

Технологическая карта урока в рамках нового сезона проекта «Цифровой ликбез»

Цели урока: сформировать представление о ценности персональных данных.

Задачи урока:

- познакомить учащихся с понятием «Незнакомцы в сети» и его особенностями;
- систематизировать знания о персональных данных и данных, которые пользователи могут публиковать в открытом доступе;
- сформировать навык «закрытия» публичной информации.

Ход урока

Слайд	Комментарий педагога	Примечание
Слайд №1	Приветствую всех на уроке в рамках нового сезона проекта «Цифровой ликбез». Мы изучим основы цифровой грамотности и правила кибербезопасности в современном мире. В этом нам помогут герои нашего ролика – начинающая журналистка Лина и осьминожек Лёлик, который столкнулся с незнакомцем в сети.	Все видеоролики доступны на сайте проекта: https://digital-likbez.datalesson.ru
Слайд №2	Сегодня мы подробно поговорим о том, как незнакомцы в сети могут добавляться к вам в друзья и каким способом узнают про ваши персональные данные.	
	Какую информацию в Интернете о себе вы публикуете? Поднимите, пожалуйста, руки	

	<p>те из вас, кто играет в компьютерные игры? Есть ли в таких играх возможность общаться с другими пользователями (игроками)? Сталкивались ли вы с таким, что незнакомец в игре пытался узнать о вас что-то? (из вашей личной жизни и т.п.)</p>	
Слайд №3	<p>Незнакомцы в сети – такие же незнакомые люди, как и в обычной жизни, которых можно встретить на улице или в общественных местах. Но если в офлайне мы стараемся не впускать в личную жизнь незнакомых нам людей, то в социальных сетях редко задумываемся об этом. Это актуальная угроза как для социальных сетей и мессенджеров, так и для компьютерных игр.</p>	
Слайд №4	<p>Давайте посмотрим видеоролик и узнаем, как же незнакомцы могли завоевать доверие юного любителя компьютерных игр – Лёлика и какую информацию украсть у него.</p>	
	<p>Все ли было понятно в видеоролике? Сталкивались ли вы с похожими ситуациями в своей жизни?</p>	
Слайд №5	<p>Теперь пришло время попрактиковаться. Начнем с того, что разграничим доступ к информации на своей странице для разных пользователей.</p>	
Слайд №6	<p>Вы можете добавить в близкие друзья тех, кого знаете в реальном мире и с кем часто общаетесь, тех, кому</p>	

	<p>вы доверяете. Если вы начинаете получать оскорбления или угрозы, то таких пользователей нужно заблокировать</p>	
Слайд №7	<p>Перейдем к разделу «Приватность» или «Конфиденциальность». В таком разделе вы указываете кому и какая информация о вас будет доступна.</p>	
Слайд №8	<p>Эксперты «Лаборатории Касперского» рекомендуют сделать всю информацию доступной только для близких друзей, таких пользователей, которых вы знаете лично и кому можете доверять.</p>	
Слайд №9	<p>Давайте проверим, какую информацию можно размещать в сети, а какую не стоит. Как вы думаете, можно ли размещать информацию о погоде?</p>	
Слайд №10	<p>Да, можно. Эта информация никак не раскрывает ваши личные данные.</p>	
Слайд №11	<p>Как вы думаете, а публиковать информацию о теме домашнего задания или проекта можно или нельзя?</p>	
Слайд №12	<p>Да, можно. Эта информация никак не раскрывает ваши личные данные.</p>	

Слайд №13	Можно ли публиковать ссылки на свои аккаунты в других социальных сетях?	
Слайд №14	<p>Лучше этого не делать. Так злоумышленники не будут знать, какие еще сервисы вам доступны.</p> <p>Благодаря этому они могут найти информацию в них, чтобы завоевать ваше доверие.</p>	
Слайд №15	Можно ли сообщать информацию о кодах верификации, информации, которую вы получили в виде смс-сообщений или пуш-уведомлений. Такие коды пользователь получает для авторизации в различных сервисах.	
Слайд №16	<p>Такую информацию нельзя публиковать нигде, даже в закрытом доступе, и сообщать посторонним.</p>	
Слайд №17	Как не стать жертвой незнакомцев в сети?	
Слайд №18	<ul style="list-style-type: none"> • Не сообщайте никакую информацию о себе посторонним людям; • Не публикуйте свои личные данные и данные ваших друзей и близких (например, настоящее имя или фамилию, номер телефона, адрес и место учебы или работы); 	

	<ul style="list-style-type: none">• Не выкладывайте фото личных переписок и не пересылайте их другим людям;• Не храните личные данные в открытых источниках или облачных хранилищах; <p>Для защиты своих аккаунтов используйте только уникальные и сложные пароли.</p>	
Слайд №19	<p>Наш урок подошел к концу. Вы отлично поработали!</p> <p>Соблюдайте безопасность в сети и до новых встреч в новом сезоне проекта «Цифровой ликбез»!</p>	