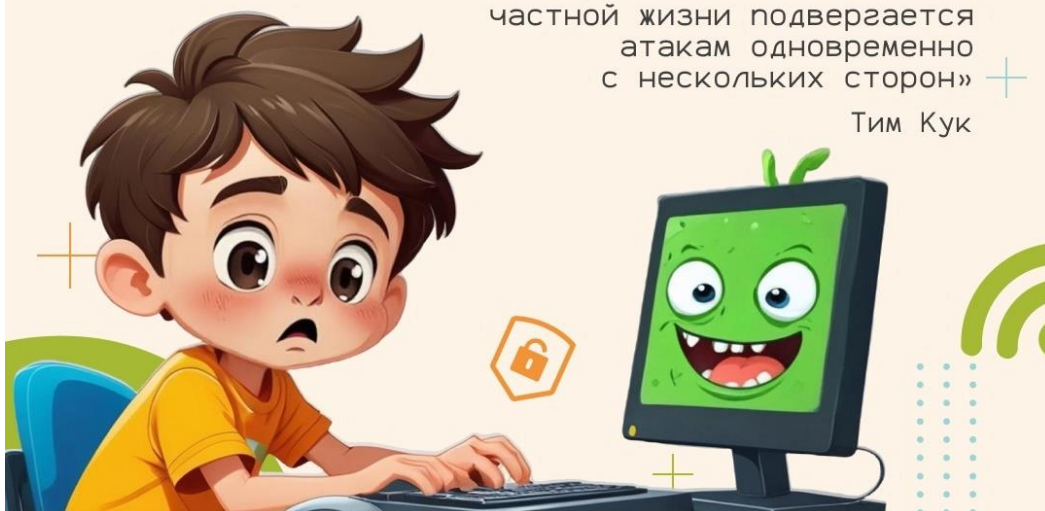


КИБЕР БЕЗОПАСНОСТЬ

ПРОСТЫЕ ПРАВИЛА,
КОТОРЫЕ ДОЛЖЕН ЗНАТЬ
КАЖДЫЙ ШКОЛЬНИК

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

Тим Кук



ОПАСНЫЕ ИГРЫ КИБЕРПРОСТРАНСТВА

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

- 1 Киберпреступление – это действия, связанные с атакой и нарушением функционирования информационных систем, совершаемые одним или группой злоумышленников ради материальной наживы.
- 2 Кибератака – это действия, направленные на получение конфиденциальной информации.
- 3 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»
- Никогда не используйте **один и тот же** пароль для разных аккаунтов
- Регулярно **меняйте** пароли



ДОПОЛНИТЕЛЬНЫЙ ШАГ К БЕЗОПАСНОСТИ

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ (2FA)

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

**ВКЛЮЧИТЕ ДВУХФАКТОРНУЮ
АУТЕНТИФИКАЦИЮ ВЕЗДЕ,
ГДЕ ЭТО ВОЗМОЖНО**



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 ШАНСА КИБЕРПРЕСТУПНИКАМ



БУДЬТЕ ОСТОРОЖНЫ С ССЫЛКАМИ И ВЛОЖЕНИЯМИ

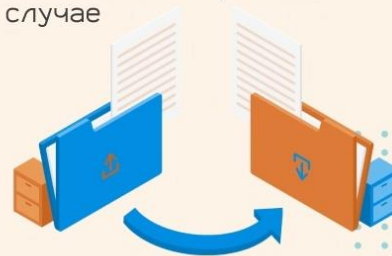
- Никогда не переходите по подозрительным ссылкам, даже если они пришли от знакомых людей (мошенники могут подделывать адреса отправителей)
- Всегда проверяйте URL-адрес ссылки перед тем, как кликнуть на неё
- Не открывайте вложения в письмах от неизвестных отправителей

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 потребуются 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 обращайтесь внимание на отзывы покупателей и репутацию продавца.

НЕКОТОРЫЕ САЙТЫ МОГУТ БЫТЬ СОЗДАНЫ СПЕЦИАЛЬНО ДЛЯ ТОГО, ЧТОБЫ УКРАСТЬ ВАШУ ПЛАТЕЖНУЮ ИНФОРМАЦИЮ



ОСТОРОЖНО

СКРИПТ-МАЙНЕР

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

СЛЕДИТЕ ЗА НАГРУЗКОЙ НА ПРОЦЕССОР И ИСПОЛЬЗУЙТЕ БЛОКИРОВЩИКИ РЕКЛАМЫ И СКРИПТОВ

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