РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ МОБИЛЬНЫХ УСТРОЙСТВ

1. Блокировка мобильного устройства

a. Установите в мобильном устройстве пароли. Графический код и цифровой код не всегда могут полноценно защитить Вас.

b. Если устройство имеет возможность биометрической блокировки, для защиты используйте двойную блокировку, например, пароль и биометрическая блокировка.

c. Отключите геолокацию и передачу данных, включайте по необходимости.

d. Если Вас попросили сдать Ваше мобильное устройство при входе в административные здания, прежде чем сдать, снимите флешку с устройства, если есть возможность снять батарейку телефона, то тоже постарайтесь снять.

e. При необходимости устанавливайте приложения, которые позволяют фотографировать злоумышленника при попытках разблокировки устройства.

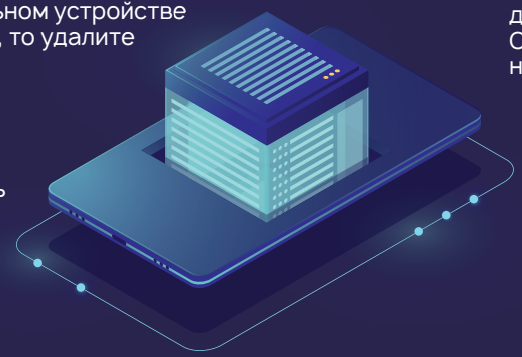
2. Защита информации в мобильном устройстве

a. Используйте защищенную папку для хранения Ваших данных или устанавливайте приложения, которые позволяют устанавливать пароли для папок.

b. Не храните в цифровом формате информацию, если не желаете, чтобы когда-нибудь в будущем она попала в интернет или в чужие руки.

c. Не храните служебную информацию на мобильном устройстве без острой необходимости. Если это необходимо, то удалите после решения задач.

d. Синхронизируйте информацию устройства с компьютером или создавайте дополнительные копии всей информации на других носителях вне Вашего устройства (например, внешний носитель или облачные сервисы ICloud, Samsung Cloud, OneDrive, и др.)



3. Защита приложений в мобильном устройстве

a. Устанавливайте на мобильное устройство только самые необходимые приложения. Если у Вас есть компьютер, нет необходимости постоянно быть он-лайн, если Вы имеете возможность использовать некоторые приложения (например, Skype, FB Messenger, MAgent и др.) на компьютере, постарайтесь не устанавливать эти приложения на мобильное устройство.

b. Устанавливайте пароли для входа в каждый мессенджер отдельно с целью защиты Ваших данных и переписок.

c. Не устанавливайте сомнительные приложения от неизвестных или ненадежных источников. Не устанавливайте приложения, запросившие доступ к Вашим персональным данным и файлам для дальнейшей работы.

4. Защита учетных записей и общения в мобильных устройствах.

a. При установке мессенджеров измените настройки и скрывайте отображение входящих сообщений на экране блокировки (смс, viber, whatsapp).

b. Не используйте одинаковые пароли для всех учетных записей и входа в приложения.

c. При острой профессиональной необходимости устанавливайте приложения, которые позволяют включить диктофон во время телефонных разговоров. Удаляйте записи разговоров если нет необходимости прослушивать заново.

d. Не перезванивайте, увидев пропущенный звонок с неизвестного международного номера.

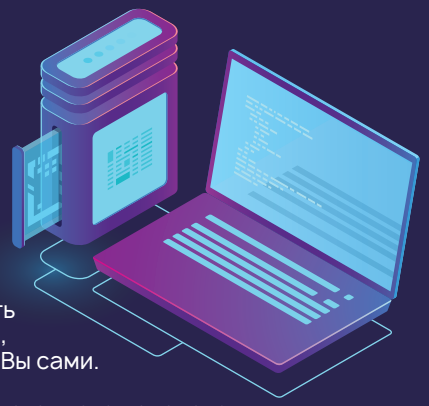
e. Для защиты электронной почты и других учетных записей используйте двухфакторную аутентификацию. Отключите сервисы, которыми не пользуетесь.

ИНСТИТУТ «ОТКРЫТОЕ ОБЩЕСТВО»
ФОНД СОДЕЙСТВИЯ - ТАДЖИКИСТАН

BHR Идораи ҳуқуқи Инсон ва Риояи Қонуният

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ КОМПЬЮТЕРА, ИНФОРМАЦИИ И УЧЕТНЫХ ЗАПИСЕЙ

1. Защита от физического доступа к компьютеру



a. В Bios
i.Отключение других способов использования компьютера, оставить только загрузку с жесткого диска
ii. Установить пароль на вход в Bios

b. Установить BitLocker[1] для защиты дисков

c. Установить пароль на вход в Windows, разделить учетную запись Администратора и пользователей, даже если этим компьютером пользуетесь только Вы сами.

d. Если компьютером постоянно пользуется больше одного человека, необходимо создать для каждого пользователя отдельные учетные записи. Если, кроме постоянных пользователей компьютером, им пользуются гости, необходимо включить учетную запись “Гость”.

e. Если Вы отходите от компьютера или предоставляете другим возможность использовать его на короткий срок, используйте функцию блокировки учетной записи с помощью клавиш Win+L. Это позволит не закрывать Ваши открытые программы и файлы и предоставляет другим использовать компьютер в другой учетной записи.

2. Защита информации в компьютере

a. Сохраняйте информацию только в рамках учетной записи. Информация, сохраненная на других дисках, может быть доступна другим учетным записям.

b. Создавайте не менее 2-х дополнительных копий информации на других носителях вне компьютера (например, внешний диск и облачный сервис).

c. Не храните в цифровом формате информацию, если не желаете, чтобы когда-нибудь в будущем она попала в интернет или в чужие руки.

d. Отслеживайте версии и копии/дубликаты информации. Упорядочьте важную информацию для удобства и защиты.

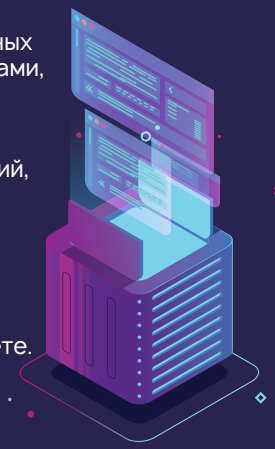
3.Защита Операционной системы и прикладных программ

a. Не пользуйтесь пиратскими версиями «ключей» для программных продуктов. Многие пиратские ключи в Интернете заражены вирусами, если у Вас на компьютере нет уверенной антивирусной защиты, постарайтесь их избегать.

b. Всегда устанавливайте обновления, в каждой версии обновлений, кроме новых возможностей, имеются коды для устранения уязвимостей в программных продуктах.

c. Всегда используйте антивирусные программы для защиты вашего компьютера и целостности вашей информации.

d. Не скачивайте программы с неизвестных источников в Интернете.

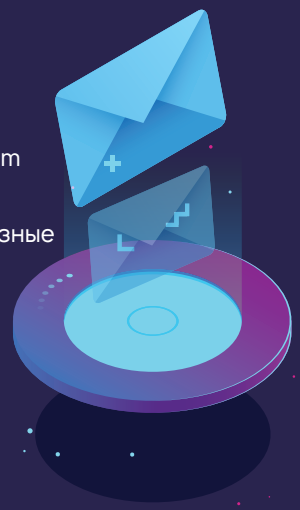


4. Защита вашего компьютера в сети

a. Использование Интернета на работе
i. Убедитесь в том, что на Ваших папках и дисках отключены общие доступы, открывайте доступы по мере необходимости и закрывайте доступы после решения задач. Проверить доступность папок и дисков можно в пункте меню «Сеть» в Проводнике Windows.
ii. Используйте рекомендуемые настройки Брандмауэра (Фаервола) в Windows. Это можно проверить через меню в Панели инструментов.
iii. Если Вам известен пароль от локальной сети организации, не распространяйте его другим лицам и гостям организации.
iv. Если в организации имеется гостевой доступ в Интернет, можете предоставлять его гостям. Если нет такого доступа, предложите разделить доступы для гостей и персонала.

b. Использование интернета в публичных сетях
i. Перед использованием сетей публичного доступа убедитесь, что Ваш Брандмауэр включен и имеет рекомендуемые настройки.
ii. Выключите обнаружения вашего компьютера в публичных сетях и отключите общие доступы ко всем папкам и дискам.

5. Защита электронной почты и других учетных записей в он-лайн ресурсах



a. При использовании он-лайн ресурсов убедитесь в правильности ввода адреса ресурса с целью защиты ваших учетных записей от злоумышленников. Например, facebook.com или fasebook.com.

b. Убедитесь, что в разных учетных записях используются разные пароли, и постарайтесь изменять пароли каждые 2-3 месяца.

c. Не записывайте пароли на бумажках или в записных книжках.

d. При возможности, используйте двухфакторную аутентификацию. О возможностях двухфакторной аутентификации он-лайн ресурсов можно прочитать в разделе «Помощь» каждого используемого Вами ресурса.

[1] BitLocker (точное название BitLocker Drive Encryption) — это технология шифрования содержимого дисков компьютера, разработанная компанией Microsoft. Она впервые появилась в Windows Vista.