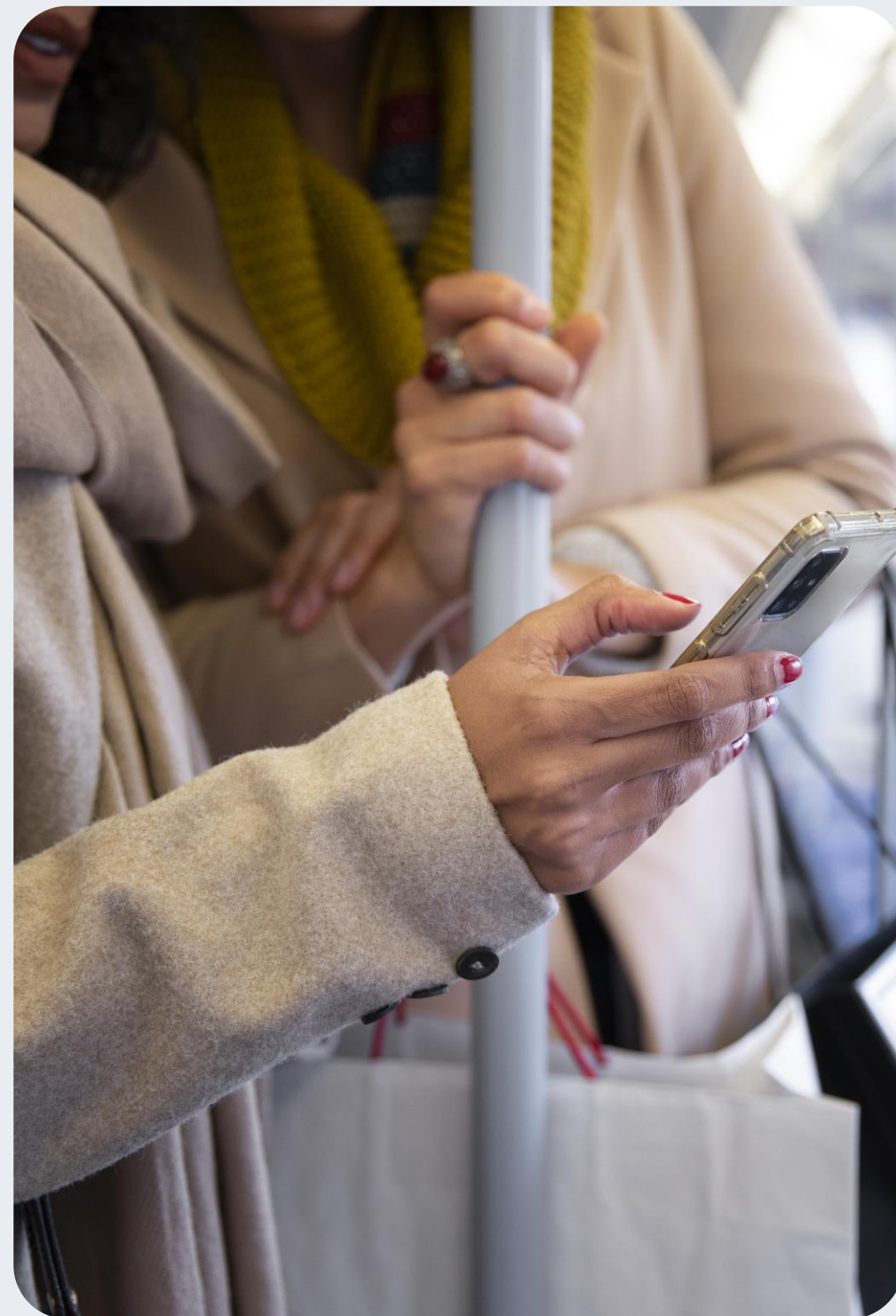




ДИТ

Практическое руководство по защите ваших данных при использовании общедоступных беспроводных сетей в кафе, аэропортах, метро, отелях и т.д.

Безопасность в публичных Wi-Fi сетях



Публичный Wi-Fi — это зона риска



Публичные Wi-Fi сети в кафе, метро, аэропортах, торговых центрах и отелях предоставляют удобный доступ к интернету, но создают серьезные угрозы безопасности ваших данных.

В отличие от домашней сети, где вы контролируете настройки безопасности, публичные точки доступа открыты для всех, что делает их привлекательной целью для киберпреступников.

Злоумышленники активно используют публичные сети для кражи личных данных, финансовой информации и паролей пользователей.

Важно знать

Любая информация, передаваемая по незащищенной публичной сети, может быть перехвачена третьими лицами

Основные угрозы безопасности



Прослушивание трафика

Злоумышленники используют специальное ПО для перехвата незашифрованных данных, включая посещаемые сайты и вводимую информацию



Поддельная точка доступа

Создание фальшивой сети с названием, похожим на легитимную
(например, «MT-FREE» вместо «MT_Free»)



Атака «Человек посередине»

Злоумышленник тайно внедряется в канал связи между вашим устройством и точкой доступа, получая возможность не только перехватывать, но и подменять передаваемые данные.

Возможные последствия



Кража сессионных куки-файлов

Злоумышленник может получить доступ к вашим аккаунтам без логина и пароля



Кража личных данных

На сайтах без HTTPS-шифрования данные могут быть легко перехвачены



Распространение вредоносного ПО

Публичные сети могут использоваться для рассылки вредоносных программ на подключенные устройства



Нарушение конфиденциальности

История поисковых запросов, местоположение, онлайн поведение могут отслеживаться



Признаки опасной Wi-Fi сети



Будьте внимательны, если заметили:

→ **Отсутствие пароля для подключения**

Открытые сети без защиты — самая легкая цель для перехвата данных

→ **Подозрительное название сети**

Несоответствие официальному названию заведения или дублирование с небольшими ошибками

→ **Всплывающие окна с требованием установки ПО**

Легитимные сети не требуют установки дополнительного программного обеспечения

→ **Предупреждение о небезопасном соединении**

Браузер помечает соединение как «Небезопасное» или «Не защищено»



Рекомендации по безопасному использованию публичных Wi-Fi сетей



Соблюдение этих рекомендаций поможет значительно снизить риски и защитить ваши данные при подключении к общедоступным беспроводным сетям

1. Выбирайте сети с идентификацией

Старайтесь подключаться к публичным сетям, которые требуют идентификации через номер телефона (получение кода по SMS) или через аккаунт в портале Госуслуг. Такие сети обеспечивают более высокий уровень контроля

2. Уточняйте легитимность сети

Уточняйте точное название сети Wi-Fi и пароль у сотрудника заведения или на официальном сайте. Не подключайтесь к сетям с подозрительными названиями.

3. Используйте мобильный интернет для важных операций

Для онлайн-банкинга, покупок с картой, доступа к рабочим сервисам и ввода паролей используйте мобильную сеть оператора

4. Включите двухфакторную аутентификацию

Настройте двухфакторную аутентификацию для всех важных сервисов. Даже при перехвате пароля злоумышленник не получит доступ без одноразового кода



Рекомендации по безопасному использованию публичных Wi-Fi сетей



Соблюдение этих рекомендаций поможет значительно снизить риски и защитить ваши данные при подключении к общедоступным беспроводным сетям

5. Убедитесь, что соединение с сайтом зашифровано

Перед вводом любых данных убедитесь, что адрес сайта в браузере начинается с `https://` (а не `http://`). Это означает, что соединение между вашим браузером и сайтом защищено.

6. Отключите общий доступ

Установите профиль «Общедоступная сеть» и отключите общий доступ к файлам в настройках.

7. Используйте уникальные пароли

Уточняйте точное название сети Wi-Fi и пароль у сотрудника заведения или на официальном сайте. Не подключайтесь к сетям с подозрительными названиями.

8. Раздавайте интернет с телефона

Режим модема безопаснее подключения к неизвестной публичной сети — ваше соединение с оператором защищено лучше

9. Отключите автоподключение

Оключите функцию автоматического поиска и подключения к открытым сетям в настройках Wi-Fi

10. Выходите и «забывайте» сеть

После работы выйдите из всех аккаунтов и выберите «Забывать эту сеть» в настройках устройства

Действия, которые не следует выполнять в общедоступном Wi-Fi



Банковские операции

Входить в онлайн-банкинг и проводить платежи.



Покупки

Совершать покупки с вводом данных банковской карты.



Рабочие сервисы

Получать доступ к рабочим сервисам и корпоративной почте.



Пароли

Вводить пароли от важных аккаунтов (соцсети, почта).