РОС КАЧЕСТВО
Российская система качества

ВВЕДЕНИЕ

В ЦИФРОВУЮ ГРАМОТНОСТЬ

ПОДКЛЮЧЕНИЕ К ОБЩЕСТВЕННЫМ СЕТЯМ WI-FI МОЖЕТ НЕСТИ ПОТЕНЦИАЛЬНУЮ УГРОЗУ ВАШЕЙ ЦИФРОВОЙ БЕЗОПАСНОСТИ

Однако при соблюдении нескольких простых правил вы можете значительно снизить риск взлома вашего устройства:

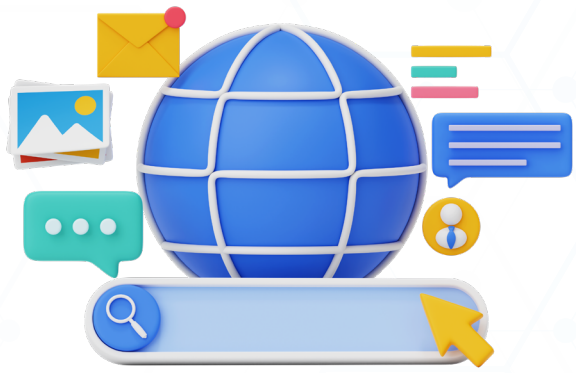
- **Отключать автоматическое подключение**
  и в целом Wi-Fi в общественных местах
  (лучше использовать мобильный интернет)

- **Удалять сохраненные ранее**
  и неиспользуемые Wi-Fi-подключения

- **Не передавать важные данные**
  через общественные Wi-Fi-сети или использовать VPN

- **Использовать антивирусное программное обеспечение**
  и своевременно обновлять компоненты системы

- **В случае подключения к открытой сети**
  убедитесь, что она действительно принадлежит данной локации: как правило, это становится очевидно из названия
  (пример: Mos_metro_WiFi, GUM_wifi, Vnukovo_Free Wifi и т. п.)



ЧТО СДЕЛАТЬ, ЧТОБЫ ОТПИСАТЬСЯ ОТ РЕКЛАМНЫХ РАССЫЛОК

01 Большинство сервисов предлагают направить письменное заявление об отказе по электронной почте или в редких случаях явиться лично

02 Если такой информации нет, то на сайте просто найдите электронный адрес компании и в свободной форме направьте письмо с просьбой прекратить рассылки

03 Обратитесь к своему сотовому оператору и попросите отписать вас от всех спам-рассылок

04 Оставьте жалобу на

https://fas.gov.ru/pages/zhaloby-sms

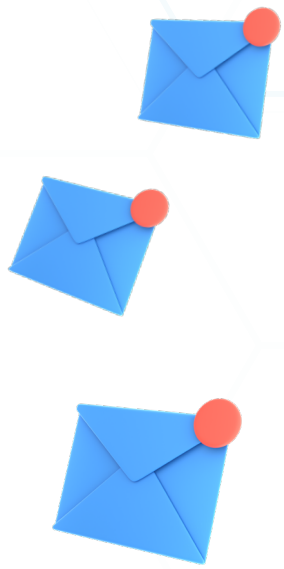
05 Воспользуйтесь услугами сотовых операторов для блокировки спама

06 Используйте опцию умной блокировки на своем смартфоне. При получении нежелательного сообщения в меню просто нажмите «Заблокировать».

КАК НЕ ПОПАСТЬ НА МОШЕННИКОВ ПРИ ПОИСКЕ РАБОТЫ

Внимательно читайте объявления и сообщения

Мошеннические электронные письма и СМС часто содержат очевидные ошибки и нечеткие контактные данные



Изучайте сайты и социальные сети

Мошеннические содержат минимум информации или созданы совсем недавно

Не предоставляйте личные данные

Мошенники пытаются запросить паспортные данные, сведения о месте жительства и счетах. Реальный работодатель не требует таких данных до этапа заключения трудового договора

Не ведитесь на громкие обещания

Вы можете получить заманчивое предложение о работе с высокой зарплатой, но с расплывчатым описанием обязанностей. Если вы подадите заявку, то можете обнаружить, что «работодатель» просит оплатить сборы или раскрыть конфиденциальные данные

Выбирайте места для общения

Реальный работодатель устроит онлайн-собеседование в одном из известных приложений с хорошей репутацией. Если же вас просят установить незнакомое ПО, особенно проприетарное, – это признак того, что работает мошенник

ГЛАВНЫЕ СОВЕТЫ ПО КИБЕРБЕЗОПАСНОСТИ

Проверять сайты, которые вы посещаете
Для этого скопируйте адрес и зайдите на сервис для проверки доменного имени reg.ru. В полученной информации вас должно интересовать два пункта – кому принадлежит сайт и дата регистрации. Если сайту меньше месяца или вообще пара недель, то стоит задуматься о его благонадежности

Регулярно обновляйте браузер,
последние версии содержат новейшую защиту от киберугроз.

Проверяйте сайт,
прежде чем переводить деньги с его помощью

Если проверить сайт нет возможности,
попросите у продавца выставить вам счет для безналичной оплаты. Официально зарегистрированные юридические лица сделают это без вопросов

Не вступайте в диалог с людьми,
которые просят деньги либо присылают подозрительные ссылки

Если знакомый человек просит срочно перевести ему деньги,
уточните у него лично, действительно ли он в этом нуждается. Часто мошенники пишут со взломанных страниц друзьям жертвы

10 ПРИЗНАКОВ, ЧТО ВАМ ПИШЕТ ИЛИ ЗВОНИТ МОШЕННИК

01 **Наличие запутанной истории**

(что кто-то взял на вас кредит по доверенности и т.п.)

02 **Применение разных видов принуждений**

в разговоре
(«если вы не..., то тогда мы...»)

03 **Человек дает уклончивые ответы**

04 **Угрозы**

05 **Предложения перейти по сторонней ссылке**

06 **В текстах содержатся грамматические ошибки**

07 **Провокации**

(«только сегодня и только для вас»)

08 **Звонящий упоминает МВД, ЦБ**

или представляется их сотрудником

09 **Громкие обещания**

(«Вложи 1000 р – через месяц получи 10К р», «Авиабилеты за полцены» и т. п.)

10 **У пишущего в соцсети плохо оформленный профиль**

14 СПОСОБОВ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ СМАРТФОНА

1. СИЛЬНЫЙ ПАРОЛЬ

Придумайте уникальную комбинацию букв, цифр и символов в качестве пароля. Мы рекомендуем сочетать элементы известных вам предметов и явлений (названия книг, фильмов и т. п.), кроме имен и дат рождения, с добавлением цифр и спецсимволов (* # %).

Не используйте одну и ту же комбинацию везде и всюду, особенно для важных аккаунтов и приложений.

2. АУТЕНТИФИКАЦИЯ ПО БИОМЕТРИИ

Биометрическая аутентификация — гораздо более безопасная альтернатива, например, цифровой комбинации, поскольку ваши отпечатки, например, уникальны и их невозможно угадать.

3. ОБНОВЛЕНИЯ

Важно регулярно устанавливать обновления, чтобы залатать бреши в системе безопасности, которые постоянно возникают. Вы можете включить автоматические обновления.

Рекомендуем не выбирать опции «Игнорировать» или «Отложить», а скачивать все оперативно и своевременно.

4. ПРИЛОЖЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Чтобы избежать сайтов с вредоносным контентом, установите антивирус, чтобы предотвратить заражение вредоносным ПО. Это может помочь вам избежать взлома, когда другие средства защиты не работают.

5. ИЗЛИШНИЕ РАЗРЕШЕНИЯ ПРИЛОЖЕНИЙ

Приложения могут запрашивать доступ к вашему местоположению, камере, микрофону, файлам и хранилищу. Внимательно относитесь к таким просьбам.

Ведь приложения со сверхразрешениями могут прослушивать ваши разговоры, снимать фото и видео без вашего согласия или постоянно отслеживать ваше местоположение. Предоставление ненужных разрешений приложениям может быть приравнено к установке вредоносного ПО.

6. ОБЩЕСТВЕННЫЙ WI-FI

Хакеры вполне могут использовать общедоступные сети Wi-Fi для перехвата соединения или распространения вредоносного ПО.

Если выбора нет и придется воспользоваться общедоступным Wi-Fi, то установите виртуальную частную сеть (VPN). Она зашифрует ваши данные при передаче и защитит подключение.

7. АКТИВИРУЙТЕ УДАЛЕННОЕ ОТСЛЕЖИВАНИЕ И ОЧИСТКУ ТЕЛЕФОНА

Смартфоны iPhone и Android имеют функции удаленного поиска, блокировки или очистки потерянного или украденного устройства.

Режим пропажи на iOS можно активировать, войдя в свою учетную запись iCloud. Заблокировать гаджет удаленно можно, если у вас есть аккаунт в Google.

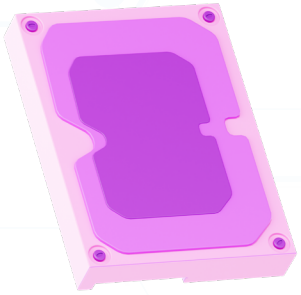
8. ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ (2FA)

Поскольку смартфоны iPhone и Android подключены к учетным записям iCloud или Google, вы можете включить двухфакторную аутентификацию для дополнительной безопасности. Это поможет защитить ваш телефон на случай, если хакеры украдут ваш пароль.

9. ПЕРЕПРОВЕРКА ССЫЛОК И ПРЕДЛОЖЕНИЙ О ЗАГРУЗКЕ

Распознавание подозрительного контента может существенно повлиять на безопасность вашего мобильного устройства.

10. ЗАШИФРУЙТЕ СВОЮ SD-КАРТУ



Если на вашем устройстве есть слот под SD-карту, зашифруйте ее.

Сделать это можно в настройках в разделе безопасности. Заранее сделайте резервную копию данных, так как вам может потребоваться отформатировать SD-карту (стереть все данные) перед ее шифрованием.

11. ОТКЛЮЧИТЬ BLUETOOTH, КОГДА ОН НЕ ИСПОЛЬЗУЕТСЯ

Хакеры могут воспользоваться уязвимостями Bluetooth-соединения только в том случае, если ваше устройство находится в пределах досягаемости и видимо для них.

Поэтому на смартфоне принимайте запросы на сопряжения только от знакомых устройств. Выключайте Bluetooth, как только закончите его использовать.

12. ИСПОЛЬЗУЙТЕ VPN

Высококачественный, платный VPN шифрует ваши данные и скрывает IP-адрес.

Таким образом, хакерам гораздо труднее отслеживать вас в интернете. А перехваченные данные становятся бесполезными.

13. УДАЛИТЬ СТАРЫЕ ПРИЛОЖЕНИЯ

Вам правда нужны все приложения на вашем телефоне? Ведь устаревшие и ненужные могут открыть доступ к вашему устройству хакерам. Не говоря уже о том, что неиспользуемое ПО захламляет память устройства.

Если вы не использовали какое-то приложение в течение нескольких месяцев, лучше удалите его. Если для приложения была заведена учетная запись, то также удалите и ее.

14. РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ

Оно не обязательно защитит ваше устройство от киберпреступников, но может свести к минимуму ущерб от атаки и потери данных.

Если хакеры заразят устройство программой-вымогателем, восстановить работу телефона все еще можно будет с помощью сброса настроек. Однако в этом случае все ваши данные будут потеряны.

Поэтому целесообразно регулярно сохранять резервные копии своих файлов в облачных хранилищах.

РОС КАЧЕСТВО
Российская система качества

Премия Правительства Российской Федерации в области качества

ОРГАНИК ORGANIC РОС КАЧЕСТВО

ЗЕЛЕНЫЙ ЭТАЛОН GREEN ONE

ВИННЫЙ ГИД РОССИИ