



РОСКОМНАДЗОР

**УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ  
ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И  
МАССОВЫХ КОММУНИКАЦИЙ  
ПО СИБИРСКОМУ ФЕДЕРАЛЬНОМУ  
ОКРУГУ**

(Управление Роскомнадзора  
по Сибирскому федеральному округу)

Ул. Советская, 33, а/я 325, г. Новосибирск, 630099  
Справочная: (383) 349-55-89; факс (383) 349-55-96  
E-mail: rsockanc54@rkn.gov.ru

16.09.2020 № 13583-06/54

На  
Об оказании содействия в популяризации  
вопросов кибербезопасности в сети  
«Интернет»

Начальнику департамента  
образования мэрии города  
Новосибирска

Р. М. Ахметгарееву

Красный проспект, д. 34, г.  
Новосибирск, Новосибирская  
область, 630099

pochta@admnsk.ru



Уважаемый Рамиль Миргазянович!

В целях защиты персональных данных и профилактики правонарушений в сфере законодательства о персональных данных Управлением Роскомнадзора по Сибирскому федеральному округу проводятся различные профилактические мероприятия, на которых специалисты разъясняют основные положения законодательства о персональных данных, правила бережного отношения к своим и чужим персональным данным, демонстрируют тематические ролики и презентации.

В настоящее время, с учетом действия в Новосибирской области ограничительных мер, принятых в связи с распространением новой коронавирусной инфекции, проведение представителями Управления Роскомнадзора по Сибирскому федеральному округу (далее – Управление) очных профилактических мероприятий не представляется возможным.

В связи с изложенным, убедительно просим оказать содействие в популяризации информационной памятки по вопросам кибербезопасности в сети «Интернет» (далее – памятка) среди сотрудников Департамента образования мэрии города Новосибирска (далее – Департамент) и его подведомственных учреждений (организаций), а также граждан, обращающихся в Департамент и его подведомственные учреждения (организации), путем размещения памятки на официальном сайте, в социальных сетях и на информационных стендах Департамента и его подведомственных учреждений.

О результатах рассмотрения настоящего письма прошу сообщить в Управление на адрес электронной почты rsockanc54@rkn.gov.ru до 15.10.2020 с указанием количества подразделений, в которых размещена памятка, и URL-адреса интернет-страницы, в случае размещения памятки на сайте.

Департамент образования  
мэрии города Новосибирска  
Дк.№ 14.1104511  
«17» 09 2020

- Приложение: 1. Файл «Информационная памятка по вопросам кибербезопасности в сети «Интернет». docx»;  
2. Информационная памятка по вопросам кибербезопасности в сети «Интернет» на 5 л., в 1 экз.

Заместитель  
руководителя

Визуализация ЭП

P. A. Марущак



## **Информационная памятка по вопросам кибербезопасности в сети «Интернет»**

### **Компьютерные вирусы**

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (копированию). В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

#### **Методы защиты от вредоносных программ:**

1. Используйте современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
2. Постоянно устанавливайте патчи (обновления, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивайте их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включите его;
3. Работайте на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на вашем персональном компьютере;
4. Используйте антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничьте физический доступ к компьютеру для посторонних лиц;
6. Используйте внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников;
7. Не открывайте компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислали ваши знакомые. Уточните, отправляли ли они данные файлы.

### **Сети WI-FI**

С помощью WI-Fi можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Так же WI-Fi является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

#### **Советы по безопасности работы в общедоступных сетях Wi-fi:**

1. Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-либо номера;
2. Используйте и обновляйте антивирусные программы и брандмауэр. Тем самым вы обезопасите себя от закачки вируса на свое устройство;
3. При использовании Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;

4. Не используйте публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту;

5. Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводите именно «<https://>»;

6. В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без вашего согласия.

### **Социальные сети**

Социальная сеть - это сайт, который предоставляет возможность людям осуществлять общение между собой в интернете. Чаще всего в них для каждого человека выделяется своя личная страничка, на которой он указывает о себе различную информацию, начиная от имени, фамилии и заканчивая личными фотографиями. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

#### **Основные советы по безопасности в социальных сетях:**

1. Ограничьте список друзей. У вас в друзьях не должно быть случайных и незнакомых людей;

2. Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату своего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как вы и ваши близкие планируете провести каникулы;

3. Защищайте свою репутацию - держите ее в чистоте и задавайте себе вопрос: хотели бы вы, чтобы другие пользователи видели, что вы загружаете? Подумайте, прежде чем что-то опубликовать, написать и загрузить;

4. Если вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информацию: имя, место жительства, место работы (учебы) и прочее;

5. Избегайте размещения фотографий в Интернете, где вы изображены на местности, по которой можно определить ваше местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда, если вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

### **Электронные деньги**

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 не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в не анонимных идентификации пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

#### **Основные советы по безопасной работе с электронными деньгами:**

1. Привяжите к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудете свой платежный пароль или зайдете на сайт с незнакомого устройства;
2. Используйте одноразовые пароли. После перехода на усиленную авторизацию вам уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выберите сложный пароль. Преступникам будет непросто 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 и т.п. Например, StROng!;
4. Не вводите свои личные данные на сайтах, которым не доверяете.

#### **Электронная почта**

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.

#### **Основные советы по безопасной работе с электронной почтой:**

1. Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, которых вы знаете и кто из них первый в рейтинге;
2. Не указывайте в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «рома13»;
3. Используйте двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присыпаемый по SMS;
4. Выберите сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используйте эту возможность;
6. Используйте несколько почтовых ящиков. Первый для частной переписки с адресатами, которым вы доверяете. Этот электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывайте файлы и другие вложения в письмах даже если они пришли от ваших друзей. Лучше уточни, отправляли ли они вам эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

#### **Кибербуллинг или виртуальное издевательство**

Кибербуллинг — преследование сообщениями, содержащими оскорблении, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

#### **Основные советы по борьбе с кибербуллингом:**

1. Не бросайтесь в бой. Успокойтесь. Если вы начнете отвечать оскорблением на оскорблении, только больше разожжете конфликт;
2. Управляйте своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все ваши действия и сохраняет их. Удалить их будет крайне затруднительно;
5. Ведите себя вежливо;
6. Игнорируйте единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7. Ограничьте доступ агрессору. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
8. Если вы свидетель кибербуллинга. Ваши действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь.

### **Мобильный телефон**

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для персональных компьютеров, 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.

### **Основные советы для безопасности мобильного телефона:**

1. Будьте осторожны, ведь когда вам предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
2. Думайте, прежде чем отправить SMS, фото или видео. Вы точно знаете, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему вашего смартфона;
4. Используйте антивирусные программы для мобильных телефонов;
5. Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
6. После того как вы выйдете с сайта, где вводили личную информацию, зайдите в настройки браузера и удалите cookies;
7. Периодически проверяйте, какие платные услуги активированы на вашем номере мобильного телефона;
8. Давайте свой номер мобильного телефона только людям, которых вы знаете и кому доверяете;
9. Bluetooth должен быть выключен, когда вы им не пользуетесь. Не забывайте иногда проверять это.

## **Фишинг или кража личных данных**

Главная цель фишинга - вида Интернет-мошенничества, состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

### **Основные советы по борьбе с фишингом:**

1. Следите за своим аккаунтом. Если вы подозреваете, что ваша анкета была взломана, необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используйте безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используйте сложные и разные пароли. Таким образом, если злоумышленники взломают ваш аккаунт, то получат доступ только к одному вашему профилю в сети, а не ко всем;
4. Если вас «взломали», необходимо предупредить об этом всех знакомых, которые добавлены у вас в друзьях, так как, возможно, им от вашего имени будет рассыпаться спам и ссылки на фишинговые сайты;
5. Установите надежный пароль (PIN) на мобильный телефон;
6. Отключите сохранение пароля в браузере;
7. Не открывайте файлы и другие вложения в письмах даже если они пришли от ваших друзей. Лучше уточните, отправляли ли вам эти файлы.