Что делать, чтобы обеспечить себе безопасное пребывание в интернете?

1. Пользуйтесь программными средствами защиты (антивирусами).

2. Работайте только на актуальных версиях программного обеспечения (браузеры, приложения и операционные системы).

3. Работая за чужим компьютером или за компьютером в общественном месте, никогда не пользуйтесь функциями браузеров по запоминанию паролей.

Отвечайте отрицательно на вопросы о сохранении паролей. Не забывайте выйти из учетной записи после окончания работы на чужом устройстве или примените для работы функцию браузеров «приватное окно».

4. При регистрации на сайтах используйте рекомендации по выбору стойкого пароля. Всегда обращайтесь к средствам восстановления пароля и двухфакторной аутентификации*, если такие возможности предоставлены сервисом (секретные вопросы, дополнительные почты или телефоны).

*Используйте двухфакторную аутентификацию

Кроме ввода пароля, нужно также ввести код, который приходит на почту/телефон или получается из аппаратного ключа-генератора.

Вспомогательные инструменты:

-физическое устройство;

-приложение-генератор проверочных кодов;

-смс и звонки/почта.

- следить за постоянным обновлением программного обеспечения и средств защиты на устройстве;

- использовать сервисы удаленной работы, согласованные и разрешенные службой ИБ/ИТ;

- следить за соблюдением правил парольных политик для рабочих сервисов удаленной работы;

- ограничить доступ к рабочему устройству посторонних лиц, не имеющих отношения к вашей организации;

- использовать рабочее персональное устройство только для решения рабочих вопросов.

Для обеспечения безопасности вашего интернет-соединения, необходимо:

Найти безопасное подключение к сети интернет.

Разрешено использовать:

- частную/домашнюю Wi-Fi сеть, защищенную паролем по способу защиты доступа WPA2;

- интернет-соединение телефонных операторов (раздача с мобильного устройства / Wi-Fi или USB-модем).

Запрещено использовать:

- открытые Wi-Fi сети общественных мест и организаций (метро, кафе и др.).

Как очистить метаданные?

1. MacOS: в открытом документе перейти «Сервис-Защитить документ-Конфиденциальность» и поставить галочку «Удалить из этого файла персональные данные при сохранении».

2. Windows: Файл → Сведения → Поиск проблем → Инспектор документов → Проверить → Свойства документа и персональные данные → Удалить все.

3. Программы типа ExifPurge

В мессенджерах:

1. Используйте облачные пароли, pin-коды.

2. Контролируйте активные сессии:

Telegram: Настройки – Устройства.

WhatsApp: WhatsApp Web.

3. Никому не сообщайте информацию из системных сообщений (проверочные коды, коды доступа).

В социальных сетях:

1. Установите двухфакторную аутентификацию на все аккаунты.

2. Используйте резервные каналы восстановления аккаунтов.

ВАЖНО! В качестве резервного канала нужно использовать ту почту, которую вы нигде больше в интернете не размещали. Придумывая контрольные вопросы не используйте факты из личной жизни, даты, имена и любую другую информацию, которую можно найти в открытом доступе.

Для обеспечения безопасности вашего устройства при удаленной работе, необходимо:

- использовать отдельное устройство. Если такой возможности нет, завести на личном устройстве отдельную учетную запись;

- согласовать использование персонального устройства для удаленной работы с вашей службой ИБ/ИТ;

- установить пароль для учетной записи, соблюдая все правила парольной политики;

5. При создании аккаунтов, почтовых адресов и личных страниц не указывайте свои персональные данные в домене (телефон@ mail.ru , ФИО@ yandex.ru и пр.).

6. Внимательно относитесь к присланным вам ссылкам на сайты. Проверьте: знаком ли вам данный сайт, нет ли ошибок в написании доменного имени (опечатки, удвоенные символы, переставленные буквы). Остерегайтесь «коротких» ссылок - часто злоумышленники используют подобные сервисы для сокрытия настоящего адреса, на который вас просят перейти.

7. Никогда не передавайте конфиденциальные данные в ответ на письма или сообщения в социальных сетях. Не предоставляйте ваши персональные данные людям, в личности которых вы недостаточно уверены.

8. Не вводите свои данные на сайтах, которые не используют протокол HTTPS* (в адресной строке браузера ссылка должна начинаться с символов «https: //»).

**Протокол HTTPS - расширение протокола HTTP для поддержки шифрования в целях повышения безопасности.*

9. Не публикуйте в социальных сетях данные, которые могут нанести репутационный, моральный или финансовый урон вам или вашим близким.

10. При необходимости ввести личные/ финансовые/учетные данные на каком-либо сайте всегда обращайте внимание на адресную строку в браузере. Проверьте, действительно ли вы находитесь на том сайте, на котором предполагаете.

11. Не устанавливайте расширения* браузеров без крайней необходимости. Следите за разрешениями, которые вы им даете.

**Расширение - компьютерная программа, которая увеличивает функциональные возможности браузера.*

12. Используйте шифрование при передаче данных. Защищайте документы (rar, zip и другие форматы) паролем.

13. Очищайте метаданные* в изображениях и документах

**Метаданные — это информация о создателе файла, геолокация, информация о фото/видео оборудовании и пр.*

14. Не пользуйтесь автосохранением паролей в браузерах, сервисах и приложениях.