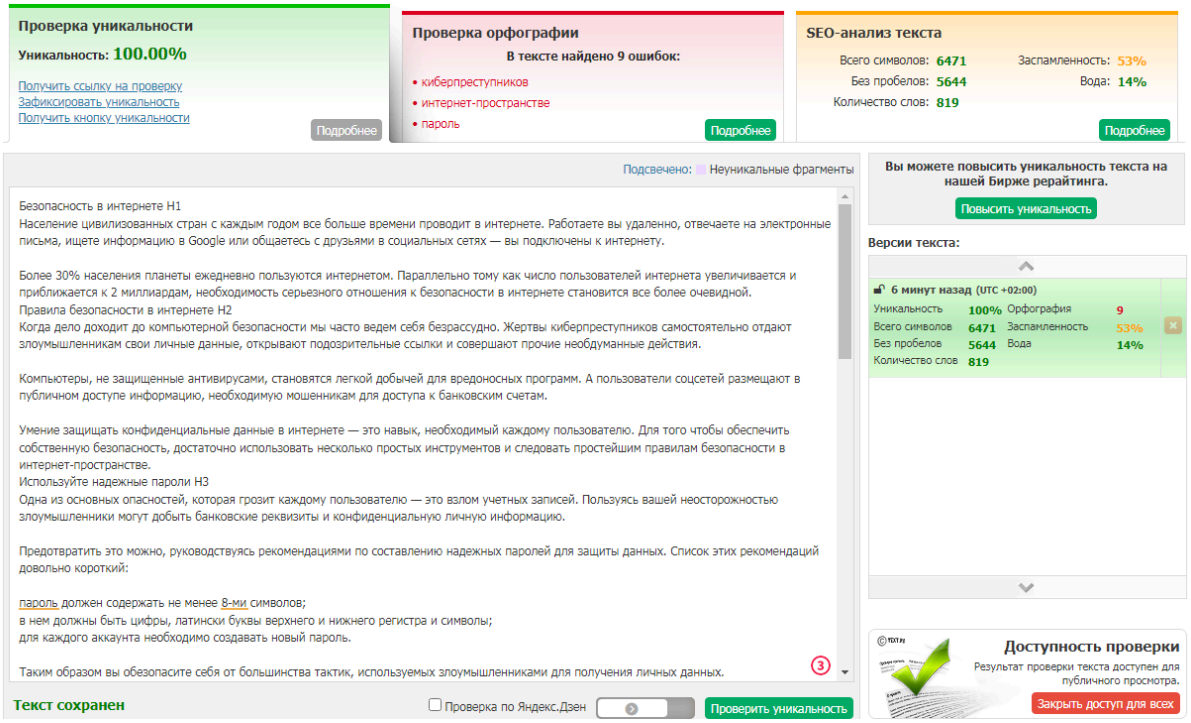
Вывод H2

Кибератаки могут быть разрушительными и происходят во всех уголках интернета. Если крупные корпорации становятся жертвами злоумышленников, то и вы, несомненно, будете уязвимы. От фишинговых атак по электронной почте до случайной загрузки вредоносных программ, похищающих информацию — жертвой может стать каждый.

Мошенники могут использовать разные инструменты и ухищрения для того, чтобы украсть ваши данные или заразить устройство вредоносной программой. Но вы легко сможете избежать каждой из этих угроз, если будете следовать простейшим правилам безопасности в интернет-сети.

_____

Уникальность: 100%
Заспам: 53%
Вода: 14%
https://text.ru/antiplagiat/61b8d9f31697c



Title: Безпека в інтернет-мережі: важливі рекомендації

Опис: Важливість забезпечення особистої безпеки при використанні Інтернету. Правила створення паролів. Небезпека вірусних програм. Атаки електронною поштою і в соцмережах. Як захиститися від зловмисників?

Безпека в Інтернеті H1

Населення цивілізованих країн з кожним роком все більше часу проводить в Інтернеті. Працюєте ви віддалено, відповідаєте на електронні листи, шукаєте інформацію в Google або спілкуєтеся з друзями в соціальних мережах — ви підключені до Інтернету.

Понад 30% населення планети щодня користуються інтернетом. Паралельно тому як число користувачів Інтернету збільшується і наближається до 2-х мільярдів, необхідність серйозного ставлення до безпеки в Інтернеті стає все більш очевидною.

Правила безпеки в Інтернеті H2

Коли справа доходить до комп'ютерної безпеки ми часто поводимося безрозсудно. Жертви кіберзлочинців самостійно віддають зловмисникам свої особисті дані, відкривають підозрілі посилання і здійснюють інші необдумані дії.

Комп'ютери, не захищені антивірусами, стають легкою здобиччю для шкідливих програм. А користувачі соцмереж розміщують у публічному доступі інформацію, необхідну шахраям для доступу до банківських рахунків.

Уміння захищати конфіденційні дані в Інтернеті — це навичка, необхідна кожному користувачеві. Для того, щоб забезпечити власну безпеку, достатньо використовувати кілька простих інструментів і дотримуватися простих правил безпеки в Інтернет-просторі.

Використовуйте надійні паролі H3

Одна з основних небезпек, яка загрожує кожному користувачеві — це злом облікових записів. Користуючись вашою необережністю зловмисники можуть добути банківські реквізити та конфіденційну особисту інформацію.

Запобігти цьому можна, керуючись рекомендаціями щодо складання надійних паролів для захисту даних. Список цих рекомендацій досить короткий:

- пароль повинен містити не менше 8-ми символів;
- у ньому повинні бути цифри, латинські букви верхнього і нижнього регістра й символи;
- для кожного облікового запису необхідно створювати новий пароль.

Таким чином ви убезпечите себе від більшості тактик, що використовуються зловмисниками для отримання особистих даних.

Уникайте вірусів Н3

Будьте обережні з файлами й посиланнями, які знаходите на підозрілих ресурсах. Кіберзлочинці можуть використовувати їх, для зараження вашого пристрою шкідливими програмами.

Необхідно з обережністю ставитися до підозрілих джерел. Якщо 10 років тому зловмисники відправляли повідомлення з вірусами випадковим користувачам, то зараз більшість з них використовує набагато більш хитрі методи.

Кіберзлочинець може написати вам з підробленого профілю знаменитості, або знайомої вам людини. Крім того, він може зламати акаунти звичайних користувачів і використовувати їх для поширення шкідливого програмного забезпечення (ПЗ).

Для своєчасного виявлення і видалення шкідливих програм з вашого пристрою, необхідно встановити якісний антивірус. Це програмне забезпечення повідомлятиме вас про підозрілі вебсайти та файли.

Будьте обережні з підозрілими листами Н3

E-mail розсилки — ще один популярний інструмент, який часто використовується хакерами для поширення шкідливих програм. Ви можете отримати лист із привабливою рекламною пропозицією, який буде містити посилання на звантаження шкідливого ПЗ.

Часто користувачі навіть не усвідомлюють, що завантажили заражений файл. Завантаження починається автоматично і триває всього кілька секунд. А виявити подібний файл в системі може лише антивірусна програма.

Листи зловмисників також можуть містити посилання на сайти, що копіюють популярні ресурси. Ніколи не вводьте свої особисті дані, переходячи за такими посиланнями, інакше ними відразу заволодіють злочинці.

Захиститися від атак електронною поштою простіше ніж від будь-яких інших загроз. Досить просто не відкривати підозрілі листи та, найголовніше, не переходити за посиланнями, які в них містяться.

Перевіряйте контакти в соціальних мережах Н3

Соціальні медіа, здається, є головною мішенню в наші дні. Обманювати людей, використовуючи вже зламаний аккаунт у Facebook і запускаючи функцію "Довірений контакт" — один з найбільш поширених способів крадіжки особистих даних.

Найкращий спосіб захиститися від шахрайства з "Довіреним контактом" в Facebook — зв'язатися з другом безпосередньо. Не електронною поштою або в SMS, а особисто або телефоном.

Увімкніть двофакторну аутентифікацію H3

Двофакторна аутентифікація — відмінний спосіб додатково підвищити рівень безпеки. Замість того щоб просто увійти в акаунт за допомогою імені користувача і пароля, вам необхідно буде підтвердити свою особу через друге джерело.

Наприклад, для входу в акаунт Facebook необхідно буде ввести у відповідному полі код з SMS. Таким чином, навіть отримавши ваш логін і пароль, злочинець не зможе отримати доступ до облікового запису.

Безпека в Інтернеті для дітей H2

Діти з раннього віку починають користуватися пристроями, з доступом до Інтернету. Неважливо, чи буде це смартфон, планшет або комп'ютер, ви повинні переконатися, що дитина зможе безпечно використовувати Інтернет-ресурси.

Тому важливо навчити її основ інтернет-безпеки та встановити на пристрої батьківський контроль. Так ви гарантуєте, що юний користувач не відвідає небажані ресурси.

Важливо розуміти, що установка засобів контролю не гарантує абсолютної безпеки. Серія виховних бесід буде набагато ефективнішою за будь-які електронні захисні засоби.

Сучасні діти й підлітки сприймають девайси та Інтернет, як невіддільну частину власного життя. Вони також схильні розміщувати велику кількість особистої інформації в соціальних мережах.

Зловмисники можуть використовувати ці дані для підбору паролів або відповідей на загальні питання безпеки. Тому дуже важливо проводити з дітьми бесіди на наступні теми:

- відповідальне використання особистих даних;
- правила поведінки в Інтернеті;
- принципи спілкування з користувачами.

Ці запобіжні заходи зведуть до мінімуму ризик того, що ваша дитина стане жертвою шахраїв.

Висновок H2

Кібератаки можуть бути руйнівними та відбуваються у всіх куточках Інтернету. Якщо великі корпорації стають жертвами зловмисників, то і ви, безсумнівно, будете вразливі. Від фішингових атак електронною поштою до випадкового завантаження шкідливих програм, що викрадають інформацію — жертвою може стати кожен.

Шахраї можуть використовувати різні інструменти й хитрощі для того, щоб вкрасти ваші дані або заразити пристрій шкідливою програмою. Але ви легко зможете уникнути

кожної з цих загроз, якщо будете дотримуватися простих правил безпеки в інтернет-мережі.