

Пользуйтесь Wi-Fi в общественных местах только в редких случаях



У общественных сетей очень низкая степень защиты от хакеров — они могут украсть ваши данные. Кроме того, киберпреступники часто создают сети, замаскированные под открытый Wi-Fi.

Поэтому лучше не подключаться к бесплатным сетям в кафе, гостиницах или на улице. Даже если они имеют пароль. Особенно лучше воздержаться, если собираетесь пользоваться банковскими приложениями, электронной почтой или заходить в соцсети.



Не переходите по ссылкам в сообщениях и письмах от сомнительных отправителей

Заманчивые «спецпредложения» могут привести вас на сайт-зеркало, где попросят указать данные банковской карты. При этом фальшивый ресурс может отличаться от настоящего всего одним символом.



Уделяйте внимание безопасности в соцсетях



Включите двухфакторную аутентификацию. Это усложнит вход, но значительно снизит риски: система будет запрашивать логин и пароль, а после отправлять на телефон или электронную почту проверочный код.

Сделайте аккаунты в соцсетях скрытыми и делитесь личной информацией только с близкими и друзьями.

Не выкладывайте в соцсетях фотографии документов. Даже авиабилетов.

По указанному на них коду можно узнать информацию о вашем рейсе, получить доступ к паспорту, электронной почте и номеру телефона, изменить настройки бронирования.



Как сохранить личную информацию в интернете?

*Пять простых правил
безопасности*



объясняемрф

Установите антивирус



И не принимайте cookie-файлы автоматически. Выбирайте данные, которые нужный вам сайт может сохранить. Ссылка на меню настроек есть в автоматическом уведомлении об использовании cookie.



Используйте сложные пароли

Составляйте пароли из букв и цифр в неочевидной последовательности, произвольно чередуйте верхний и нижний регистры. **Усложняйте комбинации символов.**

Старайтесь **не использовать один пароль для разных сервисов.**

