

# Осторожно - мошенники!

## Как не стать жертвой киберпреступника



**Помните! Никому нельзя сообщать: номер, срок действия, коды подтверждения на обороте карты, коды из СМС-сообщений, логины и пароли.**

## ПЕРСОНАЛЬНЫЕ ДАННЫЕ

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).*

### **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.

### **Обработка персональных данных допускается в следующих случаях:**

- 1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- 2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- 3) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- 4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- 5) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно-значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

### **Как защитить свои персональные данные?**

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.

### **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.

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

При необходимости размещения объявления в Интернете воспользуйтесь временной сим-картой и вымышленным 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. 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.

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.