Тема 3: Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально - психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности

Жизнь в последние недели стремительно уходит в онлайн. Существенную часть своей жизни современные дети и подростки проводят в интернете, а значит без базовых знаний в области кибербезопасности им, как и взрослым, не обойтись. Чем раньше начать прививать навыки безопасного взаимодействия с виртуальной средой, тем прочнее они усвоятся. И станут такими же естественными, как мытье рук.

Подумайте, как часто родители попадают в такую ситуацию: ребенок смотрит видео в интернете. Вы выражаете недовольство тем, сколько времени он проводит за этим занятием или какой контент выбирает. На что получаете резонный ответ: «Если бы в твоем детстве было онлайн-видео, ты бы вел себя иначе?»

Многие представители поколения Z (люди, родившиеся между 1997 и 2015 годами) не выпускают смартфоны из рук. Гаджеты для них подобны новому органу чувств, объединяющему с глобальной сетью. Они выросли вместе с интернетом, это естественная и неотъемлемая часть их жизни. У поколения Z в интернете создается свой образ, новое «я», там же происходит постижение и проверка окружающего мира.

Согласно исследованию, проведенному GlobalWebIndex в 2019 году, у 97% представителей поколения Z есть мобильный телефон, и 78% из них считают его основным устройством для доступа в интернет.

С учетом особенностей поведения детей и подростков в интернете и их потребностей, стоит уделить особое внимание анонимности и приватность, целостности цифрового образа, защите репутации, защите от кибербуллинга и нежелательных знакомств, а также финансовых онлайн-транзакций и счетов.

Сам факт того, что через интернет можно что-то украсть или нанести вред не вызывает у подростков особого удивления. Гораздо больший интерес они проявляют к тому, что можно украсть именно у них и как хакеры и кибермошенники могут навредить через интернет именно им.

По данным недавнего исследования компании Proofpoint, производящей решения для безопасности электронной почты, менее 1% всех атак эксплуатируют уязвимости систем. Остальные используют человеческий фактор. Другими словами, технические средства предупреждения и мониторинга атак успешно совершенствуются,

искусственный интеллект и средства автоматизации позволят быстро реагировать на большинство инцидентов, но как быть с действиями сами людей?

Вспоминается красивая история про французского маршала Лиоте. Маршал служил в Африке. Однажды, сетуя на жару и сильное солнце, он приказал подчиненным обсадить дорогу деревьями. Подчиненные возразили, что деревья вырастут только через 50 лет. На что Лиоте парировал: «Именно поэтому работу надо начать сегодня же».

В ближайшие десятилетия поколение Z унаследует планету, оно будет стоять у руля компаний, организаций, государств. Оно будет жить в мире, где без навыков информационной безопасности уже не обойтись. Чтобы эти навыки сформировались, потребуется немало времени, именно поэтому работу стоит начать сегодня.

Что же делать родителям и учителям? Запрещать, проверять или пустить все на самотек? В первую очередь надо осознать, что полностью контролировать поведение ребенка или подростка в интернете невозможно. Так же, как раньше было невозможно полностью контролировать, что ребенок делает во дворе после уроков.

Однако взрослые могут и должны быть авторитетным источником информации о том, что такое хорошо и что такое плохо в новых реалиях.

В цифровом пространстве есть свои правила гигиены. К использованию интернета и потреблению информации стоит относиться так же, как к потреблению в физическом мире. Кстати, поколение Z воспринимает эту идею достаточно легко, поскольку границы между реальным и виртуальным миром для него несколько размыты.

Вот 10 базовых приемов информационной безопасности, о которых нужно знать и говорить детям и подросткам:

1. Не давайте свой телефон незнакомым людям, которым якобы нужно срочно позвонить. Вы же не хотите, чтобы в руки незнакомцев попал разблокированный телефон?
2. Используйте длинные и надежные пароли, а также биометрию и двухфакторную аутентификацию, особенно для платежей и денежных переводов. Использование удобных коротких паролей может плохо кончиться.
3. Меньше рассказывайте о себе в интернете. Думайте, кому и что вы говорите. Злоумышленники могут использовать раскрытые вашими же руками личные данные, чтобы атаковать вас.
4. Не принимайте запросы на дружбу от незнакомых людей в социальных сетях. Как минимум, это может кончиться валом рекламного спама. Про более скверные сценарии пишут в таблоидах каждый день.

5. Следите за тем, какие приложения получают на ваших устройствах доступ и к чему. Новой игре совершенно не обязательно знать, где вы сейчас находитесь или иметь доступ к камере или микрофону.

6. Обновляйте программы и операционные системы на всех устройствах (не только мобильных). Разработчики не зря едят свой хлеб и в новых версиях добавляют не только красивые кнопки, но и закрывают уязвимости.

7. С осторожностью открывайте электронные письма. Открывать письма с неизвестных адресов — все равно, что есть еду, которую нашел на улице. Эффект может быть схожим— заражение.

8. Аккуратнее относитесь к использованию публичных сетей Wi-Fi при обращении к своему мобильному банку. В сети гостиниц и других мест отдыха часто внедряются любители легкой наживы.

9. Не скачивайте «поломанное» программное обеспечение с неизвестных сайтов. Заражение фактически обеспечено. Для этого и размещают такое ПО, нашпигованное ловушками, а вовсе не для удобства наивных пользователей.

10. Контролируйте, что ваш ребенок покупает в интернете — все средства для этого встроены в современные операционные системы. Вы должны давать ребенку разрешение на покупку в сети в каждом случае. Наконец, заведите для этих целей отдельную дебетовую карту и пополняйте ее на ту сумму, которую не боитесь потерять.

Учите на собственном примере

Помните, что дети и подростки в целом разбираются в использовании компьютеров и мобильных устройств лучше вас. Но они не имеют вашего жизненного опыта и более доверчивы. Как поговаривала Фрекен Бок, «мой руки и учи уроки». А современным родителям стоит регулярно напоминать своим чадам: «Используй длинные пароли и не скачивай на свой телефон что попало».

Нельзя предусмотреть все. Но можно научить ребенка базовым и принципиальным вещам. А в остальном он разберется самостоятельно. Но прежде всего, конечно, сработают ваш личный пример и доверительные отношения.