Доступ к камере и фотографиям

Часто приложения запрашивают доступ к микрофону, камере, фото и видео. Открыть доступ можно, но лучше единоразово во время использования сервиса.

Удаление cookies

Cookies — это фрагмент данных о сайтах, на которые вы раньше заходили. Благодаря этим фрагментам, сайты запоминают историю покупок, наполнение корзины, фиксируют сведения о вашей активности и интересах. Периодически чистите файлы cookies в телефоне и в ноутбуке для обеспечения собственной безопасности.

Защищённое соединение

Банковские, государственные сайты и интернет-магазины применяют защищённое соединение, с помощью которого все сведения шифруются посредством SSL. Чтобы определить, использует ли сайт защищённое соединение, обратите внимание на зелёный замочек рядом с названием сайте https://. Если он есть, значит, ваш адрес и банковские реквизиты защищены. Проверяйте наличие этого знака каждый раз, когда вводите личные данные в информационном пространстве.

Wi-Fi в общественных местах

Во многих кафе и торговых центрах есть возможность подключить бесплатный Wi-Fi, однако это небезопасно. Мошенники могут легко заполучить ваши пароли. Когда вы находитесь в общественном месте и используете открытый Wi-Fi, то не заходите на сайты, в которых нужно ввести пароль или личную информацию. В таких случаях лучше воспользоваться мобильным интернетом.

ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«СРЕДНЯЯ ШКОЛА №9 Г.МОЗЫРЯ»

Практика применения правил и норм информационной безопасности

Кибербезопасность: как защитить персональные данные в интернете

Методы защиты персональных данных в сети, которые помогут предотвратить кражу паролей и отслеживание ваших действий в интернете.

Сайты, мобильные приложения и онлайн-сервисы регулярно собирают сведения о посетителях. С одной стороны, это практично — сайты запоминают логины, пароли и автоматически вводят их для входа в личный кабинет, хранят ссылки, которые вы раньше открывали. С другой стороны, мошенники могут взломать ваш аккаунт и получить доступ к почте или банковской карте. Чтобы обезопасить себя, запомните несколько правил.

Пароли

Это главный способ защитить себя в сети, поэтому к созданию и хранению паролей важно отнестись очень внимательно.

Создавайте длинные пароли, используйте заглавные и строчные буквы, различные знаки, цифры. Придумайте для каждого сервиса и программы свой пароль. Или запомните 5 типовых паролей, при этом они не должны совпадать с самыми распространенными паролями. *Нередко бывает, что персональная информация утекает в сеть по вине владельцев информационных систем. Для проверки своих учетных данных рекомендуем использовать этот ресурс https://monitor.firefox.com/.*

- Не используйте следующую информацию для создания паролей: дата рождения, номер телефона, адрес, имена и фамилии близких людей. Эти данные злоумышленники могут отыскать самостоятельно в интернете и разгадать ваш пароль.
- Все пароли лучше выписать в яркий блокнот, который нужно хранить в сухом и труднодоступном месте. Также можно установить специальную программу «Менеджер паролей», в которой данные будут надежно сохранены. Не создавайте файлы с паролями на ноутбуке или в телефоне, мошенники могут взломать систему и получить нужные данные.
- Настройте двухэтапную аутентификацию, чтобы защитить свои аккаунты. Проверяйте сообщения на почте и смс — в случае если придет подозрительное письмо, вы успеете отреагировать и пресечь попытку взлома.

Пример самых популярных типов паролей

123456	1234567	123	111111	123123
123456789	qwerty	qwer123456	987654321	123abc

Цифровая гигиена

- Не делитесь слишком личной информацией в социальных сетях, чтобы мошенники не могли воспользоваться этими сведениями.
- Следите за своим цифровым следом, так как приложения и сайты собирают данные о вашем местоположении. Полностью скрыть геолокацию не получится, но можно ее отключить в тех программах, в которых она не нужна для работы.
- Делайте резервное копирование данных, в последнее время участились случаи блокировки устройств с целью выкупа.

Политика конфиденциальности

Во время установки программы, подключения онлайн-сервиса или регистрации в социальной сети важно прочитать политику конфиденциальности. Проверьте, чтобы сервис не мог управлять вашей персональной информацией — фото, видео, номер телефона, электронный адрес.