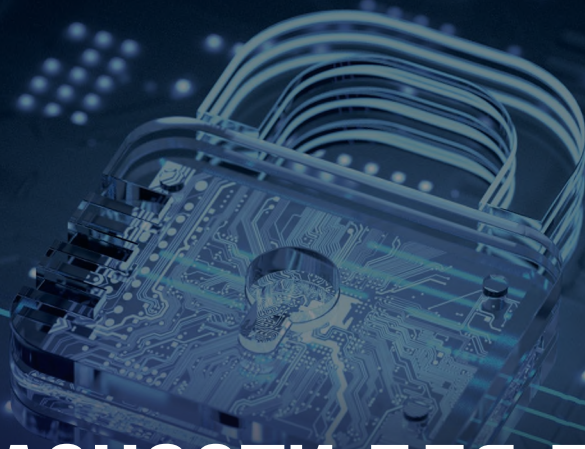




ПРАВИТЕЛЬСТВО
МОСКОВСКОЙ
ОБЛАСТИ

ГЛАВНОЕ УПРАВЛЕНИЕ
РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ
МОСКОВСКОЙ ОБЛАСТИ



ПРАВИЛА БЕЗОПАСНОСТИ ДЛЯ ДЕТЕЙ В ИНТЕРНЕТЕ

**ТЕХНОЛОГИИ ИГРАЮТ ВАЖНУЮ РОЛЬ
В ЖИЗНИ. ДЕТСТВО — ИДЕАЛЬНАЯ
ПОРА РАЗВИТЬ НАВЫКИ,
НЕОБХОДИМЫЕ ДЛЯ ОБЕСПЕЧЕНИЯ
БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ.**

ТРИ ОСНОВНЫЕ КАТЕГОРИИ УГРОЗ:

УГРОЗЫ ОТ НЕЗНАКОМЦЕВ

- ❗ Кэтфишинг: злоумышленники притворяются детьми в социальных сетях и на игровых сайтах с целью завоевать доверие ребенка и выведать личные данные
- ❗ Киберпреступники обманом выясняют у ребенка пароли или платежную информацию

УГРОЗЫ ОТ СВЕРСТНИКОВ

- ❗ Издевательства, травля со стороны знакомых в социальных сетях и мессенджерах: публикация личной информации, порочащей честь или морально травмирующей ребенка
- ❗ Публикация данных сексуального характера, например интимных фотографий, что по степени вреда классифицируется как уголовное преступление

УГРОЗЫ ИЗ-ЗА ЛИЧНОЙ НЕОСТОРОЖНОСТИ

- ❗ Дети часто публикуют личную информацию, переходят по ссылкам или устанавливают программное обеспечение, не понимая последствий своих действий

КАК ЗАЩИТИТЬ РЕБЕНКА:

- 🔒 Создайте доверительную и уважительную атмосферу в общении с детьми
- 🔒 Утвердите перечень сведений, которые можно сообщать в Интернете безопасно
- 🔒 Объясните, как проверить подлинность сайта и почему следует избегать опасных ссылок
- 🔒 Покажите, как создать надежный пароль с двухфакторной аутентификацией
- 🔒 Если что-то пошло не так, поддержите ребенка и покажите, как извлечь уроки на будущее

БАЗОВЫЕ ПРАВИЛА ДЛЯ МАЛЫШЕЙ:

- 🔒 Не выходите в Интернет без разрешения взрослых
- 🔒 Перед экраном устройства проводите не более 30 минут в день
- 🔒 Спрашивайте разрешение для установки/использования приложений

ДЕТЯМ ПОСТАРШЕ:

- 🔒 Если вы столкнулись в Интернете с чем-то, что заставляет вас чувствовать себя неловко, сообщите об этом родителям
- 🔒 Не передавайте никому личную информацию (контакты, данные близких)
- 🔒 Не публикуйте в Интернете свои фото, фото семейной машины и ценных вещей
- 🔒 общайтесь только с теми людьми, кого знаете вживую
- 🔒 Всегда спрашивайте разрешение у родителей, прежде чем совершить онлайн-платеж



ПРАВИТЕЛЬСТВО
МОСКОВСКОЙ
ОБЛАСТИ

ГЛАВНОЕ УПРАВЛЕНИЕ
РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ
МОСКОВСКОЙ ОБЛАСТИ

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКОВ

КИБЕРМОШЕННИЧЕСТВО – ОДИН ИЗ ВИДОВ КИБЕРПРЕСТУПЛЕНИЙ. ЦЕЛЬ ТАКОЙ АКТИВНОСТИ – ПРИЧИНЕНИЕ МАТЕРИАЛЬНОГО ИЛИ ИНОГО УЩЕРБА ПУТЕМ ХИЩЕНИЯ ЛИЧНОЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЯ (НОМЕРА БАНКОВСКИХ СЧЕТОВ, ПАСПОРТНЫЕ ДАННЫЕ, КОДЫ, ПАРОЛИ И ДР.)

ОСНОВНЫЕ КИБЕРУГРОЗЫ:

- ❖ Вирусы попадают на устройство при скачивании файлов и разрушают его
- ❖ Спам – зараженные письма с вложениями, которые поражают компьютер
- ❖ Фишинг – копирование дизайна и интерфейса известных сайтов
- ❖ Кибербуллинг – запугивание и травля детей и взрослых
- ❖ Удаленный взлом – злоумышленники получают доступ к данным
- ❖ Ddos-атаки, цель – вывести систему из строя

КАК ЗАЩИТИТЬСЯ:

- 🔒 При подозрительных звонках из банка и/или полиции сбросьте вызов и перезвоните самостоятельно по номеру, указанному на обороте вашей карты или на официальном сайте, не перезванивайте мошенникам
- 🔒 Не сообщайте никому конфиденциальные банковские данные (трехзначный код на обороте и одноразовые СМС и push-уведомления)
- 🔒 Подключите мобильный банк и СМС/push-уведомления для контроля операций
- 🔒 Не переходите по сомнительным баннерам и ссылкам, обещающим цены ниже, чем в официальных магазинах
- 🔒 Перед установкой приложений и программ читайте отзывы
- 🔒 Установите антивирус и меняйте пароли раз в месяц или чаще
- 🔒 Обращайте внимание на адрес сайта: защищенное соединение начинается с https
- 🔒 Осматривайте банкоматы на наличие посторонних предметов и закрывайте клавиатуру рукой, пока набираете код
- 🔒 Если деньги все же украли, незамедлительно звоните в банк и блокируйте карту, пишите заявление о несогласии с операцией – не позднее следующего дня
- 🔒 Перепроверяйте информацию
- 🔒 Не покупайте медицинские справки в интернете – справку о коронавирусе можно получить только в медицинском учреждении