Интернет-безопасность: определение и описание

Интернет-безопасность – это безопасность действий и транзакций, совершаемых в интернете. Интернет-безопасность входит в более широкие понятия, такие как кибербезопасность и компьютерная безопасность, и включает безопасность браузера и сети, а также правильное поведение в сети. Проводя значительное время в сети, можно столкнуться со следующими угрозами интернет-безопасности:

- Взлом – получение неавторизованными пользователями доступа к компьютерным системам, учетным записям электронной почты и веб-сайтам.
- Вирусы и вредоносные программы, которые могут повредить данные и сделать системы уязвимыми для других угроз.
- Кража личных данных, например, личной и финансовой информации злоумышленниками.

Частные лица и организации могут защититься от подобных угроз, используя приемы интернет-безопасности.

Распространенные угрозы интернет-безопасности

Чтобы сохранить конфиденциальность и безопасность в интернете, важно знать о различных типах интернет-атак. Ниже описаны распространенные угрозы интернет-безопасности.

Фишинг

Фишинг – это кибератака с использованием поддельных писем. Злоумышленники пытаются обмануть получателей электронной почты, убедив их в подлинности и актуальности сообщения. Например, они маскируют письма под запросы из банка или сообщения от коллег, чтобы пользователи переходили по ссылкам или открывали вложения. Цель атаки состоит в том, чтобы обманным путем заставить пользователей раскрыть личную информацию или загрузить вредоносные программы.

Фишинг – одна из старейших угроз интернет-безопасности, возникшая еще в 1990-х годах. Он остается популярным и сегодня, поскольку является одним из самых дешевых и простых способов кражи информации. В последние годы фишинговые сообщения и используемые методы становятся все более изощренными.

Взлом и удаленный доступ

Злоумышленники всегда стремятся использовать уязвимости частной сети или системы для кражи конфиденциальной информации и данных. Технология удаленного доступа предоставляет им дополнительные возможности. Программное обеспечение для удаленного доступа позволяет пользователям получать доступ к компьютеру и управлять им удаленно. Его использование значительно выросло в период пандемии, когда все больше людей работают удаленно.

Протокол, позволяющий пользователям удаленно управлять компьютером, подключенным к интернету, называется RDP – протокол удаленного рабочего стола. Многие компании, независимо от размера, широко используют RDP, поэтому высоки шансы недостаточно надежной защиты сети. Злоумышленники используют различные методы выявления и эксплуатации уязвимостей RDP, чтобы получить полный доступ к сети и ее

устройствам. Они могут как самостоятельно осуществлять кражу данных, так и продавать учетные данные в даркнете.

Вредоносные программы и вредоносная реклама

Термин вредоносные программы охватывает все программы: вирусы, черви, трояны и прочие, которые злоумышленники используют для нанесения ущерба и кражи конфиденциальной информации. Любое программное обеспечение, предназначенное для повреждения компьютера, сервера или сети, может расцениваться как вредоносное.

Термин «вредоносная реклама» описывает онлайн-рекламу, распространяющую вредоносные программы. Интернет-реклама – это сложная экосистема, включающая веб-сайты рекламодателей, рекламные биржи, рекламные серверы, сети ретаргетинга и сети доставки контента. Злоумышленники используют эту сложность для размещения вредоносного кода там, где рекламодатели и рекламные сети не всегда могут его обнаружить. Пользователи, взаимодействующие с вредоносной рекламой, могут загрузить вредоносные программы на свое устройство или перейти на вредоносные веб-сайты.

Программы-вымогатели

Программы-вымогатели – это вредоносные программы, блокирующие использование компьютера или доступ к определенным файлам на компьютере, пока не будет уплачен выкуп. Они часто распространяются как троянские программы – вредоносные программы, замаскированные под легальные. После установки программа-вымогатель блокирует экран системы или определенные файлы до тех пор, пока злоумышленники не получат выкуп.

Для сохранения анонимности злоумышленники обычно требуют платежи в криптовалютах, например, биткойнах. Стоимость выкупа варьируется в зависимости от программы-вымогателя и курса обмена цифровых валют. Однако злоумышленники не всегда разблокируют зашифрованные файлы после получения выкупа.

Количество атак программ-вымогателей растет, продолжают появляться новые варианты программ-вымогателей. Наиболее обсуждаемые программы-вымогатели включают Maze, Conti, GoldenEye, Bad Rabbit, Jigsaw, Locky и WannaCry.

Ботнеты

Термин ботнет означает сеть компьютеров, специально зараженных вредоносным ПО с целью выполнения автоматических задач в интернете без разрешения и ведома владельцев этих компьютеров.

Когда компьютер управляется ботнетом, он может использоваться для выполнения злонамеренных действий. К ним относятся:

- Создание фальшивого интернет-трафика на сторонних веб-сайтах с целью получения прибыли.
- Использование компьютера для участия в распределенных атаках типа «отказ в обслуживании» (DDoS), вызывающих сбои в работе веб-сайтов.
- Рассылка спама миллионам пользователей интернета.
- Совершение мошеннических действий и кража личных данных.
- Атаки на компьютеры и серверы.

Компьютеры становятся частью ботнета так же, как и заражаются любой другой вредоносной программой: например, при открытии вложений электронной почты, загрузке

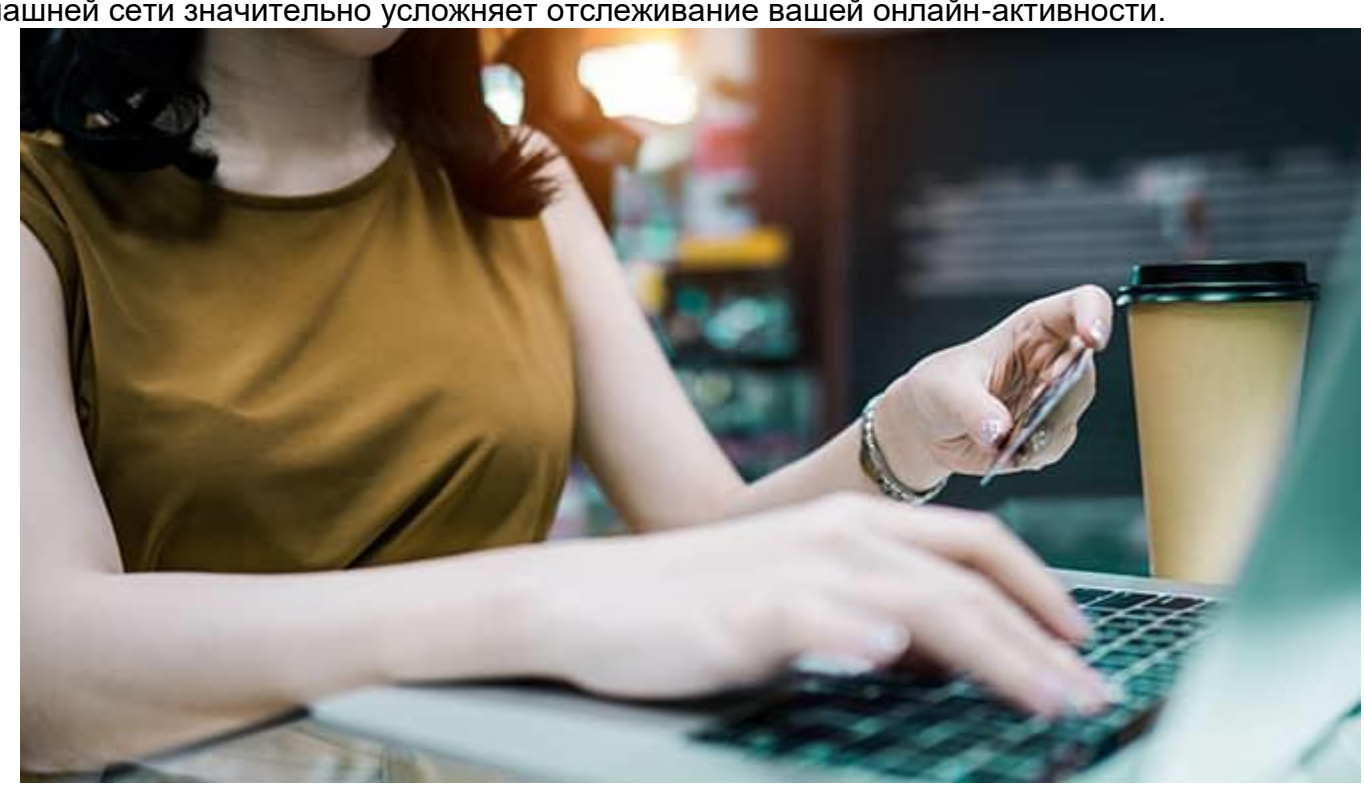
вредоносных программ, посещении веб-сайтов, зараженных вредоносными программами. Ботнеты также могут передаваться с одного компьютера на другой по сети. Количество ботов (зараженных компьютеров) в ботнете зависит от способности заражать незащищенные устройства.

Опасности в публичных и домашних сетях Wi-Fi

Использование публичных сетей Wi-Fi – в кафе, торговых центрах, аэропортах, отелях и ресторанах – сопряжено с определенными рисками, поскольку уровень безопасности в этих сетях часто низкий или защита полностью отсутствует. Это означает, что киберпреступники могут отслеживать действия пользователей в интернете и красть пароли и личную информацию. Другие опасности использования публичных сетей Wi-Fi включают:

- **Прослушивание сети** – злоумышленники отслеживают и перехватывают незашифрованные данные при передаче по незащищенной сети.
- **Атаки типа «человек посередине»** – злоумышленники взламывают точку доступа Wi-Fi и подключаются к процессу передачи данных между пользователем и точкой доступа с целью перехвата и изменения данных в процессе передачи.
- **Мошеннические сети Wi-Fi** – злоумышленники создают приманку в виде бесплатной сети Wi-Fi для сбора личных данных. Точка доступа злоумышленника служит каналом для всех данных, передаваемых по сети.

Слежка за домашней сетью Wi-Fi не должна вызывать столько беспокойства, поскольку сетевое оборудование принадлежит вам. Но опасность, тем не менее, существует: в США провайдерам интернет-услуг разрешено продавать данные о пользователях. Хотя эти данные являются анонимными, сам факт сбора данных может вызывать беспокойство у тех, кто ценит конфиденциальность и безопасность в интернете. Использование VPN в домашней сети значительно усложняет отслеживание вашей онлайн-активности.



Как защитить личные данные в сети

Чтобы обеспечить безопасность в интернете и защитить свои данные, можно следовать перечисленным ниже рекомендациям.

Используйте многофакторную аутентификацию везде, где возможно

Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используется 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 адрес электронной почты.
- Ответы на личные вопросы безопасности.
- Отпечаток пальца или другая биометрическая информация, например голосовые данные или лицо.

Многофакторная аутентификация снижает вероятность кибератаки. Чтобы защитить онлайн-аккаунты, рекомендуется по возможности использовать многофакторную аутентификацию. Для обеспечения безопасности в интернете можно также можете применять сторонние приложения проверки подлинности, такие как Google Authenticator и Authy.

Используйте сетевой экран

Сетевой экран исполняет роль барьера между вашим компьютером и сетью, например интернетом. Сетевые экраны блокируют нежелательный трафик, а также помогают предотвратить заражение компьютера вредоносными программами. Часто сетевой экран входит в состав операционной системы или системы безопасности. Для обеспечения максимальной безопасности в интернете рекомендуется убедиться, что сетевой экран включен и настроено автоматическое обновление.

Внимательно относитесь к выбору браузера

Браузер – это основной инструмент для выхода в интернет, он играет ключевую роль в обеспечении безопасности в интернете. Хороший веб-браузер должен быть безопасным и обеспечивать защиту от утечки данных. Фонд свободы прессы составил подробное руководство, описывающее плюсы и минусы безопасности основных веб-браузеров.

Создавайте надежные пароли и используйте менеджер паролей

Надежный пароль помогает обеспечить безопасность в интернете. Он 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.

Замена букв и цифр похожими символами, например, “P@ssw0rd” вместо “password”, сейчас уже не является эффективной мерой – злоумышленники умеют обходить такую замену. Чем сложнее ваш пароль, тем сложнее его взломать. Использование менеджера паролей позволяет создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.

Пароли необходимо хранить в секрете, никому не сообщать и нигде не записывать. Рекомендуется не использовать один пароль для всех учетных записей, а также регулярно менять пароли.

Используйте на устройствах последнюю версию программы безопасности

Антивирус, обеспечивающий защиту в интернете, очень важен для сохранения конфиденциальности и безопасности. Лучшие программы интернет-безопасности защищают от различных видов атак, а также обеспечивают безопасность данных в интернете. Очень важно обновлять антивирусное программное обеспечение. Большинство современных программ обновляются автоматически, что гарантирует защиту от последних угроз интернет-безопасности.

Как обезопасить свою семью в интернете

Защита детей от опасного и неприемлемого контента и контактов в интернете, а также от вредоносных программ и атак очень важна. Обучение детей основам безопасности в интернете позволит их обезопасить.

Рекомендации по обеспечению безопасности детей в интернете

Дети проводят все больше и больше времени в интернете, и важно объяснить им, как оставаться в безопасности. Важно, чтобы они знали, какую информацию следует хранить в секрете. Например, следует объяснить, почему никому нельзя сообщать пароли и раскрывать личную информацию. Установка компьютера там, где вы можете наблюдать и контролировать его использование, также поможет обеспечить безопасность ребенка в интернете.

Многим детям нравится смотреть видео на YouTube. Чтобы сделать этот процесс более безопасным, можно использовать родительский контроль для YouTube. Также можно использовать специальное приложение для детей – YouTube Kids. Оно имеет удобный для детей интерфейс, а видео в приложении отбираются модераторами-людьми и автоматическими фильтрами, и подходят даже для детей младшего возраста.

[РИС. 3]

https://www.gettyimages.de/detail/foto/hands-of-a-little-boy-on-a-laptop-keyboard-lizenzfreies-bild/1197246563?adppopup=true

alt= “Безопасность и конфиденциальность в интернете”

Как защитить электронную почту

Электронная почта разработана так, чтобы быть максимально открытой и доступной и позволить людям общаться друг с другом. Недостатком такой доступности является уязвимость некоторых аспектов электронной почты. Это позволяет злоумышленникам использовать электронную почту для нарушения безопасности в интернете.

Что такое безопасность электронной почты?

Безопасность электронной почты – это набор методов, используемых для защиты учетных записей электронной почты и переписки от несанкционированного доступа, потери и компрометации. Учитывая, что электронная почта часто используется для распространения вредоносных программ, спама и фишинговых атак, ее безопасность является важным аспектом безопасности в интернете.

Как бороться со спамом по электронной почте?

Спам-сообщения – это массово рассылаемые нежелательные сообщения. Большинство провайдеров электронной почты используют алгоритмы фильтрации спам-сообщений, но, несмотря на это, спам может продолжать приходить. Чтобы избавиться от спама, можно предпринять следующие шаги:

- **Отмечать спам-сообщения как спам**. Это поможет провайдеру электронной почты улучшить фильтрацию спама. Способ отметить сообщение как спам зависит от используемого почтового клиента: Outlook, Gmail, Apple Mail, Yahoo Mail и т. д.
- **Никогда не переходить по ссылкам и не открывать вложения в спам-сообщениях**. В результате таких действий на устройство могут быть загружены вредоносные программы. По крайней мере, такие действия служат подтверждением для спамеров, что это активная учетная запись электронной почты, и стимулируют их рассылать еще больше спама.
- **Соблюдать осторожность при использовании 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.
- **Большинство провайдеров электронной почты имеют настройки конфиденциальности**. Убедитесь, что они установлены на комфортном для вас уровне.
- **Изучить сторонние спам-фильтры для электронной почты.** Они обеспечивают дополнительный уровень кибербезопасности, поскольку электронные письма, прежде чем попасть к адресату, должны пройти через два спам-фильтра: спам-фильтр почтового провайдера и сторонний фильтр.

Слишком много спам-писем может быть признаком того, что ваш адрес электронной почты был раскрыт в результате утечки данных. В этом случае рекомендуется сменить адрес электронной почты.

Сетевая безопасность

Сетевая безопасность – это набор действий, направленных на защиту работоспособности и целостности сети и данных. Она обеспечивает защиту от множества угроз и предотвращает их проникновение и распространение в сети.

Как настроить безопасность Wi-Fi роутера

Wi-Fi роутер является важным компонентом интернет-безопасности. Он проверяет весь входящий и исходящий трафик и контролирует доступ к сети Wi-Fi, а также к телефонам, компьютерам и другим устройствам. Надежность роутеров улучшилась за последнее время, но можно предпринять дополнительные действия для усиления защиты в интернете.

Изменение заданных по умолчанию параметров роутера, таких как имя и учетные данные для входа – это важный первый шаг. Это поможет сделать сеть Wi-Fi менее уязвимой для злоумышленников, поскольку в этом случае роутер находится в активном управлении.

Чтобы повысить безопасность Wi-Fi роутера, можно отключить различные функции и настройки. Такие функции, как удаленный доступ, универсальная настройка сетевых устройств (Universal Plug and Play) и настройка защищенного Wi-Fi, могут использоваться вредоносными программами. Несмотря на то, что эти функции очень удобны, их отключение повысит безопасность домашней сети.

Использование VPN в общедоступной сети Wi-Fi

Лучший способ защитить данные в интернете при использовании общедоступного Wi-Fi – это виртуальная частная сеть (VPN). Технология VPN создает зашифрованный туннель между вашим устройством и удаленным VPN-сервером. Весь интернет-трафик передается через этот туннель, что обеспечивает защиту данных. Когда вы подключаетесь к общедоступной сети с помощью VPN, другие пользователи в этой сети не могут отследить ваши действия, что обеспечивает надежную защиту в интернете.

Сетевая безопасность и Интернет вещей

Интернет вещей относится к физическим устройствам, отличным от компьютеров, телефонов и серверов, которые подключаются к интернету, собирают и обмениваются данными. Примеры таких устройств – фитнес-трекеры, умные холодильники, умные часы и голосовые помощники, такие как Amazon Echo и Google Home. По оценкам, к 2026 году в мире будет установлено 64 миллиарда устройств интернета вещей.

Все эти устройства, подключенные к интернету, создают новые возможности компрометации информации. Через интернет вещей передается огромный объем данных. Кроме того, сами эти данные часто являются крайне важными. Поэтому важно помнить об угрозах интернет-безопасности и соблюдать правила кибербезопасности.

Безопасность мобильных устройств в интернете

Безопасность мобильных устройств – это набор методов защиты данных на мобильных устройствах, таких как смартфоны и планшеты. Это еще один вид интернет-безопасности.

Как узнать, прослушивается ли телефон

Смартфоны могут подвергнуться прослушиванию, особенно в результате взлома или получения root-доступа. Прослушивание позволяет злоумышленникам слушать ваши телефонные разговоры и читать сообщения. О взломе телефона могут свидетельствовать такие признаки, как необычный фоновый шум при звонках, быстрый расход заряда батареи телефона и странное поведение устройства.

Если телефон самопроизвольно включается и выключается и если на нем появляются приложения, которые вы не устанавливали, это может указывать, что кто-то еще имеет доступ к вашему телефону. Также признаками прослушивания телефона могут являться странные SMS-сообщения, содержащие набор искаженных букв и цифр, и счета за телефон на более высокие, чем обычно, суммы.

С дополнительными советами по безопасности мобильных устройств можно ознакомиться в этой статье.

Что такое подмена телефонных номеров и как с ней бороться?

Подмену телефонных номеров обычно используют киберпреступники, пытающиеся убедить пользователя в том, что информация исходит из надежного источника. Они намеренно фальсифицируют отображаемый номер вызывающего абонента, чтобы выдать свой звонок за звонок с локального или знакомого пользователю номера.

Чтобы прекратить подмену телефонных номеров, выясните, есть ли у вашего оператора сотовой связи сервис или приложение для выявления и предотвращения спам-вызовов. Также для фильтрации вызовов можно использовать сторонние приложения, такие как RoboKiller или Nomorobo, однако они требуют предоставления личных данных.

Лучше всего не отвечать на звонки с неизвестных номеров. Не рекомендуется также отвечать на мошеннические звонки, поскольку в этом случае мошенники воспринимают вас как потенциальную жертву.

Как удалить шпионские приложения с телефона

При появлении признаков шпионских приложений на вашем смартфоне проверьте установленные приложения. Удалите все приложения, в надежности которых вы не уверены или не помните, что устанавливали их.

Также может помочь обновление операционной системы телефона и более радикальные меры, например, сброс настроек телефона до заводских. Несмотря на то, что эти действия могут вызвать некоторые неудобства, рекомендуется их выполнить, если вы считаете, что ваш телефон был скомпрометирован.

Для выявления и удаления вирусов и вредоносных программ с телефонов Android можно использовать Kaspersky Internet для Android. В подробной статье об удалении вирусов с Android-устройств, объясняется, как это сделать вручную.

Советы по безопасности: как защититься в интернете

Итак, каковы лучшие методы защиты в интернете? Ниже приведены рекомендации по защите от угроз интернет-безопасности и различных типов интернет-атак.

Программное решение, обеспечивающее круглосуточную интернет-безопасность

Лучшее программное обеспечение для интернет-безопасности защищает от целого ряда угроз, включая взломы, вирусы и вредоносные программы. Комплексный продукт для обеспечения безопасности в интернете должен обнаруживать уязвимости устройств, блокировать киберугрозы до момента их распространения, а также изолировать и устранять непосредственные опасности.

Блокировка доступа к веб-камере для конфиденциальности в интернете

В результате взлома злоумышленники получают доступ к камере вашего мобильного телефона или компьютера и записывают ваши действия. Это называется “camfecting”. Количество зарегистрированных атак этого типа относительно невелико, хотя в большинстве случаев жертвы не осознают, что их камеры были взломаны, и такие случаи остаются неучтенными.

Самый простой способ заблокировать доступ к веб-камере – использовать клейкую ленту. Однако это невозможно, если регулярно приходится использовать видеоконференции для работы и для общения. Гораздо эффективнее использовать антивирус, обеспечивающий защиту веб-камеры, например, Kaspersky Internet Security. Также рекомендуется выключать компьютер или ноутбук, когда он не используется.

Блокировщики, защищающие от вредоносной рекламы

Блокировщики рекламы убирают рекламу с веб-страниц. При блокировке рекламы исчезает риск просмотра и перехода на вредоносную рекламу. У блокировщиков рекламы есть и другие преимущества. Например, они снижают количество файлов cookie, хранящихся на компьютере, повышают конфиденциальность в интернете благодаря сокращению отслеживания, экономят трафик, обеспечивают более быструю загрузку страниц и увеличивают продолжительность работы батареи мобильных устройств.

Некоторые блокировщики рекламы являются бесплатными, а некоторые – платными. Однако не все блокировщики рекламы блокируют онлайн-рекламу полностью, а некоторые сайты могут работать некорректно при включенном блокировщике рекламы. Можно настроить блокировщики рекламы так, чтобы допускался показ онлайн-рекламы с определенных сайтов.

Родительский контроль для безопасности детей

Родительский контроль – это набор настроек, позволяющих контролировать контент, доступный вашему ребенку в интернете. Родительский контроль, используемый совместно с настройками конфиденциальности, повышает безопасность детей в интернете. Настройка родительского контроля зависит от платформы и устройства. На сайте организации Internet Matters приведены пошаговые инструкции по настройке для каждой платформы. Можно также использовать приложение для родительского контроля, например, Kaspersky Safe Kids.

Очистка компьютера

Очистка компьютера – это инструмент для удаления ненужных и временных файлов и программ из системы. В Kaspersky Total Security предусмотрена функция очистки компьютера, позволяющая находить и удалять редко используемые или установленные без вашего согласия приложения и браузерные расширения.

Кроссплатформенная защита

Интернет-защита должна распространяться на все устройства, используемые для выхода в Интернет: ноутбуки, компьютеры, смартфоны и планшеты. Лучшие программы интернет-безопасности можно установить на несколько устройств, что обеспечит кроссплатформенную защиту от угроз интернет-безопасности.

Безопасный онлайн-банкинг и онлайн-шоппинг

Рекомендации по безопасности при онлайн-шоппинге:

- Убедитесь, что вы совершаете транзакции на защищенном веб-сайте. Его веб-адрес должен начинаться с https://, а не с http://; буква s означает «безопасный» и указывает на наличие у сайта сертификата безопасности. Слева от адресной строки также должен отображаться значок замка.
- Обращайте внимание на веб-адрес сайта. Злоумышленники могут создавать поддельные сайты с веб-адресами, аналогичными настоящим. Они часто меняют несколько буквы в веб-адресе, чтобы ввести пользователей в заблуждение.
- Избегайте предоставления финансовой информации при использовании публичных сетей Wi-Fi.

Рекомендации по безопасности при онлайн-банкинге:

- Аналогично онлайн-шоппингу, избегайте предоставления финансовой и личной информации при использовании публичных сетей Wi-Fi.
- Используйте надежные пароли и регулярно меняйте их.
- По возможности используйте многофакторную аутентификацию.
- Чтобы не стать жертвой фишингового мошенничества, вводите веб-адрес банка напрямую или используйте банковское приложение, но не переходите по ссылкам в сообщениях электронной почты.

- Регулярно проверяйте выписки по банковским счетам, чтобы выявить непонятные транзакции.
- Поддерживайте операционную систему, браузер и приложения в актуальном состоянии. Это гарантирует, что в них исправлены известные уязвимости.
- Используйте надежные решения для обеспечения интернет-безопасности, например продукты, предлагаемые «Лабораторией Касперского».

В мире, где большая часть жизни проходит онлайн, безопасность в интернете очень важна. Понимание того, как преодолевать угрозы интернет-безопасности и противостоять различным типам интернет-атак, является ключом к обеспечению безопасности и защите данных в интернете.