1. Не пересылайте личную информацию (номер банковской карты, ПИН-код, данные паспорта, ИНН, СНИЛС) через мессенджеры социальных сетей. Письма со сканами документов лучше удалять сразу после отправки или получения, не нужно хранить их в почтовом ящике, тем более в «облачном» хранилище Интернета.
2. Если заходите на свою страничку в социальных сетях, почтовый ящик с чужого компьютера, телефона, не забывайте удалять свой логин и пароль.
3. Не доверяйте непроверенным Wi-Fi-соединениям которые не запрашивают пароль. Чаще всего именно такие сети злоумышленники используют для воровства личных данных пользователей.
4. Помните: банки, сервисы, и магазины никогда не рассылают письма с просьбой перейти по ссылке, изменить свой пароль, ввести номер банковской карты и секретный код подтверждения или сообщить другие личные данные!
5. Установите и обновляйте антивирусные программы. Устаревшие версии не могут гарантировать защиту от вредоносного программного обеспечения. Ежедневно в мире появляется несколько новых вирусов. И антивирусу нужно как можно чаще получать информацию о методах борьбы с ним.
6. Кликать по ссылкам, пришедшим в сообщениях от незнакомых людей, верный способ попасться на удочку кибермошенников и заразить свое устройство вирусами. Опасная ссылка может прийти и от взломанного компьютера знакомого, поэтому лучше уточните, что такое он вам прислал и нужно ли это открывать.
7. Не запускайте неизвестные файлы. Особенно с расширением **.exe.**
8. Внимательно проверяйте адреса ссылок, логотипы, текст и отправителя сообщений.
9. Никогда не отвечайте на спам.
10. Если вам в мессенджере пришла от знакомого просьба срочно выслать деньги, ничего не отправляйте! Сначала перезвоните ему и удостоверьтесь, что аккаунт не был взломан злоумышленниками.
11. Прочитайте книгу Кевина Митника «Искусство обмана». Вы узнаете, как киберпреступники втираются в доверие к людям, манипулируя их чувствами.
12. Не делитесь личной информацией в соцсетях: не афишируйте уровень достатка, домашний адрес. Не описывайте свой маршрут, не пишите, когда вас не бывает дома.
13. Сообщайте своим родителям о найденной нежелательной информации. Не вся информация в сети достоверна.
14. Не скачивайте сомнительные приложения и не пытайтесь это делать по неизвестным ссылкам. Пользуйтесь только официальными магазинами **App Stope, Google Play, Windows Market.**
15. Постарайтесь ничего не покупать в социальных сетях. Особенно с предоплатой. Не рекомендуется переводить деньги на карту физических лиц (то есть, когда кто-то просто дает вам номер или реквизиты своей карты).
16. Не делайте репостов жалостливых объявлений про милого котика, который срочно ищет дом (а в посте – телефон владельца или номер карты, куда можно перечислить деньги на содержание животного). Велика вероятность, что это мошенники, решившие заработать на сердобольных и доверчивых гражданах.
17. Если на смартфоне появилась надпись «Вставьте сим-карту», срочно зайдите в ближайший офис вашего мобильного оператора или позвоните ему с другого телефона и выясните, в чем проблема. Возможно, кто-то получил дубликат вашей сим-карты и ее нужно срочно заблокировать.
18. Мошенники создают сайты, на которых вы якобы можете бесплатно посмотреть или скачать приглянувшийся фильм, но сначала надо оставить номер своего телефона или отправить сообщение на короткий номер. Таким образом с вашего счета могут списать внушительную сумму за SMS, а ваш номер телефона попасть в базу спамеров.
19. Не участвуйте в акциях с призами, где нужно что-то оплатить, а потом попросить сделать то же самое нескольких людей. Это пирамида!
20. Ни в коем случае не отправляйте SMS, чтобы получить информацию из Интернета. Иногда на экране компьютера всплывает окошко (очень яркое, мигающее) примерно с таким содержанием: «Только сегодня у тебя уникальный шанс! Участвуй и выигрывай!» Если навести на окошко курсор и щелкнуть левой кнопкой мыши, появится сообщение «Чтобы принять участие в розыгрыше, тебе необходимо прислать SMS!». Вполне возможно, что вы имеете дело с мошенниками, и одно отправленное вами SMS может очень дорого вам обойтись.
21. Не всегда бывает так, что «друзья» в Интернете нам знакомы в реальной жизни. И если вдруг ваш новый «интернет-друг» предложит вам встретиться, обязательно сообщайте об этом родителям, посоветуйтесь с ними. В Интернете человек может представляться совсем не тем, кем является на самом деле, и в реальной жизни 12-летняя девочка может оказаться 40-летним дядечкой, который хочет причинить вам вред.
22. Спрашивайте у родителей, какие странице в Сети вам следует посещать. Родители вас любят, о вас заботятся и никогда не посоветуют вам плохого.

Пользуясь Интернетом, не забывайте, что он – не главное увлечение жизни. Кроме него, есть еще любимые книги, занятия спортом, прогулки на свежем воздухе, общение с друзьями в реальной жизни и многое другое.

**Комиссия по делам несовершеннолетних**

**и защите их прав**

**Пролетарского района городского округа Саранск**

**Правила пользования детей Интернетом**



**Саранск – 2021**