

## КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СМАРТФОНОМ, ПЛАНШЕТОМ

*Эта памятка поможет тебе безопасно пользоваться  
мобильными устройствами*

Смартфоны и планшеты содержат в себе взрослый функционал и могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

### Советы по безопасному использованию мобильных устройств

- 1 Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
- 2 Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
- 3 Необходимо обновлять операционную систему своего смартфона.
- 4 Используй антивирусные программы для мобильных телефонов.
- 5 Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.
- 6 После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.
- 7 Периодически проверяй, какие платные услуги активированы на твоем номере.
- 8 Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.
- 9 Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.



## КАК БЕЗОПАСНО РАСПЛАЧИВАТЬСЯ ЭЛЕКТРОННЫМИ ДЕНЬГАМИ

*Эта памятка поможет тебе безопасно расплачиваться  
электронными деньгами*

Электронные деньги – это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и неанонимные. Разница в том, что анонимные – это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

### Меры защиты электронных денег

- 1 Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства.
- 2 Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля.
- 3 Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли – это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак. Например, StROng!;
- 4 Не вводи свои личные данные на сайтах, которым не доверяешь.



## КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

Эта памятка поможет тебе безопасно пользоваться  
электронной почтой

Электронная почта – это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя\_пользователя@имя\_домена. Также, кроме передачи простого текста, имеется возможность передавать файлы.

### Меры защиты электронной почты

- 1 Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге.
- 2 Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2018@» вместо «андрей2005@».
- 3 Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присыпаемый по SMS.
- 4 Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.
- 5 Если есть возможность написать самому свой личный вопрос, используй эту возможность.
- 6 Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Этот электронный адрес не надо использовать при регистрации на форумах и сайтах.
- 7 Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.
- 8 После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».



## КАК ОБЕСПЕЧИТЬ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РЕБЕНКА

*Эта памятка поможет обеспечить  
информационную безопасность вашего ребенка*

- 1 Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку – главный метод защиты.
- 2 Если ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и другие), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
- 3 Проверьте, с какими другими сайтами связан социальный сервис вашего ребенка. Страницы вашего ребенка могут быть безопасными, но могут содержать и ссылки на нежелательные и опасные сайты (например, порносайт или сайт, на котором друг упоминает номер сотового телефона вашего ребенка или ваш домашний адрес).
- 4 Поощряйте вашего ребенка сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда он это делает (из-за опасения потерять доступ к интернету дети не говорят родителям о проблемах, а также могут начать использовать интернет вне дома и школы).
- 5 Будьте в курсе сетевой жизни вашего ребенка. Интересуйтесь его друзьями в интернете так же, как интересуетесь реальными друзьями.



## Памятка «Как безопасно пользоваться сетью Wi-Fi»

### КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СЕТЬЮ WI-FI

*Эта памятка поможет тебе безопасно пользоваться сетью Wi-Fi*

Wi-Fi – это беспроводной способ передачи данных, использующий радиосигналы. Wi-Fi – аббревиатура от английского словосочетания Wireless Fidelity, что дословно переводится как беспроводная точность. Бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но общедоступные сети Wi-Fi не являются безопасными.

#### Советы по безопасному использованию Wi-Fi

- 1 Не передавай свою личную информацию через общедоступные сети Wi-Fi. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера.
- 2 Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твоё устройство.
- 3 При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.
- 4 Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети или в электронную почту.
- 5 Используй только защищенное соединение через HTTPS, а не HTTP, то есть при наборе веб-адреса вводи именно «https://».
- 6 В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

