КАК ГАРАНТИРОВАТЬ СВОЮ БЕЗОПАСНОСТЬ В СЕТИ

Сложное слово, простые правила

Кибербезопасность (компьютерная безопасность) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Ваш цифровой след хорошо виден! О каждом пользователе Интернета ежедневно собирается и хранится огромное количество информации. В основном ее собирают социальные сети и мессенджеры. Делается это для того, чтобы как можно точнее идентифицировать каждого пользователя и показывать ему наиболее актуальную рекламу. Чем точнее реклама попадает в интересы и увлечения пользователя, тем больше шансов, что он поддастся на нее, купит товар или приобретет услугу. Однако вся эта информация может попасть в руки к мошенникам. По данным ВЦИОМ, 57% получают звонки от телефонных мошенников, 19% получают от них сообщения, а 9% россиян потеряли деньги в результате действий мошенников.

Ключевой вопрос: Как обеспечить кибербезопасность?

Внимание!

Мошенники могут испо льзовать ваши данные самыми разными способами:

- Продать их другим мошенникам;
- Втереться в доверие и использовать для вымогательства денег;
- Использовать для шантажа;
- Использовать для травли.

Полезные советы

1. **Следите за галочками** (разрешениями), которые ставите (даёте сайтам и приложениям). Иногда кнопка «Ок», появившаяся на экране, означает полный доступ к вашему микрофону, камере или телефонной книге. Таким же образом, вы можете неосторожно оформить подписку на ненужную вам услугу или установить ненужные, а иногда и опасные программы на компьютер. Будьте бдительны!
2. **Старайтесь не пользоваться бесплатными сервисами.** Большинство бесплатных сервисов и приложений, включая мессенджеры и VPN-плагины, могут предоставлять свои услуги на бесплатной основе. Если программа доступна бесплатно, следует задуматься, чем же зарабатывают ее разработчики. Как правило – это персональные данные пользователей программы, которые она ежедневно записывает и передает разработчикам. Те же, в свою очередь, продают их сторонним организациям.
3. **Помните,** что все ваши публикации в Интернете не только публичны, но и хранятся вечно. Помните! Любая приватность может быть нарушена, публикации могут стать доступны в случае утечки.
4. **Не публикуйте и не отправляйте материалы интимного характера.** Любая информация, которую вы выкладываете в Интернет, может стать поводом для шантажа, провокации, а в будущем может даже принести проблемы в карьере. Материалы интимного характера, даже в переписках, не удаляются из Интернета и могут быть использованы преступниками для изготовления порнографических материалов с целью последующей продажи или фальсификации компромата. Никогда не отправляйте фото и видео интимного характера даже самым близким людям, поскольку всегда существует вероятность утечки информации из-за неосторожности, взлома почты или аккаунта.
5. **На незнакомые сайты лучше даже не заходить.** Некоторые сайты способны самостоятельно устанавливать вредоносные программы и вирусы. Для этого даже не нужно ничего скачивать, достаточно просто зайти на сайт. То же относится к письмам и сообщениям, которые приходят из незнакомых источников.
6. **Ненадежные и сомнительные письма лучше не открывать** и уж тем более нельзя скачивать файлы, пришедшие от неизвестного отправителя в письмах или мессенджерах. Это относится даже к текстовым файлам. Например, файлы формата .pdf, в котором распространяется большинство документов, вполне способны распространять вирусы среди скачавших пользователей.

Личный пример

Не публикуйте в соцсетях лишнюю информацию о себе. Абсолютно вся информация, включая ваши фото, адреса, увлечения, имена домашних животных и многое другое, могут быть использованы мошенниками для установления личности, создания подробной картины о вас, как о пользователе, и подбора персональных мошеннических схем.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru