Приложение 3.3

**Средства защиты персональных данных**

«Три кита» защиты персональных данных: Надежные пароли позволят защитить ваши аккаунты на онлайн-ресурсах и приложениях от третьих лиц. Настройки приватности позволяют вам определить уровень доступа других пользователей к вашим персональным данным, размещенным на различных онлайн-ресурсах.

Правила управления персональными данными помогут вам определиться, как персональные данные, размещенные в Интернете, могут повлиять на вашу репутацию в Сети.

**Осторожно, онлайн-мошенники!**

Прежде чем вводить свои персональные данные в Интернете, необходимо убедиться, что вы находитесь именно на том ресурсе, на который хотели попасть, а не на поддельной (фишинговой) странице, созданной мошенниками.

Существует несколько простых способов убедиться в подлинности ресурса:

Всегда обращайте внимание на адресную строку браузера. Адрес поддельной странички может отличаться всего на одну букву, которую легко не заметить, например: в адресе [www.odnoklassniki.ru](http://www.odnoklassniki.ru) может быть пропущена всего одна буква «s», но это будет уже совсем другой сайт. Не стоит переходить на ресурсы, требующие ввода персональных данных, по ссылкам, которые вы получили по электронной почте или в личной переписке, – многие из них ведут на поддельные сайты. Забейте адрес в адресную строку самостоятельно, а еще лучше используйте для поиска нужных ресурсов надежные поисковые системы, например, Яндекс. Прежде чем вводить персональные данные в Интернет, убедитесь, что ресурс, на котором вы находитесь, использует защищенное соединение. Если в адресной строке браузера присутствует иконка замка, а сам адрес начинается с аббревиатуры https:// вместо привычной http://, то такое соединение использует шифрование при передаче ваших персональных данных. В этом случае злоумышленникам будет гораздо сложнее перехватить и воспользоваться вашими персональными данными.

Комплексные антивирусные программы также могут помочь защититься от мошенников. Многие из них содержат базы данных опасных и ненадежных ресурсов и способны предупреждать о возможной опасности, блокируя переход по фишинговым ссылкам. Следует помнить о том, что надежно защитить от мошенников может соблюдение всех этих правил одновременно.

**Защита персональных данных на своем устройстве:**

Чтобы удалить «цифровые следы» с компьютера после работы в Интернете очистите «журнал посещений» (в браузере) и «историю поисковых запросов» (в аккаунте сайта-поисковика). Функция «очистка диска» (в операционной системе) позволит вам удалить автономные веб-страницы, временные файлы из Интернета, а также cookies (небольшие фрагменты данных, которые отправляются онлайн-ресурсом и хранятся на компьютере пользователя; они помогают сайтам «запоминать» пользователей и их индивидуальные предпочтения), которые также могут многое рассказать о вашей работе в Сети. Все это вы сможете сделать, только если обладаете правами администратора. В противном случае используйте режим «инкогнито», чтобы исследовать Интернет, не оставляя «следов».

В настройках программ сетевой защиты также можно установить запрет на загрузку временных файлов и cookies с незнакомых сайтов, ограничившись лишь проверенными и надежными ресурсами. Будьте внимательны с настройками мобильных приложений: отключите опцию «автосинхронизации» данных, автоматического проставления «геометок» и т. д., если хотите избежать случайного попадания персональных данных в Сеть.

**Защита персональных данных на чужом устройстве:**

При входе в свой аккаунт с чужого устройства всегда выбирайте опцию «чужой компьютер», «не сохранять пароль», «безопасный ввод» и т. д. (на странице онлайн-ресурса). В этом случае вы можете быть уверены, что никто не войдет в ваш аккаунт после вас.

Чтобы не оставить «цифровых следов» на чужом устройстве, используйте функцию «инкогнито» (в браузере). Благодаря ей история поисковых запросов и посещенных страниц не сохраняется в браузере, а сайты не загружают cookies на устройство.

**Защита персональных данных от третьих лиц:**

Используя вкладку «настройки приватности» (на странице онлайн-ресурса), запретите другим пользователям отмечать вас на фотографиях и упоминать в постах. Ограничьте круг лиц, которые могут комментировать ваши записи. Как правило, добавление пользователя в «черный список» автоматически лишает его возможности просматривать и комментировать ваши посты, а также упоминать вас в своих постах. Если другой пользователь использует ваши персональные данные, на пример фотографии, без вашего согласия, вы можете пожаловаться в «службу поддержки ресурса» (на странице онлайн-ресурса), приложив доказательства нарушения. Если другой пользователь, разместив недостоверную или устаревшую информацию, нанес существенный урон вашей чести и достоинству, вы можете обратиться в суд.