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 (цифровые заплатки, 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. Ограничте 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, отправлял 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. Ограничте 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, присылаемый 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 оскорбления, 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 оскорблениями на оскорбления, 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. Ограничте 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 удали cookies;

7. Периодически проверяйте, какие платные услуги активированы на вашем номере мобильного телефона;

8. Давайте свой номер мобильного телефона только людям, которых вы знаеште 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 рассылаться 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.

Вх. № 64 от 11.02.2020

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

31.01.2020 № 1312-06/54

На

Об оказании содействия

Генеральному директору
ООО УК «Бульвар»

А.С. Филимонову

ул. Тимирязева, д 95, этаж техническое подполье помещение 33,
г. Новосибирск, 630082

office@bulvar-uk/ru

Уважаемый Александр Сергеевич!

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в соответствии с частью 1 статьи 23 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон) и пунктом 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16.03.2009 № 228 (далее – Положение), является Уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных.

Анализ сегодняшнего состояния защиты персональных данных граждан в Российской Федерации показывает, что помимо системных нарушений требований законодательства Российской Федерации в области персональных данных, носящих повторяющийся характер, появились новые вызовы и угрозы, возникшие вследствие интенсивного развития и внедрения в повседневную жизнь информационных технологий, появления новых форматов взаимоотношений между операторами и субъектами персональных данных, а равно фактов обработки наиболее чувствительной информации различных групп граждан, в том числе несовершеннолетних и лиц пожилого возраста.

В целях взаимодействия с гражданами и операторами, осуществляющими обработку персональных данных, и их профессиональными объединениями Роскомнадзором сформулирована Стратегия институционального развития и информационно-публичной деятельности в области защиты прав субъектов персональных данных на период до 2020 года (далее – Стратегия). Одной из приоритетных целей реализации Стратегии, является создание условий для развития системы поведенческих практик, направленных на соблюдение требований законодательства Российской Федерации в области персональных данных, в том числе посредством внедрения механизмов саморегулирования.

Согласно пункту 4 Положения Роскомнадзор осуществляет свою деятельность непосредственно и через свои территориальные органы.

Для достижения указанной цели территориальные органы Роскомнадзора решают следующие задачи:

- повышение уровня правовой информированности граждан и операторов, осуществляющих обработку персональных данных.

- формирование правовой модели поведения операторов, направленной на соблюдение требований законодательства Российской Федерации в области персональных данных;

- минимизация числа нарушений прав и законных интересов несовершеннолетних лиц при обработке их персональных данных;

- пресечение нарушения прав и законных интересов граждан, недопущение распространения негативного общественного резонанса.

- взаимодействие с операторами обработки персональных данных в целях защиты прав субъектов персональных данных;

- доведение информации до субъектов персональных данных об их правах и обязанностях в сфере персональных данных.

Управление Роскомнадзора по Сибирскому федеральному округу (далее – Управление) на основании пункта 2 Положения об Управлении Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Сибирскому федеральному округу, утвержденного приказом Роскомнадзора от 25.01.2016 № 45, является территориальным органом Роскомнадзора.

Решая поставленные задачи, Управление проводит обширную профилактическую работу с населением: встречи, семинары, проведение Дней открытых дверей и др. с целью разъяснения основных положений законодательства о персональных данных и правил бережного отношения к своим и чужим персональным данным.

В то же время, учитывая количество населения Новосибирской области, вышеуказанные профилактические меры в настоящее время являются недостаточными.

С учетом направлений деятельности управляющих компаний просим оказать содействие Управлению в исполнении вышеуказанного полномочия путем размещения информации о правилах поведения в сети «Интернет» в офисе и на интернет-сайте ООО УК «Бульвар».

О результатах рассмотрения настоящего письма просим сообщить в Управление на адрес электронной почты rsockanc54@rkn.gov.ru до 17 февраля 2020г.

Приложение: Файл «Информационная памятка.doc».

Заместитель руководителя — Визуализация ЭП — Р. А. Марущак

Документ подписан электронной подписью в системе электронного документооборота Роскомнадзора

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат	1d5ae4825a02bf00000000329920003
Владелец	Марущак Роман Анатольевич
Действителен	с 09.12.2019 по 09.12.2020

Исполнитель: Коваленко Л. Г.
Тел.: (383) 3495579 доб. 564