Кибер безопасность

простые правила, которые должен знать каждый

«Неприкосновенность нашей частной жизни подвергается атакам одновременно с нескольких сторон»

Тим Кук

Опасные игры в киберпространстве

киберугрозы, о которых нужно знать

Кибербезопасность

– комплекс мер по защите информации,компьютеров, серверов, мобильных устройств и сетей от несанкционированного доступа, кражи данных, вредоносных программ и других киберугроз.

Три основных вида опасностей:

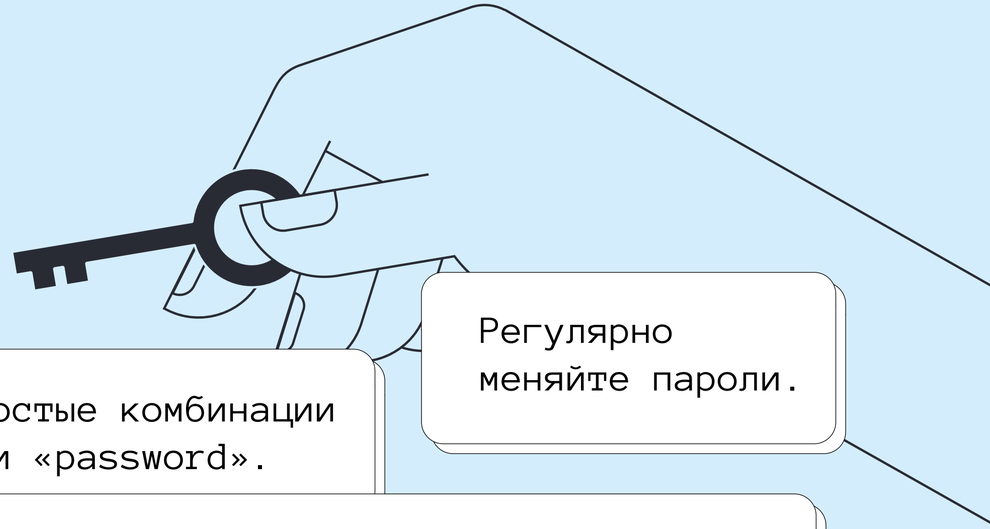
Киберпреступление – это действия, связанные с атакой и нарушением функционирования информационных систем, совершаемые одним или группой злоумышленников ради материальной наживы.

Кибератака – это действия, направленные на получение конфиденциальной информации.

Кибертерроризм – это действия, имеющие своей целью дестабилизацию электронных систем с намерением посеять страх или панику среди населения.

Безопасность превыше всего

создай пароль, который не взломают



Пароль должен быть длинным (не менее 8 символов) и содержать буквы разного регистра, цифры и специальные символы.

Не используйте простые комбинации вроде «123456» или «password».

Регулярно меняйте пароли.

Никогда не используйте один и тот же пароль для разных аккаунтов.

******

Дополнительный шаг к безопасности

двухфакторная аутентификация (2FA)

Включите двухфакторную аутентификацию везде, где это возможно.

Это дополнительный уровень защиты, при котором после ввода пароля вам нужно подтвердить свою личность через код, отправленный на телефон или электронную почту.

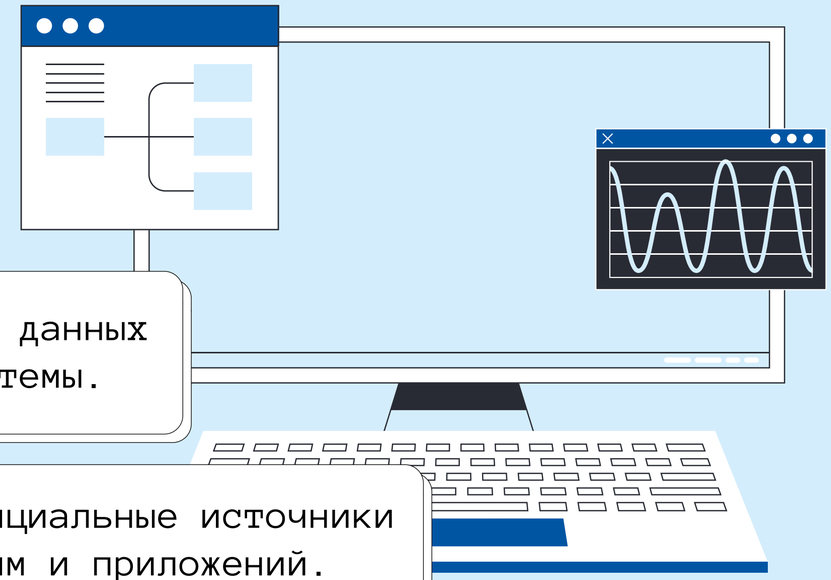
Не дайте вирусам шанса

антивирусное ПО

Установите антивирусные программы на все устройства, которые вы используете для выхода в интернет.

Регулярно обновляйте их базы данных и проводите сканирование системы.

Используйте только официальные источники для скачивания программ и приложений.



Обновления программного обеспечения

Повышение эффективности и новые функции

Убедитесь, что операционная система вашего компьютера, а также все установленные приложения, всегда обновлены до последних версий.

Обновления часто содержат исправления уязвимостей, которые могут использовать злоумышленники.

Не дайте кибер-преступникам шанса

будьте осторожны с ссылками и вложениями

Никогда не переходите по подозрительным ссылкам, даже если они пришли от знакомых людей. Мошенники могут подделывать адреса отправителей.

Всегда проверяйте URL-адрес ссылки перед тем, как кликнуть на неё.

Не открывайте вложения в письмах от неизвестных отправителей.

Резервное копирование

сохраняем важную информацию

Регулярно создавайте резервные копии важных файлов, чтобы избежать потери данных в случае атаки вирусов-шифровальщиков (ransomware).

Социальные сети

сохрани свои данные в безопасности

Настройте приватность своих профилей в социальных сетях, чтобы ограничить доступ посторонних лиц к вашей информации.

Не принимайте запросы дружбы от незнакомых людей.

Будьте внимательны при публикации фотографий и видео – они могут быть использованы против вас.

VPN

обеспечить безопасность в интернете

Если вы подключаетесь к общественным Wi-Fi сетям, используйте виртуальные частные сети (VPN), чтобы зашифровать свой трафик и предотвратить перехват данных.

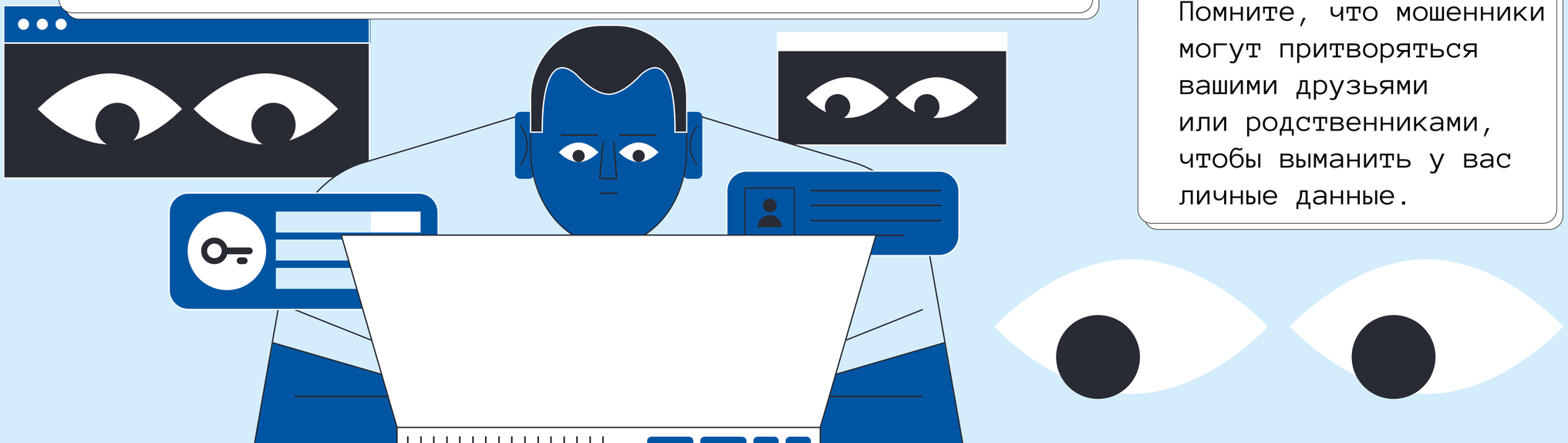
Сохраняем приватность

ограничьте доступ к личной информации

Не публикуйте слишком много личных данных в социальных сетях и на форумах.Информация вроде вашего полного имени, адреса проживания, номера телефона или даты рождения может стать инструментом в руках злоумышленников.
Мошенники могут использовать эту информацию для создания фальшивых профилей или атак типа «социальной инженерии».

Если кто-то просит вас предоставить личную информацию через электронную почту или сообщения, всегда проверяйте источник запроса.

Помните, что мошенники могут притворяться вашими друзьями или родственниками, чтобы выманить у вас личные данные.



Фишинг

обезопась себя и свои финансы

Злоумышленники создают поддельные сайты или письма, которые выглядят как настоящие, чтобы заставить вас ввести личные данные, такие как логины, пароли или номера банковских карт.

Будьте внимательны и проверяйте URL-адреса сайтов перед вводом конфиденциальной информации.

Вам могут предложить получить бесплатный подарок или участвовать в розыгрыше, но для этого потребуется ввести личную информацию или оплатить небольшую сумму. Это уловка для получения ваших данных.

Осторожно, мошенники

не стать жертвой шантажа и вымогательства

Мошенники могут угрожать раскрыть ваши личные фотографии или переписки, если вы не заплатите им деньги.

Никогда не платите вымогателям.

Немедленно сообщите об этом родителям, учителям или специалистам.

Осторожно, фальшивки

поддельные магазины и аукционы

При покупках в интернете обращайте внимание на отзывы покупателей и репутацию продавца.

Некоторые сайты могут быть созданы специально для того, чтобы украсть вашу платёжную информацию.

Осторожно, скрипт-майнер

Следите за нагрузкой на процессор и используйте блокировщики рекламы и скриптов.

Эти скрипты встраиваются в веб-страницы и используют ресурсы вашего компьютера для добычи криптовалюты без вашего ведома.

Социальная инженерия

не стать пешкой в чужой игре

Этот вид мошенничества основан на психологическом манипулировании. Например, вам может позвонить человек, представившийся сотрудником банка, и попросить предоставить номер карты или PIN-код. Помните, что настоящие сотрудники банков никогда не запрашивают такую информацию по телефону.