

## ПРАВИЛА БЕЗОПАСНОСТИ. КИБЕРМОШЕННИЧЕСТВО



**Кибермошенничество** — один из видов киберпреступления, целью которого является обман пользователей: хакер незаконно получает доступ к личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб. Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

### Предупреждение кибермошенничества

1. Ни под каким предлогом не выдавай незнакомым людям свои личные данные (домашний адрес, номер телефона и т.д.) и пароли.
2. Перед тем, как воспользоваться развлекательными услугами Интернета (скачать музыку, фильм и т.д.), проверь, что после этого тебя не попросят заплатить деньги.
3. Не верь всему, что видишь в Интернет.
4. Старайся остерегаться новых предложений и услуг, все они требуют вложения крупной суммы денег (например, местонахождение человека по номеру его мобильного, повышение рейтинга в социальной сети и т.д.)
5. Советуйся со взрослыми перед тем, как загрузить, скачать или установить ту или иную услугу.
6. Очень внимательно выбирай сайты, на которых ты хочешь сделать покупки и удостоверься в их надежности. Собери как можно больше информации о сайте, спросив, например, название, адрес и номер телефона центрального офиса, описания общих положений контракта и, особенно о том, как отменить заказ; кроме того выясни о защите и управлении личными данными и безопасности оплаты; и сравни цены, отыскав такой же предмет на других сайтах.
7. Если ты получил неожиданное электронное письмо, в котором тебе предлагается невероятно выгодная сделка, вероятность того, что это мошенничество, очень велика.

### Борьба с кибермошенничеством

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

## **Предупреждение кибербуллинга**

1. Не сообщай свои данные агрессору (реальное имя, фамилию, адрес, телефон, номер школы и т.п.). Когда злоумышленнику становятся известны твои анкетные данные, происходит так называемый «троллинг» или травля.
2. Не открывай доступ к своей страничке незнакомым людям.
3. Следи за информацией, которую ты выкладываешь в Интернете
4. Придерживайся правил сетевой этики, не отвечай грубо на сообщения, этим ты можешь спровоцировать собеседника. Игнорируй сообщения от незнакомых, агрессивных и подозрительных личностей. Нужно понимать, что онлайн-общение не является приватным. Другие пользователи могут скопировать, распечатать или переслать твою личную переписку.
5. Если ты видишь или знаешь, что твоего друга запугивают, поддержи его и сообщи об этом.
6. Не посылай сообщения или изображения, которые могут огорчить кого-нибудь.

***Грумминг** — установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече.*

## **Предупреждение груминга**

1. Следи за информацией, которую ты выкладываешь в Интернете. Не выкладывай свои личные данные в Интернете (домашний адрес, номер телефона, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.). Помни, любая информация может быть использована против тебя, в том числе в корыстных и преступных целях
2. Используй псевдоним при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании он-лайн играми и других ситуациях
3. Не размещай и не посылай свои фотографии незнакомцам
4. Будь осторожен при общении с незнакомыми людьми. Старайся рассказывать как можно меньше информации о себе.

## **Борьба с грумингом**

1. Если новый знакомый пытается говорить с тобой на неприятные или пугающие тебя темы и говорит об этом как о секрете, который останется только между вами – немедленно сообщи об этом родителям или старшим
2. Сделай снимок с экрана (screen-shot)
3. Никогда не соглашайся на личные встречи с незнакомцами. Твои собеседники могут оказаться совсем не теми, за кого себя выдают. Или приходи на встречу только со взрослым