

Безопасность мобильных устройств



В современном мире, где ноутбуки стали незаменимыми инструментами для работы и общения, вопрос безопасности мобильных устройств приобретает особую актуальность. Корпоративные пользователи, хранящие на ноутбуках ценные данные и конфиденциальную информацию, должны уделять особое внимание защите своих устройств от несанкционированного доступа и физических угроз.

Как обеспечить безопасность своего мобильного устройства?

НОУТБУКИ

Физическая защита:



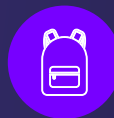
Во время поездок провозите ноутбуки только в ручной клади



Используйте для транспортировки ноутбуков сумки, не явно демонстрирующие их предназначение



Не оставляйте ноутбук без присмотра в публичных местах: в кафе, ресторанах, переговорных и т. п.



Всегда берите ноутбук с собой, не оставляйте его в автомобиле (даже в запертом)



В командировках храните ноутбук в сейфе или в запираемом ящике/шкафу/чемодане

Техническая защита:



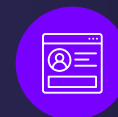
Убедитесь, что на ноутбуке установлено актуальное антивирусное ПО



Используйте надежные, легко запоминающиеся пароли. При создании паролей применяйте мнемонические правила



Не забывайте блокировать экран ноутбука нажатием клавиш Win + L, даже если отлучаетесь на минуту



Никому и никогда не передавайте вашу учетную запись



Отключайте Wi-Fi и Bluetooth, если они не используются



Никогда не отключайте антивирусное ПО, следите за его регулярным обновлением



Для хранения данных учетных записей используйте специализированное ПО, не размещайте эту информацию на рабочем столе в открытом доступе



Подключайтесь только к доверенным/защищенным сетям связи

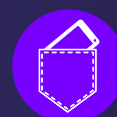
СМАРТФОНЫ/ПЛАНШЕТЫ



Во избежание физических повреждений устройств используйте защитные чехлы и стекла



Не оставляйте смартфоны/планшеты без присмотра в общественных местах: в кафе, ресторанах, переговорных и т. п.



Храните смартфоны/планшеты в сумках, избегайте хранения в задних карманах одежды, в легкодоступных карманах рюкзаков и сумок

Техническая защита:



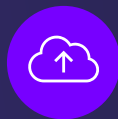
Активируйте возможность дистанционной блокировки смартфона. С ее помощью вы сможете заблокировать злоумышленникам доступ к данным на устройстве и даже стереть их



Всегда используйте сложный PIN-код или вход по биометрическим данным. Даже если ваш телефон украдут, вору придется приложить усилия, чтобы взломать смартфон и получить доступ к его содержимому



Регулярно делайте резервное копирование данных или настройте его автоматическое выполнение раз в неделю. Так вы в любом случае сохраните ценные данные, даже если лишитесь устройства



По той же причине храните фотографии, видео и документы в облачном хранилище, а не на устройстве. В этом случае вы без ущерба для важных файлов сможете удаленно стереть все с устройства, при этом сами данные сохранятся



Используйте антивирусное ПО, регулярно его обновляйте



Используйте для зарядки смартфонов/планшетов специальные зарядные устройства, не подключайте личные смартфоны/планшеты к служебным компьютерам/ноутбукам для подзарядки или передачи данных



Подключайтесь только к доверенным/защищенным сетям связи



Отключайте Wi-Fi и Bluetooth, если они не используются



Будьте осторожны с персональной информацией, которой вы делитесь в интернете. Избегайте отправки конфиденциальных данных через ненадежные каналы связи



Найдите в настройках IMEI и серийный номер своего устройства и запишите их — номера могут пригодиться в случае кражи устройства. 15 цифр IMEI можно обнаружить на упаковке и в гарантийном талоне или при наборе команды *#06#. Серийный номер можно посмотреть на упаковке или в сведениях об устройстве в настройках



В случае кражи/потери смартфона:

- Заблокируйте сим-карту
- Заблокируйте банковские карты
- Заблокируйте телефон удаленно
- Измените основные пароли и включите 2FA (двухфакторную аутентификацию)
- Предупредите своих друзей и семью (о фишинговых атаках)
- Обратитесь в полицию, напишите заявление в отделении по месту происшествия, указав IMEI и серийный номер устройства