Как защитить себя и своего ребенка в интернете?

Памятка для родителей и учителей

Смотрите на ссылки, по которым переходите.
Отличие всего в одну букву заметить не так
просто, но эта невнимательность может
стоить вам дорого.

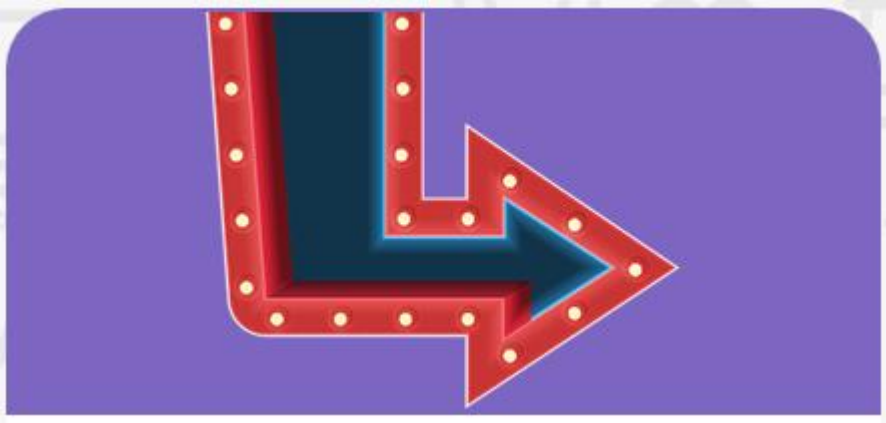
Не доверяйте письмам о крупном наследстве
или внезапной блокировке банковского счета.
Всегда перепроверяйте информацию.

Помните, что комиссии для организаторов за получение
крупных выигрышей и призов, пусть и
небольшие, — это явный признак мошенничества.
Критически оценивайте любые заманчивые предложения.

Не переходите по подозрительным ссылкам в почте,
социальных сетях и мессенджерах, даже если их
прислали ваши знакомые. Установите **защитное решение**
с технологиями противодействия спаму и фишингу.

Если у вас есть маленький ребенок, который начинает
познавать цифровой мир, установите на его и на свое
устройство специальное **решение для детской онлайн-безопасности.**

Не совершайте покупки на сомнительных сайтах,
а чтобы проверить информацию о портале, изучите
отзывы о нем или воспользуйтесь Whois сервисами,
которые позволяют узнать дату регистрации
и возраст домена, а также контакты, по которым
можно связаться с организацией, которой он принадлежит.



Не скачивайте книги и фильмы с подозрительных ресурсов.
Больше всего шансов подцепить вирус именно там.

Расскажите ребенку о том, что такое кибербуллинг
и как действовать в неприятной ситуации: не отвечать
на травлю, добавить обидчиков в «черный список»,
сообщить о травле администраторам того ресурса,
где она происходила, рассказать о буллинге родителям.

Используйте сложные пароли (от 8 знаков,
с буквами в разном регистре, цифрами и спецсимволами),
установите разные комбинации для каждой учетной
записи. Для надежного хранения паролей
используйте **специальные решения.**

Старайтесь поменьше делиться в социальных сетях
подробностями своей личной жизни и информацией
о детях. Не стоит также без необходимости
добавлять геометки к фотографиям.

Своевременно обновляйте все программы и приложения.

С осторожностью используйте публичные Wi-Fi-сети:
старайтесь не совершать через них онлайн платежи
и не вводить пароли для входа в личные аккаунты.

Не спешите голосовать за друга в конкурсе или
переводить ему денег на карту. Для начала убедитесь,
что это действительно он: позвоните
или задайте уточняющий вопрос.

Установите защитное решение. **Kaspersky Total Security**
не только защитит от большинства киберугроз,
но и поможет создать и надежно хранить пароли,
а также оградит от неприятностей в сети вашего
ребенка благодаря встроенному модулю
родительского контроля **Kaspersky Safe Kids.**

При поддержке **Kaspersky**