Правила кибербезопасности дома

ИСПОЛЬЗУЙТЕ СЛОЖНЫЕ ПАРОЛИ	Самые популярные для взлома: «qwerty123», «qwerty», «123456», «a111» и «123456789», «ищукен», «пароль» и «любовь». Надежный пароль должен содержать минимум 8 символов, в идеале – 12. Среди них должны быть большие и маленькие буквы, цифры и спецсимволы
НЕ ОТКРЫВАЙТЕ ПОДОЗРИТЕЛЬНЫЕ СООБЩЕНИЯ, ПИСЬМА И ВЛОЖЕНИЯ	Не переходите по ссылкам, где требуют ввести личную информацию. Преступники присылают фишинговые письма, очень похожие на сообщения от банков, компаний, органов власти или Госуслуг. Ссылки ведут на поддельные сайты. Став жертвой фишинга, можно лишиться денег или доступа к своим аккаунтам
ЗАГРУЖАЙТЕ ПРИЛОЖЕНИЯ ТОЛЬКО ИЗ ОФИЦИАЛЬНЫХ МАГАЗИНОВ	Здесь есть строгий контроль, рейтинг, статистика по количеству скачиваний и отзывы пользователей. Если хотите установить приложения банков под санкциями, скачайте их с официальных сайтов организаций
УСТАНОВИТЕ И РЕГУЛЯРНО ОБНОВЛЯЙТЕ АНТИВИРУСНОЕ ПО	Антивирусы обнаружат вредоносную программу, если она уже оказалась на устройстве. Защитные системы блокируют переходы на зараженные сайты, проверяют ссылки в почте, СМС и мессенджерах, ищут небезопасные настройки
НЕ ПРИНИМАЙТЕ ПОСПЕШНЫХ РЕШЕНИЙ, ОСОБЕННО ЕСЛИ ОНИ КАСАЮТСЯ ДЕНЕГ ИЛИ СЛУЖЕБНОЙ ИНФОРМАЦИИ	Всегда берите паузу, чтобы разобраться в том, что происходит. Скажите, что перезвоните самостоятельно, и завершите звонок. Чтобы уточнить информацию, используйте телефоны, которые знали раньше или сами нашли в независимых источниках
ЗАЩИТИТЕ ДОМАШНИЙ WI-FI ПАРОЛЕМ	Если этого не сделать, ваш трафик могут перехватить. Мошенники захватят секретные данные, в том числе логины и пароли от всех ваших аккаунтов, почты, банковских приложений
НЕ ВЫКЛАДЫВАЙТЕ МНОГО ИНФОРМАЦИИ О СЕБЕ В ИНТЕРНЕТ	Киберпреступники охотятся за чужими личными данными. Их цель – номера карт, доступ к онлайн-банкам, домашний адрес, рабочие документы и личные фото

Памятка для педагогов