## Полезные советы:

- ✓ Защищайте свою информацию. Нужно предпринять меры, чтобы избежать распространения своих конфиденциальных сведений;
- ✓ Добавляйте данные в социальные сети с осторожностью. Чтобы уберечь себя и близких от мошенников, не выкладывайте фотографии с отпусков, не указывайте места работы, номера телефонов и прочие личные данные;
- ✓ Относитесь осторожно к платежным системам;
- ✓ Позаботьтесь о том, чтобы ваши данные в электронном виде хранились в безопасности;
- ✓ Спрашивайте документы, прежде чем пустить в квартиру медицинских работников, полицейских и прочих представителей госструктур. Особенно касается случаев, когда к вам пришли без приглашения;
- ✓ Избегайте азартных игр и предсказаний будущего;
- ✓ Относитесь внимательно к звонкам от посторонних людей;
- ✓ Не доверяйте незнакомым.


Составитель: библиотекарь отдела
информационных технологии
Э.Ф. Вильданова

Оформление: гл. библиотекарь
Отдела методической и инновационной работы
Т.В. Мосунова

Library_pyti-yah-muzej@mail.ru
www.pytyahlib.ru

Муниципальное автономное учреждение культуры
«Культурный центр: библиотека-музей»
**Центральная городская библиотека**
***Отдел информационных технологий***

# «Правовые проблемы интернет – пространства»

***буклет***

Пыть-Ях
2019 г.

12+

## Основными проблемами в сети Интернет, нуждающимися в скорейшем нормативно-правовом урегулировании, являются:

- Распространение экстремистских материалов;
- Проблемы, связанные с защитой прав интеллектуальной собственности;
- Проблемы правового регулирования исключительных прав на сетевой адрес (доменное имя);
- Защита персональных данных;
- Правовое регулирование электронной торговли;
- Пропаганда, незаконная реклама наркотических средств и психотропных веществ;
- Незаконное распространение порнографических материалов;
- Клевета;
- Мошенничество.

## Мошенничество в сети Интернет

Мошенничество в соответствии со ст. 159 Уголовного кодекса РФ - «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием». На данный момент существует огромное количество различных видов мошенничества в сети Интернет, следует учитывать и то, что с течением времени появляются все новые виды мошенничества.

В интернете мошенничество происходит чаще всего под такими предлогами:

- Заработок;
- Помощь страждущим;
- Разблокировки опций программ, приложений;
- Выгодное приобретение товаров;
- Розыгрыш ценных призов.

## Как бороться со спамом и сетевыми мошенниками:

**1.** Проверяйте отправителя. Отправителем спама зачастую является неизвестное вам лицо со странным адресом электронной почты. Но это не значит, что со всех странных адресов отправляется исключительно спам. С незнакомых вам адресов могут отправляться информационные бюллетени или письма от администрации сайтов (например, для сброса пароля);

**2.** Обратите внимание на ссылки. Щелкайте по ссылкам в письмах от надежных отправителей. Если вы не знаете отправителя письма и оно включает ссылку, то это, скорее всего, спам. Наведите курсор на ссылку, чтобы посмотреть ее адрес;

**3.** Обратите внимание на орфографию. Зачастую в спаме есть орфографические и стилистические ошибки, включая множество слов прописными буквами и странную пунктуацию. В конце сообщения может появиться бессвязный текст;

**4.** Прочитайте сообщение. Спам - это любое сообщение, извещающее вас о победе в конкурсе, в котором вы не участвовали, или о том, что вы можете получить определенную сумму денег, или о бесплатной раздаче электроники. Любое сообщение, в котором вас просят указать пароль - это спам. Сразу удаляйте письма от незнакомых вам людей. Многие почтовые сервисы имеют окно предварительного просмотра, в котором вы можете прочитать письмо, не открывая его;

**5.** Обратите внимание на вложения. Вредоносные программы и вирусы зачастую маскируются под вложения к электронным письмам. Никогда не скачивайте вложения к письмам от неизвестных отправителей;

**6.** Не сообщайте ваш адрес электронной почты в сети. Специальные программы-боты могут быстро скопировать тысячи адресов электронной почты с тех сайтов, где адреса являются публичной информацией. Иногда люди копируют адреса с веб-сайтов и используют их для регистрации на различных ресурсах, на которых предлагается что-то бесплатное;

**7.** Никогда не отвечайте на спам. Ответив или нажав «Отписаться», вы будете получать больше спама, потому что спамер поймет, что это действующий почтовый ящик. Лучше всего удалить спам и сообщить о нем.

## Выделим те из них, которым наиболее часто подвергаются пользователи Сети:

- **Интернет-попрошайничество** - один из наиболее известных видов мошенничества в Сети, которое выражается в просьбе пожертвовать некоторую сумму денежных средств под различными предлогами, например, от имени благотворительных фондов;
- Мошенничества, связанные с **интернет-магазин**ами. В качестве примера по данному виду мошенничества можно рассмотреть следующую ситуацию: покупатель оплачивает товар, а затем либо не получает его, либо получает, но в меньшем количестве или худшего качества;
- **Сайты-подделки** - внешне не отличаются от оригинальных сайтов. Однако сайты-подделки популярных социальных сетей создаются с целью выманивания денежных средств или взлома аккаунтов, с последующей рассылкой писем, содержащих ссылки на вредоносные программы - спама;
- **Программы-блокеры** - созданы для проникновения в систему и блокирования доступа к ней. Для разблокировки системы пользователю требуется, как пример, отправить платное sms-сообщение;
- **Фишинг** является также одним из наиболее распространенных видов мошенничества, его целью является получение доступа к конфиденциальным данным пользователей. Осуществляется данный вид интернет-мошенничества путем проведения массовых рассылок электронных писем от известных пользователю представителей. Например, **отправление личного сообщения на электронный адрес пользователя от имени банка.**