Как обезопасить себя в интернете: простые советы по защите личных данных

Наша повседневная жизнь тесно связана с интернетом, взять хотя бы мобильный банкинг, покупки онлайн, социальные сети и чат-боты, которые дарят нам множество полезных функций. Но ими также пользуются злоумышленники: не соблюдая меры предосторожности, в мировой паутине легко потерять деньги или стать жертвой кражи личности.

В этом подробном обзоре вы найдете информацию о том, как обезопасить себя в интернете. Рассмотрим основные угрозы и главные принципы безопасного поведения онлайн. А также дадим советы о том, как защитить свои данные и что делать, если их уже украли.

Самое необходимое для безопасности в интернете

Чтобы безопасно пользоваться интернетом, нужно иметь надежный антивирус, понимание того, как работают сервисы, с которыми вы взаимодействуете, и кое-что еще.

Антивирус

Для защиты от приложений-шпионов, программ-вымогателей, межсайтового скриптинга и других распространенных угроз не обойтись без антивирусного программного обеспечения. Оно будет не только сканировать устройство на предмет вирусов и уничтожать вредоносное ПО, но и мониторить ваш интернет-трафик, а также отражать кибератаки.

Чтобы обеспечить высокий уровень безопасности, выбирайте лучший из доступных антивирусов. Например, передовые антивирусные программы, способные распознавать и блокировать большое количество разных угроз, выпускает «Лаборатория Касперского». При этом на ее ПО можно сэкономить, использовав промокод Kaspersky.

В том числе у компании есть решение, помогающее защитить практически все грани цифровой жизни пользователей, — Kaspersky Premium. В него, помимо защиты от вирусов, взлома и утечек данных, входит целый ряд дополнительных опций. Среди них антиспам, надежный менеджер паролей и проверка домашней сети Wi-Fi, а также приоритетный доступ к техподдержке.

Хорошее оборудование

С развитием диджитал-сферы появляются новые, более усовершенствованные вредоносные программы. Для защиты от них важно использовать актуальное программное

обеспечение, разработанное с учетом новых видов угроз, но его не потянет старая электроника. Современное ПО требует хорошего современного оборудования.

Основные угрозы в интернете

В онлайн-пространстве можно столкнуться с множеством потенциальных угроз. Прежде всего это несанкционированное использование ваших личных данных, фишинг и мошенничество, опасности публичных Wi-Fi-сетей, а также риски чат-ботов.

Угрозы безопасности личных данных

Злоумышленники охотятся за личными данными пользователей: датами рождения, адресами электронной почты, физическими адресами, номерами телефонов, полными именами, номерами документов и банковских карт, а также фотографиями и даже сведениями о состоянии здоровья. При этом украсть информацию они могут не только из открытых источников, но и взломав персональный аккаунт или сайт, на котором вы оставляли свои конфиденциальные данные.

Утечка личных данных грозит как минимум получением назойливых звонков от «сотрудников службы безопасности банка», а как максимум — кражей личности. Преступники могут создать фейковый аккаунт, чтобы обманывать людей от вашего имени, взять на вас кредит и даже переоформить ваше имущество на третье лицо.

Фишинг и мошенничество

Один из самых распространенных способов интернет-обмана — это фишинг, то есть рассылка писем или сообщений от имени банков, организаций и брендов. Такое сообщение обычно содержит ссылку на поддельный сайт компании и побуждает пользователя ввести на нем свой логин и пароль. После того как жертва это делает, мошенник получает доступ к ее аккаунту или банковскому счету.

Овладев вашим банковским аккаунтом, злоумышленники могут перевести себе ваши личные и кредитные средства, а также использовать ваш счет для совершения незаконных операций. А получив контроль над соцсетями пользователя, злоумышленники часто начинают рассылать списку его контактов просьбу занять денег, рекламировать мошеннические схемы или вымогать плату за восстановление доступа.

Опасности публичных Wi-Fi-сетей

Публичные сети Wi-Fi обычно имеют низкую степень защиты. Кроме того, мошенники могут создавать собственные сети, маскируясь под открытый Wi-Fi ресторана, торгового центра или другого общественного пространства. Подключившись к такой

точке и войдя в свое банковское приложение или введя на каком-либо сайте свои персональные данные, вы передадите эту информацию и пароли злоумышленникам.

Риски при использовании чат-ботов

У чат-ботов есть свои уязвимости, которыми пользуются мошенники. Они могут красть данные с серверов, на которых обычно хранят сведения, полученные от пользователей. Также преступники могут взломать чат-бот и изменить его настройки, чтобы от имени магазина или организации выведать конфиденциальную информацию. Кроме того, бывают случаи, когда с помощью чат-ботов выполняют рассылку вредоносных программ или программ-вымогателей.

Основные принципы безопасного поведения в интернете

Существуют простые способы обезопасить себя от многих киберугроз. Как минимум стоит начать с правильного обращения с паролями, использования двухфакторной аутентификации, регулярного обновления ПО и изучения политики конфиденциальности сервисов, которыми вы пользуетесь.

Создавайте сложные и уникальные пароли

Одна из самых главных брешей в безопасности пользователей — это слишком простые пароли, которые злоумышленникам легко подобрать. Чтобы позаботиться о своей безопасности:

- придумывайте сложные пароли длиной от 12 символов, со случайными комбинациями заглавных и строчных букв, цифр и специальных знаков;
- не используйте в пароле личные данные, которые легко найти в общем доступе, например дату рождения, имена родных и питомцев;
- не устанавливайте один и тот же код доступа на разные аккаунты;
- не разрешайте браузеру автосохранение паролей, особенно от сайтов, на которых вы вводите номер своей банковской карты;
- периодически меняйте пароли на самых ключевых профилях, включая электронную почту, мобильный банк и соцсети;
- сразу меняйте пароль на всех новых умных устройствах, будь то смартфон, роутер, телевизор или кофеварка.

Также не стоит хранить коды доступа в файле на компьютере. Лучше запоминать их, выписывать в бумажный блокнот или хранить в специальном менеджере паролей.

Используйте двухфакторную аутентификацию

Везде, где это возможно, пользуйтесь двухфакторной аутентификацией, то есть входом в учетные записи с использованием нескольких проверок подлинности вашей личности. Тогда, помимо логина и пароля, система будет требовать одноразовый проверочный код, отправленный на ваш номер телефона. Либо нужно будет вводить отпечаток пальца, сканировать лицо или предоставлять другую дополнительную информацию. Это снизит риск попасть в руки киберзлодеев.

Кроме того, регулярно просматривайте мейлы и СМС на предмет странных уведомлений, которые могут свидетельствовать о попытках злоумышленников войти в ваш аккаунт.

Регулярно обновляйте программное обеспечение и антивирусы

Важно регулярно обновлять не только антивирусы, но и операционные системы, а также любые программы и приложения, которыми вы пользуетесь. В обновлениях разработчики не только добавляют новые функции и улучшают интерфейс, но и устраняют уязвимости ПО к самым новым угрозам. Особенно внимательно стоит следить за обновлениями приложений, использующих ваши конфиденциальные данные и банковские реквизиты.

Изучайте политику конфиденциальности сервисов

У каждого сервиса, который мы используем онлайн, есть политика конфиденциальности, то есть описание того, как им собираются, обрабатываются и хранятся наши персональные данные. Многие принимают ее условия, не читая этот документ, а зря. Лучше потратить немного времени на изучение настроек конфиденциальности, чтобы убедиться в том, что вы не дали сайту излишней свободы в использовании своих данных. На многих ресурсах этими параметрами можно управлять, закрывая доступ к определенным типам информации о вас.

Также стоит обращать внимание, какие разрешения запрашивают используемые вами приложения.

Как безопасно пользоваться чат-ботами

Чтобы не попасть в руки мошенников при использовании ботов, соблюдайте три простых правила.

Проверьте источник и репутацию чат-бота

Используйте только чат-боты, разработанные известными компаниями. Также не помешает изучить отзывы пользователей о конкретном чат-боте на разных площадках.

Кроме того, как и в случаях с любыми другими онлайн-сервисами, стоит изучить политику и настройки конфиденциальности чат-бота.

Избегайте передачи личных данных в диалогах

Все, что вы пишете в чате, будет сохранено и проанализировано компанией, которой принадлежит чат-бот, для улучшения его обучения. Но, помимо благих целей, это увеличивает риск утечки любой сообщенной вами информации и кражи ее злоумышленниками. Поэтому эксперты советуют не передавать в диалогах с ботами следующие данные:

1. Персональную информацию, включая полное имя, дату рождения, адрес, телефон, а также идентификационные номера.
2. Логины, пароли, ПИН-коды и любые другие данные, открывающие доступ к вашим аккаунтам.
3. Номера банковских карт, размер доходов и другие финансовые сведения.
4. Рабочие конфиденциальные данные и коммерческие секреты.
5. Свои оригинальные творческие идеи.
6. Информацию о состоянии своего здоровья, включая диагнозы и назначенное вам лечение.
7. Личные мысли, мнения и переживания, а также факты о вас, которые вы бы не хотели сделать публичными.

Кроме того, если чат-бот предлагает такой выбор, лучше не давать разрешение на использование ваших данных для обучения языковых моделей. А также можно пользоваться чат-ботом в режиме инкогнито и очищать историю разговора.

Используйте чат-боты только на защищенных устройствах

Пользуйтесь чат-ботами только на смартфонах и ПК с актуальным программным обеспечением и надежным антивирусом. Это снизит риск перехвата конфиденциальной информации злоумышленниками.

Как защитить свои данные от утечек

Для защиты своих данных нужно делать резервные копии, пользоваться VPN, чистить cookies и быть осторожными со ссылками, по которым вы переходите.

Регулярно делайте резервные копии важных данных

Один из видов киберугроз — это программы-вымогатели, блокирующие доступ к информации на вашем компьютере, и другие типы вредоносного ПО, которые могут портить и удалять файлы. Поэтому, чтобы не остаться без важных данных, рекомендуется

регулярно создавать резервные копии. Для их хранения можно обзавестись внешними жесткими дисками.

Используйте зашифрованные соединения (VPN)

Чтобы предупредить кражу персональной информации, никогда не используйте публичные сети Wi-Fi для операций, требующих указывать ваши финансовые и личные данные. В первую очередь не заходите в мобильное приложение банка и не совершайте онлайн-покупки. Если этого никак не избежать и транзакция не может подождать до момента, когда вы попадете домой, делайте это через VPN. Технология виртуальной частной сети поможет защитить вашу личную информацию благодаря шифрованию передаваемых вами данных в реальном времени.

Не доверяйте незнакомым ссылкам и файлам

Под любым программным обеспечением и контентом могут быть замаскированы вредоносные программы. Они способны нарушить работу ПК или смартфона, украсть персональные данные или предоставить злоумышленникам доступ к вашему устройству. Поэтому не открывайте и не скачиваете файл, если сомневаетесь в его происхождении. Также не переходите по сомнительным ссылкам: может быть достаточно одного этого клика, чтобы заразить ваше устройство вирусом.

Вредоносные файлы и ссылки часто рассылаются через email, поэтому, если вы получили письмо, подлинность которого вызывает у вас сомнения, не нажимайте ни на какие его элементы. Внимательно рассмотрите адрес ссылки: злоумышленники часто создают фейковые сайты известных компаний, адрес которых может отличаться от настоящего всего одним символом. Также, если это письмо от важного отправителя, например банка, можно перезвонить туда, чтобы уточнить, действительно ли такой мейл был вам направлен.

Аналогично действуйте в мессенджерах: в сообщениях от незнакомцев не нажимайте на любые ссылки и вложения, включая GIF. Также будьте внимательны во время интернет-серфинга: не кликайте на гиперссылки с «выгодными предложениями» и онлайн-викторины. Прекращайте пользоваться сайтом, если вместо заявленной информации при переходе по ссылке обнаруживается кликбейтная страница со сплетнями о звездах. Кроме того, регулярно проверяйте папку загрузки на смартфоне и ПК и, если там обнаруживаются неизвестные файлы, сразу же их удаляйте.

Чистите cookies и кеш браузера

Cookies — это специальные файлы, которые содержат информацию о ваших действиях на разных онлайн-ресурсах. Благодаря этим фрагментам данных сайты помнят ваши пароли, личные данные, настройки и предпочтения, что очень удобно. Но в то же время cookies можно перехватить и с их помощью получить доступ к вашей учетной записи. Поэтому желательно периодически очищать cookies и кеш браузера, что можно делать через его настройки.

И это далеко не все способы обеспечения цифровой безопасности. Например, рекомендуется быть осторожными с публикациями в социальных сетях: не выкладывать фото билетов и документов, а также держать свой аккаунт закрытым. Кроме того, чтобы обеспечить большую безопасность, можно завести отдельную электронную почту для регистрации на разных сайтах и отдельную банковскую карту для онлайн-покупок. А также лучше удалять старые учетные записи, которыми вы не пользуетесь.

Что делать, если ваши данные уже украли

Если ваши данные все же были украдены, следующие шаги помогут минимизировать ваши потери.

Заблокируйте доступ к аккаунтам

Если вы подозреваете, что данные вашей кредитной карты попали в руки третьих лиц, нужно немедленно ее заблокировать. Это можно сделать через мобильное приложение банка или по телефону его горячей линии. После этого сделайте запрос на перевыпуск карты и сможете пользоваться новыми реквизитами.

Смените все пароли

Если появилось подозрение, что произошла утечка ваших персональных данных и незнакомцам могут стать известны ваши пароли, смените их на всех важных сервисах и сайтах. Например, это обязательно нужно сделать при утере или краже смартфона.

Проверьте свои устройства на наличие вредоносных программ

Если в вашем аккаунте наблюдаются странные действия, возможно, нужно удалить с ПК или смартфона вирусное ПО. Запустите на своих устройствах сканирование антивирусом, а также проверьте папки загрузок на предмет наличия в них странных файлов, которые вы не скачивали. Удалите вредоносные программы и подозрительные элементы.

Свяжитесь с технической поддержкой

Если вы обнаружили свои данные на каком-либо сайте, обратитесь в его службу поддержки. Например, если в соцсети появился фейковый профиль, который использует ваши фотографии, пожалуйтесь на него с его же страницы. Если ваша личная информация всплывает в поисковой системе, также можно сообщить о нарушении в техподдержку поисковика и потребовать удаления контента из общего доступа.

Существует много киберугроз, но, зная, как себя обезопасить от злоумышленников и как действовать в случае утечки данных, вы сможете комфортно пользоваться всеми преимуществами интернета.

Источник информации:

https://hi-tech.mail.ru/news/121434-roskomnadzor-obyasnil-prichiny-sboya-v-internete-24-yanvarya/?from=swap&swap=3