Памятка для родителей

Финансовая безопасность детей в интернете

Финансовая безопасность детей в интернете - постоянный диалог и набор правил, которые помогут ребёнку безопасно распоряжаться деньгами и защищать личные данные.

Что важно объяснить ребёнку

-Не сообщайте личные данные. Объясните, что к ним относятся ФИО, дата рождения, адрес, номер телефона, данные банковской карты (номер, CVV-код), пароли и коды из СМС. Подчеркните: даже если собеседник представляется другом или «представителем банка», он всё равно может пытаться выманить эти сведения. Если в сети кто-то просит такие данные, пусть ответит: «Спрошу разрешения у родителей» — часто после этого мошенники исчезают.

- Не переходите по подозрительным ссылкам. Объясните, что ссылки в спам-сообщениях, письмах (особенно с обещаниями крупного выигрыша, бонусов или срочных призывов) часто ведут на фишинговые сайты или заражённые страницы, где можно потерять деньги или заразить устройство вирусом.

- Будьте осторожны с онлайн-покупками и подписками. Договоритесь, что перед любой покупкой или оформлением подписки ребёнок сначала обсуждает это с вами. Объясните, что бесплатный пробный период часто незаметно переходит в регулярные списания. Научите проверять надёжность магазина: смотрите на отзывы, наличие SSL-сертификата (замок в адресной строке), корректность интерфейса.

- Не участвуйте в сомнительных схемах заработка. Расскажите, что обещания «лёгких денег», «высокодоходных инвестиций» или «подработки» с требованием внести предоплату — частый признак мошенничества. Объясните, что порядочный работодатель не будет просить перевести деньги перед оформлением. Отдельно предупредите о дропперстве: передача своей карты или данных третьим лицам для якобы «легальных» операций — это серьёзное преступление, которое может привести к уголовному преследованию.

- Не доверяйте сообщениям о выигрыше с условием. Сообщение вроде «Вы выиграли приз! Переведите комиссию, чтобы получить выигрыш» — почти всегда обман.

- Перепроверяйте просьбы о помощи. Если друг в соцсети пишет, что попал в беду и просит денег, не спешите переводить. Скорее всего, аккаунт взломали. Попросите ребёнка сначала связаться с другом по телефону или видеосвязи, чтобы убедиться, что ему действительно нужны деньги.

- Не скачивайте программы с непроверенных сайтов. Объясните, что так можно заразить устройство вирусом, который украдёт данные карты или пароли.

- Не оставляйте геометки в открытом доступе. По таким меткам мошенники могут узнать, где ребёнок живёт, учится, какие места часто посещает.