



ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ



ПОДКЛЮЧЕНИЕ К ИНТЕРНЕТУ

- ✓ Выключайте Wi-Fi, когда им не пользуетесь.
- ✓ Отключите функцию автоматического подключения к Wi-Fi в телефоне.
- ✓ Используйте проверенные Wi-Fi-соединения.
- ✗ Не заходите в онлайн-банки и другие важные сервисы через открытые Wi-Fi-сети в кафе или на улице. Воспользуйтесь мобильным интернетом.



РАБОТА С ЭЛЕКТРОННОЙ ПОЧТОЙ

- ✓ Используйте разную электронную почту для разных целей (личная, рабочая и развлекательная).
- ✓ Для каждого электронного ящика придумайте разные сложные пароли.
- ✗ Не переходите по ссылкам, пришедшим в сообщениях от незнакомых людей.
- ✗ Не отвечайте на спам и подозрительные письма.



ПАРОЛЬНАЯ ЗАЩИТА

- ✗ Не записывайте пароли на бумаге или в файле на компьютере.
- ✓ Используйте двухфакторную аутентификацию, например, пароль и смс-код.
- ✗ Не используйте в качестве секретного вопроса девичью фамилию матери, если она есть в социальных сетях.
- ✓ Регулярно меняйте пароли.



ПРОДОЛЖЕНИЕ



ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ



БЕЗОПАСНОСТЬ ЛИЧНЫХ ДАННЫХ

-  Не пересылайте конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через соцсети.
-  Не отправляйте сканы документов на неизвестные электронные адреса.
-  Не публикуйте в интернете свой адрес и другую личную информацию.
-  При отправке конфиденциальной информации на сайтах адрес должен начинаться с «https://», рядом с которым нарисован закрытый замок. Так передаваемая информация останется конфиденциальной.
-  Регулярно выполняйте резервное копирование данных, в т.ч. и с телефона, на внешний физический носитель и (или) в облачное хранилище.



ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

-  Банки не рассылают писем с просьбой изменить свой пароль, ввести номер карты и секретный код подтверждения.
-  Если пришло сообщение с просьбой от знакомого человека срочно выслать денег, ничего не отправляйте.
-  Совершайте покупки только в надежных интернет-магазинах.
-  Заведите для покупок в интернет отдельную карту, не привязанную к основным банковским счетам. Не храните на ней большие суммы
-  При оплате в интернете вас должны переадресовать на защищенную страницу (адрес начинается с «https://»).
-  Подключите в своем банке СМС- или PUSH-информирование об операциях по картам.



ПРОДОЛЖЕНИЕ



ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ



БЕЗОПАСНОСТЬ В МЕССЕНДЖЕРАХ

- ✓ Включите двухфакторную аутентификацию для учетной записи.
- ✗ Никому не передавайте одноразовые коды.
- ✓ Проверяйте новые контакты. Блокируйте и удаляйте подозрительные контакты.
- ✗ Не переходите по ссылкам, даже от друзей. Аккаунт мог быть взломан.



АНТИВИРУСНАЯ БЕЗОПАСНОСТЬ

- ✓ Установите на компьютер, планшет и мобильный телефон антивирусную программу. Периодически обновляйте антивирус.
- ✓ При подозрении на заражение устройства (подвисание, нетипичная работа, самопроизвольные действия) запустите проверку антивируса.
- ✓ При подключении сторонних устройств (флешек, карт памяти, мобильных телефонов) запускайте их проверку антивирусом.
- ✗ Не запускайте неизвестные файлы, особенно с расширением .exe
- ✗ Не скачивайте сомнительные приложения или приложения на неизвестных сайтах. Проверьте приложение антивирусом.



БЕЗОПАСНОСТЬ ДЕТЕЙ

- ✓ Используйте специальные режимы интернета для детей («детский» интернет).
- ✓ Установите безопасный режим для ребенка в браузерах и программах.
- ✓ Говорите с ребенком об интернете, что можно искать, с кем общаться и какую информацию о себе сообщать.
- ✓ Объясните ребенку, что при общении в сети с незнакомыми, они могут оказаться не теми, за кого себя выдают.



ПРОДОЛЖЕНИЕ



ИНФОРМАЦИОННЫЕ КАНАЛЫ ПО КИБЕРБЕЗОПАСНОСТИ



**Канал «Вестник Киберполиции России»
в «Макс»**



Канал «Полиция Южного Урала» в «Макс»



Канал Банка России в «Макс»



**Раздел «Профилактика
кибермошенничества» на сайте
Минцифры Челябинской области**



**Канал Минцифры Челябинской области
«Процифру74» в «Макс»**