

Обращать внимание на сайты

Один из приемов, который часто используют мошенники – фишинг. Они создают поддельный сайт, который очень похож на тот, которым все часто пользуются. Он может имитировать почтовый сервис, социальную сеть или игру. Но введя туда свои конфиденциальные данные, можно стать жертвой интернет-мошенников. Поэтому важно быть внимательным и обращать внимание на детали, в частности, на адрес сайта: он может отличаться от правильного всего на одну-две буквы, например, для «ВКонтакте» – vc.com или vk-com.com вместо правильного vk.com.



**Центральная библиотека,
ул. Ленина, дом 18.**

ТЕЛЕФОН: (87935) 3-10-06,

E-mail: cblerm@yandex.ru

Сайт: <http://lerm-cbs.ru/>



centrlib26ru

Часы работы:

11-00 – 18-00

Воскресенье:

11-00 – 17-00

Выходной:

Суббота

Безопасность в сети : информационный
буклет / Муниципальное казённое
учреждение города Лермонтова
«Централизованная библиотечная система» :
Центральная библиотека; составитель
Чуркина А.А. – город Лермонтов, 2024

Муниципальное казённое учреждение
города Лермонтова
«Централизованная библиотечная система»
Центральная библиотека
16+

Безопасность в сети



г. Лермонтов 2024

Интернет - это виртуальный мир, но здесь также действуют свои правила, схожие с реальной жизнью. В наше время важно соблюдать меры безопасности в сети. Что нужно соблюдать, чтобы обезопасить себя в Интернете?

Советоваться с родителями

Если подросток хочет зарегистрироваться на каком-либо сайте, создать профиль в социальной сети и выложить свои фотографии, лучше перед этим посоветоваться с родителями. Взрослый человек сможет лучше проанализировать ситуацию и понять, опасен ли сайт, а также помочь выбрать снимки, которые можно выложить на всеобщее обозрение.



Беречь личные данные

Если ребенок думает, что хорошо знает человека, с которым общается онлайн, не нужно рассказывать подробности о себе и о родителях. Номер телефона, адрес, номер школы и класса, место работы родителей и их график, время, когда в квартире нет взрослых, а также данные из документов, номера банковских карт - такую информацию ни в коем случае нельзя передавать другим людям.

Не делиться информацией о знакомых

Не нужно рассказывать про друзей и одноклассников, сообщать, где они живут и учатся, какие кружки посещают. Нельзя показывать их фотографии – ни выкладывать их в своих профилях в социальных сетях, ни тем более в частной переписке.



Фильтровать информацию

Мошенники активно используют интернет в своих интересах. Они могут обманывать людей и манипулировать ими, давая на жалость или страх. Поэтому не стоит слепо доверять всему, что пишут в онлайн.

- не открывать подозрительные письма;
- игнорировать сообщения, полученные от незнакомцев;
- не переходить по ссылкам, обещающим много интересного бесплатно.

Не общаться с чужими людьми

Это правило очень сложно соблюдать в интернете. Одно дело - говорить с тем, кто уже месяц или полгода играет в ту же онлайн-игру, и совсем другое - отвечать на первое же письмо того, кто назойливо стучится в личные сообщения. Любая назойливость, частые обращения, просьбы что-то написать и тем более прислать фото - это весомый повод для того, чтобы сразу же прекратить общение и заблокировать человека.

Придумывать сложные пароли

Простой пароль не только легко запомнить, но и очень просто взломать. Поэтому при его составлении лучше:

- придумывать сложные комбинации, состоящие из заглавных и строчных букв, цифр и символов;
- использовать разные пароли для разных сайтов – иначе тот, кто взламывает один профиль, легко получит доступ ко всем прочим.

