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

Цели урока: формирование базовых правил безопасной работы с личными аккаунтами в сервисах Интернета.

Задачи урока:
— познакомить учащихся с понятием «Безопасность аккаунта» и его особенностями;
— научить обучающихся распознавать потенциально опасные схемы, которые могут использовать злоумышленники, чтобы украсть аккаунт или получить доступ к персональным данным;
— познакомить учащихся с понятием «социальная инженерия».

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 поможет начинающая журналистка Лина, которая проходит стажировку в компании «Карасевский».	Все видеоролики доступны на сайте проекта: **https://digital-likbez.datalesson.ru**
Слайд №2	Сегодня мы подробно поговорим о том, как злоумышленники могут украсть аккаунты в различных интернет-сервисах, а также узнаем, как их защитить.	Ссылка на видеоролик:
	Поднимите, пожалуйста, руки те из вас, у кого есть аккаунты в мессенджерах, играх или социальных	

	сетях? А кто из вас сталкивался с кражей своего аккаунта?	
Слайд №3	Давайте посмотрим видеоролик и разберемся, как же злоумышленники могут украсть ваш аккаунт.	
	Все ли было понятно в видеоролике? Сталкивались ли вы с похожими ситуациями в своей жизни?	
Слайд №4	Давайте рассмотрим несколько ситуаций, которые могут повлечь за собой кражу вашего аккаунта и личных данных.	
Слайд №5	На слайде пример: Ваш друг просит перейти по ссылке и проголосовать за него в конкурсе, который для него очень важен. Как определить, что это сообщение от злоумышленника?	
Слайд №6	Во-первых, обратите внимание на ссылку. Если ссылка содержит опечатки или выглядит подозрительно, это фишинговая ссылка, не переходите по ней. Страница сайта с голосованием никогда не будет запрашивать номер телефона, банковской карты и других личных данных.	

	Свяжитесь с другом, от которого получили сообщение, по телефону и уточните, действительно ли он участвует в конкурсе.	
Слайд №7	На слайде пример: Вы получили сообщение с предложением выиграть новый телефон, перейдя по ссылке.	
Слайд №8	Это снова уловка злоумышленников. Настороженно относитесь к очень щедрым предложениям в Интернете. Например, к возможности что-то выиграть или заработать, лишь перейдя по ссылке.	
Слайд №9	Давайте закрепим полученные знания и ответим на несколько вопросов.	
Слайд №10	Вопрос 1. Каким должен быть пароль для разных аккаунтов? Выберите наиболее полный ответ. А) он должен состоять из более чем 12 символов, цифр и специальных символов Б) он должен быть уникальным и состоять из более чем 12 символов, цифр и специальных символов В) это должен быть номер телефона, так как его легко запомнить Г) паролем должен быть домашний адрес, так как его легко запомнить	

Слайд №11	Правильный ответ на этот вопрос – Б (он должен быть уникальным и состоять из более чем 12 символов, цифр и специальных символов).	
Слайд №12	Вопрос 2. Вы получили сообщение, в котором есть ссылка на незнакомый вас ресурс. Ваши действия (Выберите несколько вариантов): А) открою ссылку, но не буду вводить никаких данных Б) не стану ничего делать, даже если явно попросят перейти по ссылке В) разошлю друзьям/родным, пусть сначала они попробуют Г) удалю пользователя из книги контактов	
Слайд №13	Правильный ответ на этот вопрос – А и Б (открою ссылку, но не буду вводить никаких данных; не стану ничего делать, даже если явно попросят перейти по ссылке).	
Слайд №14	Вопрос 3. Вы получили сообщение о том, что выиграли в лотерею денежный приз, но нигде не принимали участие. Вас просят оплатить небольшую комиссию за обработку вашего платежа и после этого обещают перевести денежные средства на ваш счет. Ваши действия (Выберите один вариант): А) все сделаю, как они просят	

	Б) разошлю друзьям, пусть они тоже поучаствуют В) никак не стану реагировать и отвечать, так как очень похоже на мошенничество Г) почитаю в Интернете, если не найду ничего плохого, то все переведу им деньги	
Слайд №15	Правильный ответ на этот вопрос – В (никак не стану реагировать и отвечать, так как очень похоже на мошенничество).	
Слайд №16	Вопрос 4. От каких сервисов злоумышленники могут украсть данные для авторизации (Выберите несколько вариантов)? А) от мессенджеров Б) от социальных сетей В) от игровых сервисов Г) от онлайн библиотеки	
Слайд №17	Правильный ответ на этот вопрос – А, Б, В, Г.	
Слайд №18	Вопрос 5. Где безопаснее скачивать новые приложения на телефон/планшет (Выберите несколько вариантов)? А) на сайте разработчика	

	Б) на специализированных форумах В) на сайтах производителей Г) спрашиваю друзей, они мне присылают ссылку	
Слайд №19	Правильный ответ на этот вопрос – А и В.	
Слайд №20	Отлично! Итак, как же защитить аккаунты от кражи?	
Слайд №21	• Не верьте сообщениям, в которых вас просят сделать что-то очень быстро (например, перейти по ссылке), даже если его прислал ваш друг; • Свяжитесь с другом любым другим удобным способом и уточните, не взломали ли его; • Не верьте очень щедрым предложениям в интернете. Например, что-то выиграть или заработать большую сумму, перейдя по ссылке; • Не скачивайте программы и игры из непроверенных источников, даже если вам предлагают самую новую версию – только из официальных магазинов; • Настройте дополнительное подтверждение входа по коду, то есть двухфакторную аутентификацию; • Установите антивирусную защиту, чтобы не перейти по фишинговой ссылке.	

Слайд №22	Наш урок подошел к концу. Вы отлично поработали! Соблюдайте безопасность в сети и до новых встреч в новом сезоне проекта «Цифровой ликбез»!	