

Безопасный интернет



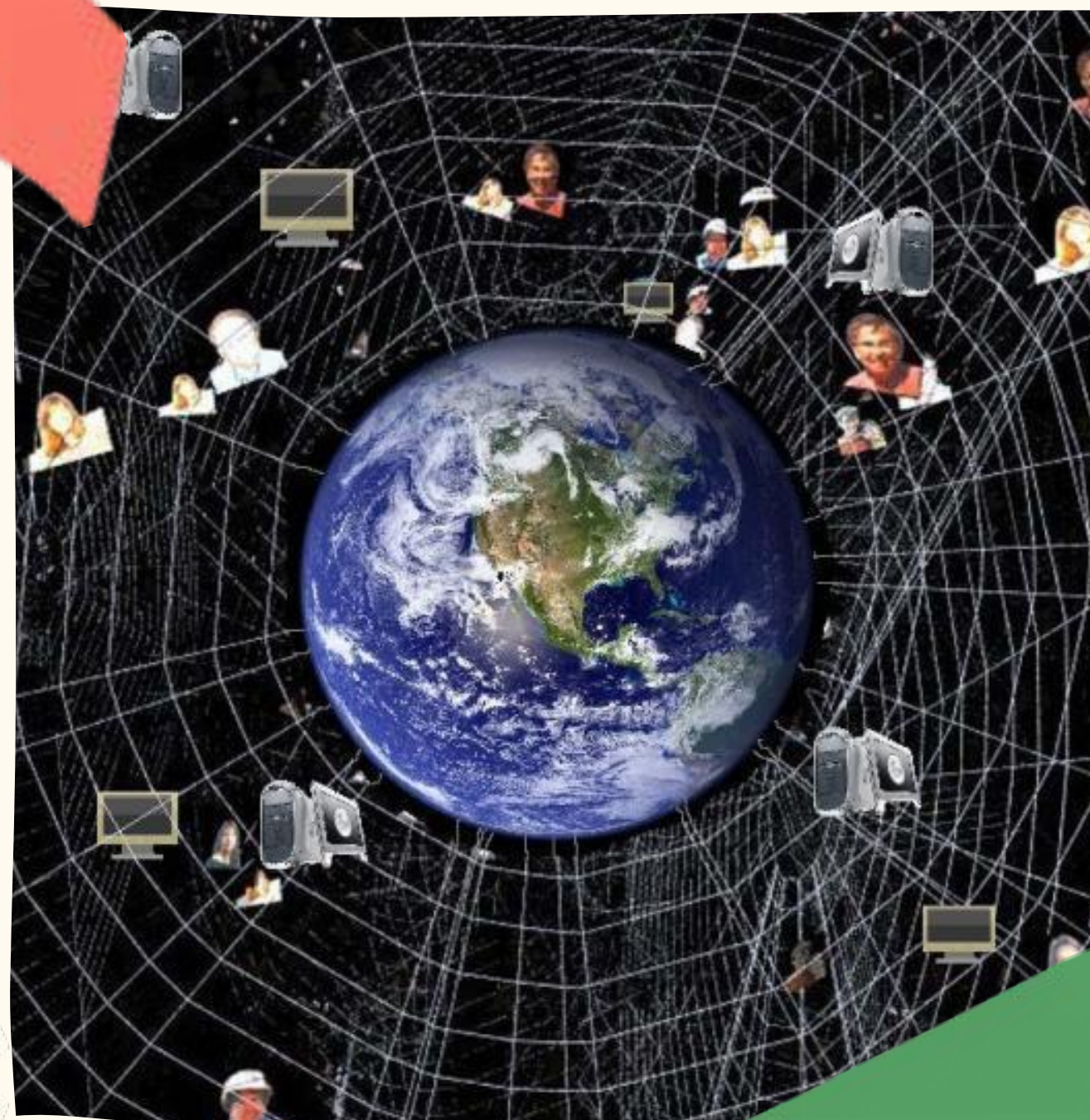
План

- Введение
- Коротко о главном
- Полезные советы
- Выводы



Введение

Привет! Сегодня мы с вами окунемся во Всемирную паутину Интернета! Узнаем множество новых слов, разберем реальные истории. Так же узнаем "Как не попасть в руки к



Основные термины

Монетизация

я

Процесс конвертации чего-либо в деньги.
Монетизация сайта (монетизация трафика) означает процесс заработка денег на сайте.

Аккаунт

Учётная запись, содержащая сведения, которые сообщает о себе пользователь при регистрации в определенном сервисе (сайте). Говоря простым языком, аккаунт — свой личный раздел (кабинет) в сервисе.

Троллинг

Провокация в интернете, в основном в социальных сетях: с помощью резких, задевающих комментариев к чужим постам или собственным публикаций. Задача тролля — разжечь и поддерживать споры и конфликты. Делают это, чтобы развлечься, выставить оппонентов в неприглядном

Основные термины

Фишинг

вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей

Кибербуллинг

намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств

Грумминг

установление дружеских отношений с ребенком с целью получения личной выгоды. Чаще всего это получение личных персональных данных или денежных средств.

Совет 1

Не пересылайте информацию
Не пересылайте
конфиденциальную
информацию (номер
банковской карты, ПИН-код,
паспортные данные) через
мессенджеры социальных
сетей. Письма со сканами
документов лучше удалять



Совет 2

Платный контент
Для некоторых приложений и сервисов предусмотрен бесплатный тестовый период (например, на 2-3 месяца), после чего вы должны самостоятельно отключить услугу. Если вы этого не сделаете, подписка может быть автоматически продлена и станет платной, а с указанной при регистрации карты начнут списывать деньги.



Совет 3

Скачивание фильма

Мошенники создают сайты, на которых вы якобы можете бесплатно посмотреть или скачать понравившийся фильм, но сначала надо оставить телефон или отправить сообщение на короткий номер. Так с вашего счета могут списать внушительную сумму за СМС, а сам телефон попадет в базу спамеров.

спамеров

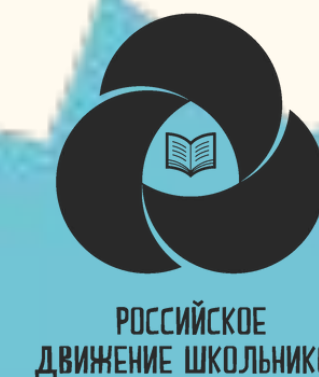
Совет 4



Установите пароль на экране блокировки

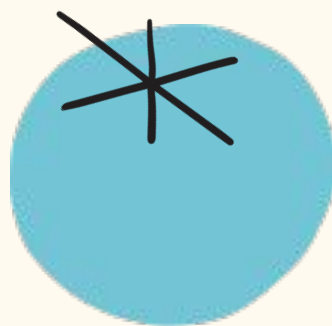
Если телефон украли, телефон украли или вы случайно его потеряли и не установили защиту на экране блокировки, то человек, который его найдёт, может получить доступ ко всем учетным записям социальных сетей, и веб браузеру со всеми сохранёнными паролями. Соответственно, он сможет управлять данными в аккаунтах, удалить их или использовать вам во вред. Если хотите избежать этого, то добавьте визуальный шаблон, «PIN-код» или отпечаток пальца на экран блокировки устройства. Теперь, такому счастливицу достанется только телефон, а ваши личные

Совет 5



Доверяйте антиспам-фильтрам электронной

Как правило, они ~~фильтруют~~ ^{почты} практически все письма, обманом завлекающие вас на тот или иной хакерский сайт. И даже если вам все-таки пришло письмо с сообщением о выигрыше миллиона фунтов стерлингов, не кидайтесь радостно на стену с криками «Я богат!»: такие сообщения получают сотни тысяч пользователей по всему миру ежедневно. Великобритания давно бы разорилась, выплачивая каждому победителю



Совет 6

Торрент

Лучше не пользоваться торрентами: если вы скачиваете нелегальный контент, вы не только обкрадываете любимого автора, но и можете загрузить зараженный вирусом файл.

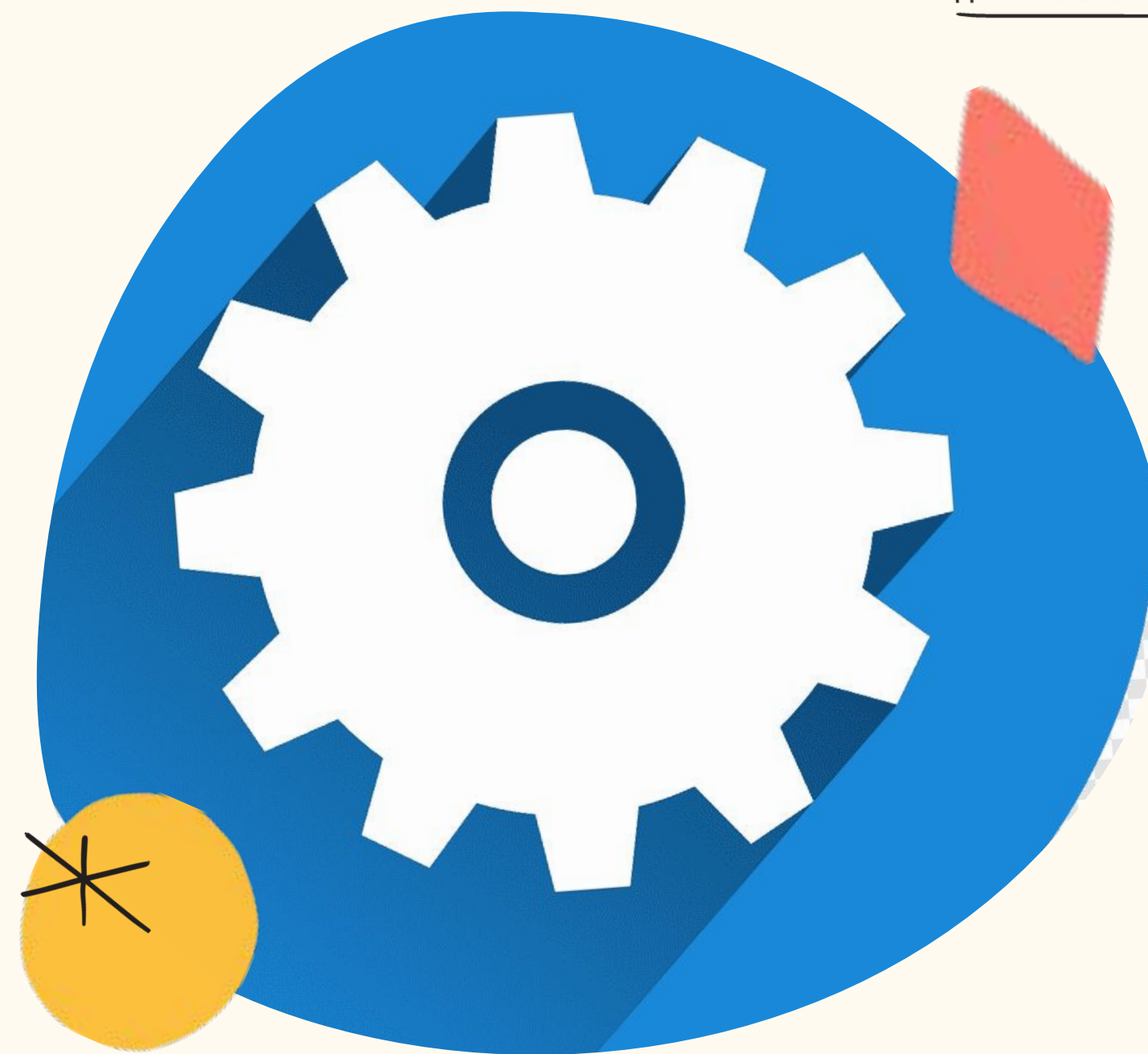


Совет 7



Настройки и Параметры

Откройте пункт «Настройки» или «Параметры» в таких службах, как Facebook и Twitter, чтобы настроить список пользователей, которые могут просматривать ваш профиль или фотографии, помеченные вашим именем, контролировать способы поиска информации и добавления комментариев о вас, а также узнать, как можно



ПОДВЕДЕМ ИТОГИ

