**ПАМЯТКА:**
**Информационная безопасность в сети Интернет**

Информационно-телекоммуникационная сеть «Интернет» все теснее проникает в нашу с вами жизнь. Для одних он стал источником знаний, для других используется в работе, кто-то нашел с помощью Интернета друзей, а кто-то даже смог наладить свою личную жизнь. Большинству из нас достаточно сложно представить день без онлайн-общения с друзьями, просмотра свежих новостей или новых роликов.

Развитие в Российской Федерации, как и во всем мире, электронных технологий и телекоммуникационных сетей, всеобщая доступность в глобальной компьютерной сети Интернет различных информационных ресурсов способствовало появлению принципиально нового вида нарушения Закона – киберпреступности.

Киберпреступность – незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей.

Практика последних лет свидетельствует об увеличении числа таких преступлений.

Ответственность за совершение компьютерных преступлений предусмотрена главой 28 Уголовного кодекса РФ, именуемой «Преступления в сфере компьютерной информации». Данная глава содержит три состава преступлений — ст. 272 (неправомерный доступ к компьютерной информации), ст. 273 (создание, использование и распространение вредоносных компьютерных программ), ст. 274 (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей).

Неправильное поведение в интернете может принести вред не только Вам, но также Вашим родным и близким.

**Что такое персональные данные и почему они так важны?**

Согласно Федеральному закону № 152-ФЗ «О персональных данных»:
***Персональные данные*** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Т.е. персональные данные – это информация о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность. Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.
Персональные данные не стоит путать с личными данными. Личные данные – это вообще совокупность всех данных о пользователе в Сети. Например, данные о геолокации, статистика по наиболее посещаемым интернет-страницам, фотографии и т.д.
**Кому нужны ваши персональные данные?**
80% преступников берут информацию в соцсетях.
Личная информация используется для кражи паролей.
Личная информация используется для совершения таких преступлений, как шантаж, вымогательство, оскорбление, клевета, киднеппинг, хищение.
Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.
Обработка персональных данных допускается:
- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом и др.

**Как защитить свои персональные данные?**
В абсолютном большинстве случаев мы сами указываем свои персональные данные при регистрации на сайтах, оформлении заказов в интернет-магазинах, заполнении профиля в социальных сетях или даже при составлении поискового запроса.
Обратите внимание, продолжая регистрацию на любом сайте, вы соглашаетесь с пользовательским соглашением, ставя «галочку» при заполнении его полей. Обычно этого достаточно, чтобы разрешить владельцам сайта использовать введенные вами данные при работе с его сервисами.
Таким образом, пользуясь сайтом или услугой, вы соглашаетесь на передачу и хранение ваших данных, будь то дата рождения, номер мобильного телефона, переписка и любые другие данные личного характера. Взамен их обязуются хранить в конфиденциальности и ни в коем случае не разглашать третьим лицам. Однако на деле это не всегда так – далеко

не всегда сторона, ответственная за хранение ваших персональных данных, добросовестно выполняет свои обязанности. Кроме того, никто не защищен от взлома баз данных, содержащих персональную информацию, или простых ошибок и человеческой опрометчивости. Например, регистрируясь или авторизуясь на сайте через социальную сеть, вы разрешаете сайту получить ваши личные данные, и точно неизвестно, как он будет ими пользоваться.

**Следование нескольким простым советам во многом сократит угрозу незаконного использования ваших персональных данных:**

- ограничьте объем информации о себе, находящейся в Интернете;
- удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию;
- не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.

При необходимости размещения объявления в Интернете воспользуйтесь временной сим-картой и выдуманным именем. Можно также воспользоваться услугой «Второй номер», которую предоставляют некоторые операторы мобильной связи. Эта услуга позволяет подключить в «Личном кабинете» второй номер только на прием звонков и СМС. Звонить с него не получится.

Используйте только сложные пароли, разные для разных учетных записей и сервисов. Повторное использование паролей категорически запрещено.

Регулярно меняйте пароли, желательно не реже раза в месяц.

По возможности используйте двухфакторную авторизацию – это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый рубеж – это логин и пароль, второй – специальный код, приходящий по СМС или электронной почте.

Заведите себе два адреса электронной почты – частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках) и публичный – для открытой деятельности (форумов, чатов и так далее).

**Что делать, если вы стали жертвой нарушения в области персональных данных?**

В первую очередь вам необходимо обратиться в уполномоченный орган в сфере персональных данных – Роскомнадзор, а точнее, его территориальное Управление.

В целях объективного и полного рассмотрения вам необходимо указать следующую информацию:

1) перечень персональных данных, неправомерно обрабатываемых на сайтах в сети Интернет;

2) сведения о документе, удостоверяющем вашу личность (копии страниц паспорта), для подтверждения принадлежности персональных данных, неправомерно размещенных на сайтах в сети Интернет, к вам как к субъекту персональных данных;

3) точные и доступные адреса страниц сайтов (указатели страниц сайтов в сети Интернет – URL), содержащие незаконно обрабатываемые (размещённые) персональные данные,

позволяющие осуществить просмотр данных страниц Управлением, а также снимки экрана с данными страницами, содержащие в себе полный адрес страницы сайта (URL) и даты публикации постов/сообщений, содержащих незаконно обрабатываемые (размещённые) персональные данные на текущий момент времени (дата) и другие сведения, подтверждающие нарушения требований законодательства в области персональных данных (видеозапись экрана с действиями, позволяющими зафиксировать нарушения и т.п.);

4) сведения, уполномочивающие вас представлять интересы физических лиц (копии доверенностей), персональные данные которых размещены на сайтах (в случае нарушения их прав как субъектов персональных данных).

**Дополнительно следует представить (при наличии):**

- сведения, подтверждающие факт направления вами в адрес администрации сайта (далее – оператор) требования об уничтожении ваших персональных данных с указанием на их незаконное получение (без согласия) оператором или с указанием того, что они не являются необходимыми для заявленной цели обработки (представляется при возможности направления указанного требования);
- ответ оператора на ваше требование об уничтожении ваших персональных данных (при наличии).

***Обращаем внимание на то, что все имеющиеся сведения должны быть представлены в адрес Управления единовременно!***

В случае если по результатам проверки Управление Роскомнадзора выявило нарушение, выдается предписание об его устранении.

Если Управление Роскомнадзора не увидело нарушения, вы можете обратиться в центральный аппарат данного ведомства.

Помимо этого, все субъекты персональных данных имеют право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Ответственность за нарушение законодательства о персональных данных предусматривается в соответствии со ст. 13.11 Кодекса об административных правонарушениях РФ.