Интернет безопасность

Нельзя отрицать того факта, что информационно-телекоммуникационная сеть «Интернет» все теснее проникает в нашу с вами жизнь.

Для одних Всемирная сеть стала источником знаний, для других работой, 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.

Киберпреступность

Наиболее распространенными преступлениями в сфере компьютерной информации являются блокирование сайтов и локальных компьютерных сетей, незаконное копирование информации.

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).

Персональные данные

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 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.

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.

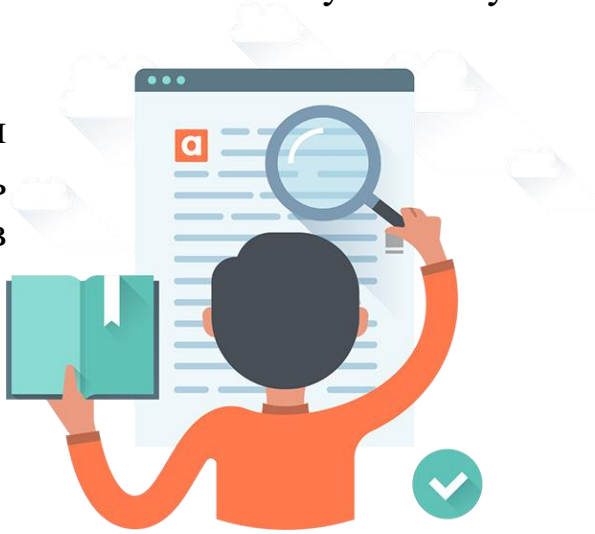
Обратите внимание, продолжая регистрацию на любом сайте, вы соглашаетесь с пользовательским соглашением, ставя «галочку» при заполнении его полей. Обычно этого достаточно, чтобы разрешить владельцам сайта использовать введенные вами данные при работе с его сервисами.

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. Точно так же любой ваш звонок в магазин или салон автоматически вносит ваш номер в базу пользователей этой компании.

Как защититься?

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.

Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат – действительно тот, за кого себя выдает.

Используйте только сложные пароли, разные для разных учетных записей и сервисов. Пользователи, которые используют один и тот же пароль для всех сервисов, при компрометации хотя бы одного из сервисов могут потерять доступ ко всем своим учетным записям. Повторное использование паролей категорически запрещено.

Регулярно меняйте пароли, желательно не реже раза в месяц.

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).

Если Вы уже стали жертвой…

Необходимо обратиться в уполномоченный орган в сфере персональных данных – Роскомнадзор, а точнее, его территориальное Управление.

Мошенничество

Телефонное мошенничество

- Обман по телефону.
- СМС-просьба о помощи.
- Выигрыш в лотерее
- Штрафные санкции
- Ошибочный перевод средств.

Мошенничество в социальных сетях

- Распространение ссылок на вредоносное программное обеспечение
- Знакомые незнакомцы.
- Просьбы о финансовой помощи, благотворительные акции.

Мошенничество на сайтах бесплатных объявлений

- Оплата или предоплата за ваш товар
- Предоплата за покупаемый товар.
- СМС-сообщения со ссылкой.

Мошенничество с банковскими картами

- СМС-сообщение о блокировке банковской карты
- Телефонный звонок «работника банка»

Безопасность в сети

- Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Используйте и обновляйте антивирусные программы и брандмауэр.
- Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://».
- В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически».
- Не допускайте автоматического подключения устройства к сетям Wi-Fi без Вашего согласия.
- Ограничьте список друзей в социальных сетях. У Вас в друзьях не должно быть случайных и незнакомых людей.
- Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату твоего рождения и другую личную информацию.
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли.
- Следите за своим аккаунтом. Если Вы подозреваете, что Ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом.
- Если Вас взломали, то необходимо предупредить всех своих знакомых, которые есть у Вас в друзьях, о том, что Вас взломали и, возможно, от Вашего имени будет рассылаться спам и ссылки на фишинговые сайты.
- Не открывайте файлы и другие вложения в письмах даже если они пришли от Ваших друзей. Лучше уточните у них, отправляли ли они Вам эти файлы.