ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КИМРСКИЙ КОЛЛЕДЖ»

МЕТОДИЧЕСКАЯ РАЗРАБОТКА ОТКРЫТОГО УРОКА

ПО ДИСЦИПЛИНЕ ОСНОВЫ ФИНАНСОВОЙ ГРАМОТНОСТИ

ТЕМА УРОКА

«КАК ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИЧЕСТВА»

Разработал преподаватель:
Преподаватель ГБП ОУ «Кимрский колледж»
Соловьева Татьяна Алексеевна

Г. КИМРЫ
2023

СОДЕРЖАНИЕ

АННОТАЦИЯ

Методическая разработка урока финансовой грамотности на тему «Как защититься от кибермошенничества» для студентов третьего курса ГБП ОУ «Кимрский колледж» представляет собой документ, содержащий: методический комментарий, в котором отражены цель и задачи, результаты, полученные преподавателями при проведении учебного занятия; план учебного занятия; технологическую карту учебного занятия; ход учебного занятия; приложения, содержащее раздаточный материал, фотоотчет о проведенном мероприятии.

МЕТОДИЧЕСКИЙ КОММЕНТАРИЙ

«Нажить много денег - храбрость; сохранить их - мудрость,
умело расходовать – искусство»
Бертольд Авербах

Указом Президента Российской Федерации №1101 от 19 августа 2011 года

«День финансиста» учрежден в качестве государственного праздника, который теперь ежегодно отмечается 8 сентября. Дата выбрана не случайно – в этот день в 1802 году император Александр I основал Министерство финансов России.

В последнее время все больше внимания уделяется проблеме повышения финансовой грамотности населения. Финансовая грамотность необходима людям в любом возрасте. Пенсионерам она нужна, чтобы умело распорядиться накопленными средствами, не потерять деньги в финансовых пирамидах, научиться пользоваться теми финансовыми инструментами, которые экономят время и усилия. Людям среднего возраста финансовая грамотность позволит выработать правильные стратегии накопления на старость, даст возможность эффективно распоряжаться имеющимися финансовыми средствами. Молодежь приобретет представление о финансах, заложит навыки планирования бюджета и сбережений, позволит решить проблемы финансирования образования и покупки жилья.

Финансовая грамотность – это совокупность способностей, которые, хотя и приобретаются в процессе финансового образования в школе и колледже, но осваиваются и проверяются на практике в течение жизни.

Цель финансового просвещения молодежи – доставка понятной качественной информации «точно в срок» до каждого нуждающегося в ней потребителя.

Актуальность методической разработки заключатся в том, что в ней представлен материал, направленный на формирование представлений о финансовых махинациях, о том, почему люди становятся жертвами финансовых мошенников, способах защиты своих интересов в современном мире. В соответствии с ФГОС СПО обучающиеся должны формировать компетенцию: Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития, сопровождающуюся поиском информации в сети интернет. Поэтому роль каждого преподавателя – показать значимость проблемы безопасности в Интернет-пространстве и пути ее решения для будущего общества и образования. Формирование финансовой грамотности должно вестись с обучающимися постоянно в рам-

ках урочной, в том числе и вне урочной деятельности с использованием всех возможных педагогических технологий.

Акцент необходимо делать на актуальности данной темы и постоянный самоконтроль обучающихся в их дальнейшей самостоятельной деятельности.

Подготовленный сценарий занятия полностью раскрывает обозначенную тему, адаптирован для целевой аудитории – обучающихся первого курса всех специальностей/профессий колледжа, изложен в доступной форме. Студенты узнают о том, что нужно делать в случае сомнительных, тревожных телефонных звонков, писем на электронную почту и СМС на личные телефоны.

Во время проведения учебного занятия происходит чередование видов работы обучающихся: совместно с преподавателем, работа в парах - самостоятельная работа. В качестве контрольно-измерительных материалов разработаны тестовые вопросы, которые могут быть использованы по окончании изучения соответствующей темы.

Целью методической разработки является описание методики проведения урока финансовой грамотности на тему «Как защититься от кибермошенничества», раскрывающей педагогический опыт работы преподавателей ГБПОУ Новокузнецкого горнотранспортного колледжа по повышению финансовой грамотности обучающихся первого курса колледжа.

Задачи методической разработки:

обосновать необходимость проведения уроков финансовой грамотности для студентов третьего курса;

представить методику проведения урока финансовой грамотности на тему «Как защититься от кибермошенничества».

Методическая разработка включает:

методический комментарий, в котором отражены цель и задачи, результаты, полученные преподавателем в процессе проведения занятия, критерии оценивания результатов;

план учебного занятия;

технологическую карту учебного занятия;

ход учебного занятия;

приложения, содержащие раздаточный материал, презентацию к учебному занятию.

В процессе занятия, обучающиеся овладевают знаниями о кибермошенничестве, методами борьбы с кибермошенниками, уголовной ответственности за кибермошенничество.

Закрепление знаний, обучающихся происходит через формирование умения решать практические ситуационные задачи по данной теме.

На занятии используются мультимедийная презентация по ключевым моментам занятия и раздаточный материал (представлен в Приложениях данного текстового документа).

В заключительной части учебного занятия преподаватель подводит итог в соответствии с

поставленными целью и задачами.

Результаты освоения учебного занятия:

Учебное занятие «Как защититься от кибермошенничества» направлено на развитие универсальных учебных действий, формирование личностных, предметных и метапредметных результатов ФГОС СОО, а также общих компетенций ФГОС СПО по специальностям/профессиям колледжа:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

Планируемые результаты освоения в соответствии с ФГОС СОО	Общие компетенции ФГОС СПО
Метапредметные:	
М1. умение самостоятельно определять цели деятельности и составлять планы деятельности; самостоятельно осуществлять, контролировать и корректировать деятельность; использовать все возможные ресурсы для достижения поставленных целей и реализации планов деятельности; выбирать успешные стратегии в различных ситуациях;	ОК 2, ОК 4, ОК 6
М2. владение навыками познавательной, учебно-исследовательской и проектной деятельности, навыками разрешения проблем; способность и готовность к самостоятельному поиску методов решения практических задач, применению различных методов познания;	ОК 2, ОК 4, ОК 5
М3. готовность и способность к самостоятельной информационно- познавательной деятельности, владение навыками получения необходимой информации, умение ориентироваться в различных источниках информации,	ОК 2, ОК 4, ОК 6

критически оценивать и интерпретировать информацию, получаемую из различных источников; М4. умение использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, М5. умение самостоятельно оценивать и принимать решения, определяющие стратегию поведения, с учетом гражданских и нравственных ценностей	ОК 4, ОК 5 ОК 2, ОК 7, ОК 8
Предметные: П1 владение навыками поиска актуальной экономической информации в различных источниках, включая Интернет; умение различать факты, аргументы и оценочные суждения; анализировать, преобразовывать и использовать экономическую информацию для решения практических задач в учебной деятельности и реальной жизни	ОК 4, ОК 5, ОК 6

Критерии оценивания результатов, обучающихся на занятии, осуществляется посредством:

1. Самоимооценки результатов выполнения тестовых заданий в соответствии с эталоном ответов и критериями оценки, представленными на слайде.
2. Проверки правильности решения ситуационных задач.

Рациональность применяемых средств развития формирование ОК 2, ОК 4, ОК 6.

- применение работы в парах (малых группах) при решении задач (ОК 2, ОК 7, ОК 8),
- использование самоконтроля, направленного на формирование ОК 2, ОК 4, ОК 6.

ПЛАН
ЗАНЯТИЯ ПО ФИНАНСОВОЙ ГРАМОТНОСТИ ОБУЧАЮЩИХСЯ

Целевая аудитория: студенты 3 – го курса

Специальность: все специальности/профессии колледжа

Преподаватель: Соловьева Т.А.

Тема занятия: Как защититься от кибермошенничества

Форма занятия: урок-практикум

Продолжительность занятия: 90 минут.

Цель занятия: формирование социально-финансовой компетентности обучающихся колледжа.

Обучающая	показать актуальность данной темы; познакомить обучающихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет и научить избегать их; отработать умения: сравнения информации, критического анализа; выделения главных мыслей и грамотного их изложение; восприятия и усвоения услышанного; научить информационной безопасности в Интернете.
Развивающая	Содействовать развитию умений и навыков: общеучебных умений и навыков: работать с источниками информации, взаимодействовать в группе; мышления: анализировать информацию, ситуации из жизни; анализировать свои ошибки и исправлять их в процессе решения задач. Расширить кругозора обучающихся. Формировать информационную культуру.
Воспитательная	Содействовать пониманию значимости финансовой грамотности. Создать условия для развития самоконтроля обучающихся и воспитание внимательного отношения к информационным ресурсам.

Формы организации учебной деятельности обучающихся:

- коллективная (в процессе изучения нового материала);
- парная (в процессе решения практических задач).

Методы обучения:

- объяснительно-иллюстративный: демонстрация наглядных пособий с использованием технических средств обучения (мультимедийной установки);
- презентация по ключевым моментам занятия «Как защититься от кибермошенничества».

Методы контроля:

- взаимоконтроль: проверка выполненных тестовых заданий;
- решение ситуационных задач в группах

Средства обучения:

- мультимедийный комплекс преподавателя: мультимедийная презентация по ключевым моментам занятия;
- карточки с ситуационными задачами для решения в группах.

Информационные источники:

Основные источники:

1. Андрей Масалков: Особенности киберпреступлений в России. Инструменты нападения и защита информации. Издательство: ДМК-пресс, 2018.
2. Уголовный кодекс РФ. Редактор: Усанов. Издательство: Эксмо-пресс, 2019.
3. Корыстные киберпреступления: уголовная ответственность и стимулирование позитивного постпреступного поведения. Автор: Висков Николай Викторович-2016.

ТЕХНОЛОГИЧЕСКАЯ КАРТА УЧЕБНОГО ЗАНЯТИЯ

Дидактический элемент занятия	Время, мин.	Деятельность ведущих занятие преподавателей (задания для обучающихся, выполнение которых приведет к достижению планируемых результатов)	Деятельность обучающихся	Планируемые результаты	
				М, П	ОК
Организационная часть	10	Приветствие обучающихся преподавателя; выявление отсутствующих обучающихся; постановка цели и задач занятия. Целеполагание. Мотивация обучающихся	Приветствуют преподавателя Внимательно прослушивают информацию преподавателей. Самостоятельно озвучивают обучающую цель. Отвечают на вопросы	М1, П1	ОК 2, ОК 4, ОК 6
2. Актуализация опорных знаний	15	Анализ социологического опроса по финансовой грамотности обучающихся Отвечают на вопросы преподавателя Командам предложена карточка с описанием ситуации из жизни. После выполнения задания карточки возвращаются преподавателю.	Внимательно прослушивают информацию преподавателей Выполнение задания по карточкам - жизненным ситуациям	М2, М5, П1	ОК 2, ОК 4, ОК 5
3.Изучение нового материала	35	Мошенничество по телефону. Как это работает? Мошеннические СМС-сообщения и электронные письма. Как это работает? Финансовое мошенничество в интернете. Как это работает? 4.Уголовная ответственность за кибермошенничество	Анализируют и выявляют по изученному материалу (работают в группах, слушают мнение эксперта): -Как защитить себя от мошенничества по телефону; - Безопасная электронная почта -Как защитить себя от мошенничества в интернете. Внимательно прослушивают информацию преподавателя.	М3, П1	ОК 2, ОК 4, ОК 6

4.Закрепление знаний	15	На закрепление изученного материала обучающиеся выполняют тест, который представлен на слайдах. После выполнения заданий обучающимся представляются на слайде эталоны ответов и оценка ответов.	Выполняют тестовые задания. Оценивают выполнение заданий с учетом представленных критериев оценки.	М4, П1	ОК 2, ОК 4, ОК5 ОК 6
5. Рефлексия	5	Предлагает обучающимся поместить стикеры (в зависимости от достигнутой цели занятия) на соответствующую ступеньку: знаю общие сведения кибермошенничестве; в основном уверен в том, что меня не обманут кибермошенники; уверен в своих знаниях и в себе!	Рефлексируют. Высказываются о целесообразности данного занятия.	М2, М3, П1	ОК2, ОК6
6.Подведение итогов занятия	7	Уважаемые обучающиеся! Посмотрите на слайды и скажите, все ли задачи, поставленные в начале занятия, мы решили, достигли ли мы цели занятия?	Участвуют в обсуждении занятия.	М3, П1	ОК 2, ОК 4, ОК 6
7.Выдача домашнего задания	3	Преподаватель предлагает студентам найти в Интернете сайты, защищающие их от «опасной» информации	Выслушивают информацию преподавателя.	М5, П1	ОК 2, ОК7, ОК8

ХОД УЧЕБНОГО ЗАНЯТИЯ

ОРГАНИЗАЦИОННЫЙ МОМЕНТ

Демонстрация слайда 1

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КИМРСКИЙ КОЛЛЕДЖ»

**МЕТОДИЧЕСКАЯ РАЗРАБОТКА ОТКРЫТОГО УРОКА
ПО ДИСЦИПЛИНЕ ОСНОВЫ ФИНАНСОВОЙ ГРАМОТНОСТИ
ТЕМА УРОКА
«КАК ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИЧЕСТВА»**

**Разработал:
Преподаватель ГБП ОУ «Кимрский колледж»
Соловьева Татьяна Алексеевна**

**Г. КИМРЫ
2023**

Преподаватель:

Отметим отсутствующих. Сегодня нас ждет увлекательное занятие, участвовать в котором мы будем командами. Прошу вас разделиться на 6 команд поровну (по 3- 4 человека) в каждой команде.

Демонстрация слайда 2

Мы живем в эпоху информационных технологий. Современные люди не представляет свое существование без Интернета. Ведь современному человеку, можно не выходя из дома работать. В Интернете можно найти информацию для реферата или курсовой работы (проекта), послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями.

Вопросы к студентам:

Приведите примеры использования Интернета в своей повседневной жизни. Приведите ситуации, в которых благодаря Интернету мы экономим время. Безопасно ли использовать данные Интернет-возможности? Почему?

Демонстрация слайда 3

В наш информационный век существует множество опасных случаев при использовании Интернета. Сеть Интернет скрывает и угрозы! В связи с массовой популярностью сети Интернет важной проблемой сегодня является безопасность в глобальной сети. Касается данная проблема абсолютно всех, начиная от Вас, Ваших родителей и заканчивая пенсионерами. Как вы думаете, о чем пойдет сегодня речь на уроке?

Тема урока: Как защититься от кибермошенничества.

А теперь попробуем самостоятельно поставить цель нашего занятия.

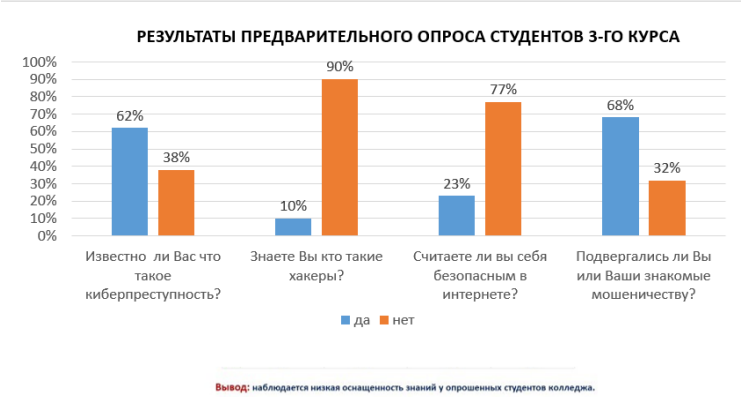
Обучающиеся самостоятельно озвучивают обучающую цель.

Демонстрация слайда 4

АКТУАЛИЗАЦИЯ ОПОРНЫХ ЗНАНИЙ

Анализ социологического опроса по финансовой грамотности обучающихся

Демонстрация слайда 5



Преподаватель:

Перед занятием был проведен социологический опрос среди студентов 3 курса. Суть опроса заключалась в том, что нужно было узнать насколько наши студенты (возраст 17-18 лет) финансово грамотны, встречались ли случаи кражи финансов.

Были предложено ответить на следующие вопросы:

1. «Известно ли Вам такое понятие как киберпреступность?»:

62% - ответили «да», 38% - затруднились с ответом.

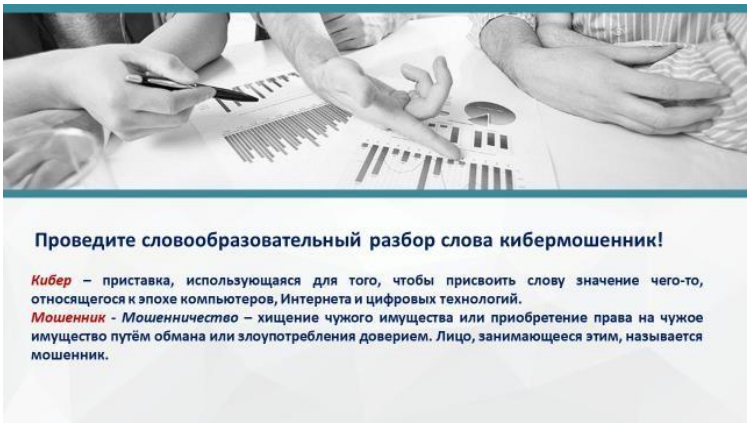
2. «Какие способы хищения коснулись вас?»: так как многие были не знакомы с этим термином, то соответственно не могли ответить. После объяснения, студенты смогли ответить на этот вопрос: 21% опрошенных ответили, что так или иначе подвергались мошенничеству. И только 10% на личном опыте встречались с кражей паролей, номеров карт.

3. «Знаете ли Вы кто такие хакеры?»: не все студенты смогли дать определение этому понятию, из этого следует вывод, что студенты мало оснащены даже базовыми знаниями о кибер-мошенничестве.

4. «Считаете ли вы себя безопасным в интернете?»: 68% считают себя небезопасным в интернет-пространстве, 32% ответили, что уверенны в себе и своих силах.

Вывод: наблюдается низкая оснащенность знаний у опрошенных студентов колледжа.

Демонстрация слайда 6



Проведите словообразовательный разбор слова кибермошенник. Найдите в этом слове приставку. Что она означает?

Кибер – приставка, использующаяся для того, чтобы присвоить слову значение чего-то, относящегося к эпохе компьютеров, Интернета и цифровых технологий.

Как вы думаете, каким образом можно назвать пространство, которое образуют компьютеры, компьютерные сети?

Демонстрация слайда 7

Всемирная паутина, интернет пространство.

Конечно, компьютеры, программы, компьютерные сети, образуют глобальное информационное пространство, в котором происходит общение через социальные сети, чаты, телефонные разговоры, передача больших объемов данных на очень высокой скорости, и которое носит название «киберпространство».

Выполнение задания по карточкам-жизненным ситуациям

Демонстрация слайда 8

Мошенники умеют выманивать деньги через киберпространство. Сейчас каждой команде будет предложена карточка с описанием ситуации из жизни (Приложение 1). Вам необходимо кратко написать свой ответ о том, что вы будете делать в предложенной ситуации, и вернуть карточки. Ваши ответы мы обсудим немного позже.

Уважаемые студенты! Вы прочитали разные ситуации, в которых вам предстояло сделать выбор: переводить деньги или нет, пересылать данные банковской карты третьим лицам или не пересылать. Давайте поговорим об этом подробно.

ПОЛУЧЕНИЕ НОВЫХ ЗНАНИЙ

Демонстрация слайда 9

МОШЕННИЧЕСТВО ПО ТЕЛЕФОНУ. КАК ЭТО РАБОТАЕТ?

Мошенники звонят, они сообщают о чем-либо, но итог один: необходимо немедленно перевести деньги по номеру телефона или перейти по ссылке, что заполнить данные своей карты и т. д. Итог один: на другом конце провода сидит мошенник, который хочет выманить с вас денег любым путем.

Как поступить в таких ситуациях. Главное - не должно быть никакой паники! Прекратите разговор и позвоните другу (родственнику). Если вас просят продиктовать номер банковской карты, ПИН-код, другие данные, ни в кое случае этого не делайте! Настоящие сотрудники банка никогда не попросят по телефону вашу персональную информацию.

Преподаватель:

А теперь давайте посмотрим ваши ответы. Вы изменили свое мнение?

Как вы поступите в описанных ситуациях? Кто-нибудь из команды пусть выступит в роли эксперта.

Студент - «Эксперт» зачитывает карточку по определенной ситуации: У сотрудников банка имеется вся необходимая информация. Чтобы удостовериться, надо перезвонить в банк по телефону.

Мы поговорили о хитростях телефонных мошенников.

Демонстрация слайда 10

МОШЕННИЧЕСКИЕ СМС-СООБЩЕНИЯ И ЭЛЕКТРОННЫЕ ПИСЬМА. КАК ЭТО РАБОТАЕТ?

Преподаватель:

Мошенники рассылают СМС-сообщения и письма на электронную почту с целью выведать данные вашего паспорта и банковской карты следующим образом:

- в социальных сетях вам предлагают купить какой-либо товар по весьма привлекательной цене. Для оплаты необходимо перейти по ссылке и ввести данные банковской карты;
- на вашу электронную почту или мобильный телефон приходит сообщение от друга (родственника) с просьбой одолжить денег или со странной ссылкой. Очень похожее сообщение может прийти от какого-нибудь адвоката вашего умершего родственника. После смерти _ _ _ остался большой счет в банке, а Вы единственный родственник, который может забрать эти деньги;
- с сайта известной компании вы получили сообщение с предложением заработать крупную сумму денег. Правда, вначале необходимо пройти обучение, которое стоит небольших денег. Оплатить курс вы можете, пройдя по ссылке;
- на вашу электронную почту или мобильный телефон приходит сообщение о вашем выигрыше в лотерею, для получения крупного денежного приза вас просят переслать реквизиты карты.

Уважаемые студенты! Не верьте! Это опять мошенники, которые хотят быстро заработать деньги.

Что делать?

Будьте осторожны, когда покупаете товары через социальные сети! В первую очередь надо проверить вероятного продавца по отзывам.

Если странные сообщения через социальные сети шлет ваш друг, то обязательно, позвоните ему и спросите, нужна ли ему помощь.

Если вам приходит на почту письмо от иностранца или от известной компании, то ничего особенного не произойдет, если вы просто прочитаете письмо. Но нельзя переходить по ссылке! В

противном случае компьютер будет заражен вирусом.

Демонстрация слайда 11

ПЯТЬ ПРАВИЛ БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их.

Никогда не отвечайте на спам.

Применяйте фильтр спама или программы работы с электронной почтой.

Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.

Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их. Раньше СМИ отвечали за каждое свое слово, а в Интернете царила свобода. Сегодня по количеству введенных запретов для пользователей Интернета российские законодатели перегнали многие развитые страны.

Преподаватель.

А что вы ответили на ситуации, описанные в следующих карточках.

Преподаватель зачитывает по одной карточке, а также ответы студентов на них.

Кто хочет побыть экспертом и зачитать ответы на данные ситуации?

Студент - «Эксперт» комментирует записи.

Теперь речь пойдет о ФИНАНСОВОМ МОШЕННИЧЕСТВЕ В ИНТЕРНЕТЕ. КАК ЭТО РАБОТАЕТ?

Демонстрация слайда 12

1. Мошенники крадут информацию о вашей банковской карте во время покупок на сайтах интернет-магазинов, при пользовании мобильным банком, копируя сайты известных компаний и банков. Например, вы решили пополнить баланс своего телефона через мобильный банк, зашли на сайт банка, а попали на сайт-клон. Если вы введете на таком сайте свои данные, они попадут в руки злоумышленников.

2. На электронную почту вам может прийти сообщение от вашего банка о том, что во время последней операции произошла ошибка, в связи с чем вам нужно перейти по ссылке и повторно ввести информацию вашей карты.

3. Скачивая различные программы и приложения на свой смартфон, вы рискуете заразить его вирусом, который передаст информацию о вашей карте мошенникам.

Демонстрация слайда 13

КИБЕРМОШЕННИЧЕСТВО. КАК ПРЕДОТВРАТИТЬ?

1. Скачивайте приложения на телефон только в официальном магазине.

2. Пользуйтесь только личными устройствами. Если вы потеряете телефон, к которому подключено СМС-информирование или мобильный банк, срочно позвоните в банк и отключите от утерянного номера все услуги.

3. Обязательно поставьте антивирус на всех своих устройствах.

4. Никогда не переходите по ссылкам из писем и СМС от неизвестных отправителей.

5. Делайте покупки только на сайтах, которые обеспечивают безопасное соединение. Адрес такого ресурса начинается с https://.

6. Выбирайте известные интернет-магазины и сервисы.

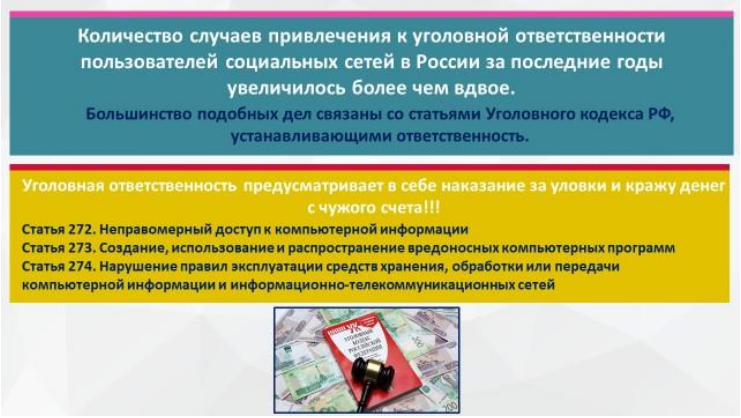
7. Никому не сообщайте персональную информацию. Чаще всего в краже средств со счета виноваты не банки или онлайн-магазины, а сами доверчивые пользователи.

Преподаватель.

А как вы ответили на вопросы по интернет-мошенничеству. (Педагог зачитывает ответы.) Заслушаем также мнение эксперта.

Студент - «Эксперт» комментирует записи.

Демонстрация слайда 14



УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА КИБЕРМОШЕННИЧЕСТВО

Уголовная ответственность предусматривает в себе наказание за уловки и кражу денег с чужого счета.

Статья 272. Неправомерный доступ к компьютерной информации (в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, - наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы

на тот же срок. (в ред. Федерального закона от 28.06.2014 N 195-ФЗ)

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Примечания. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В данной главе крупным ущербом считается сумма свыше одного миллиона рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ (в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

5. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

6. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

7. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (в ред. Федерального закона от 07.12.2011 N 420- ФЗ)

8. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно- телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, - наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

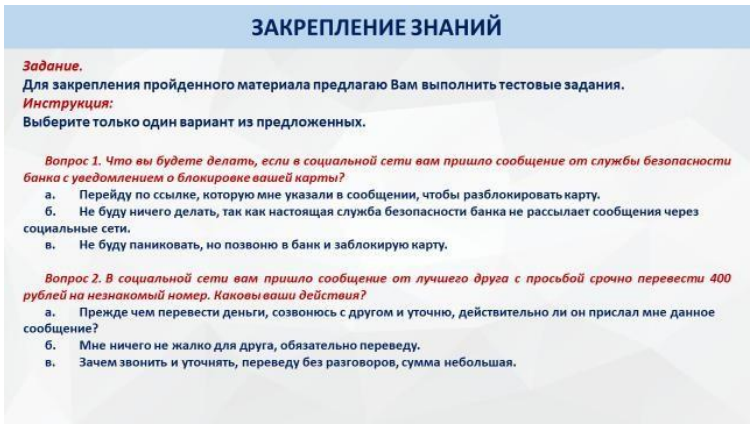
9. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, - наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок [2].

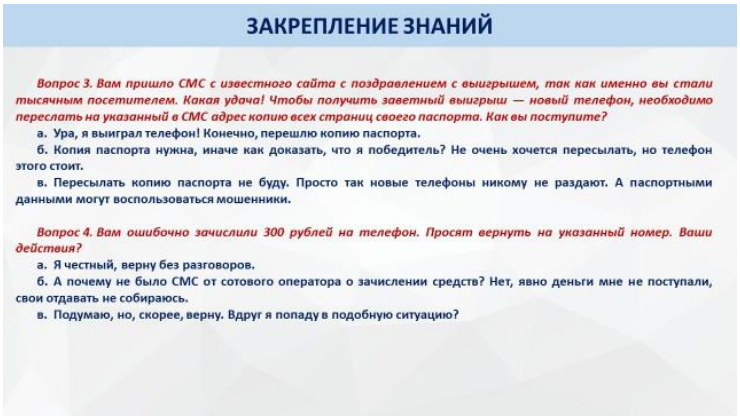
ЗАКРЕПЛЕНИЕ ЗНАНИЙ

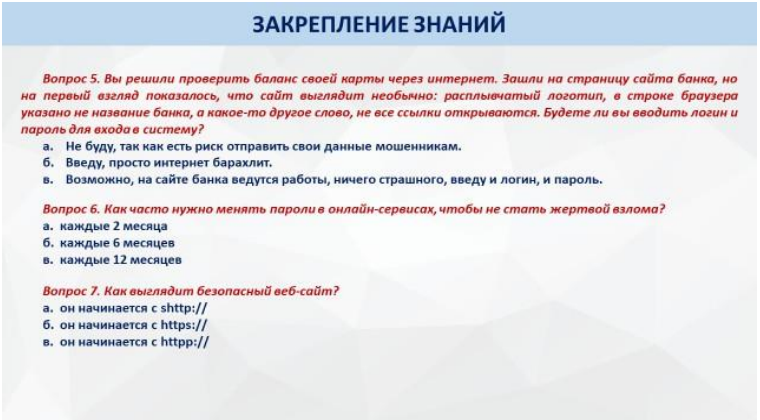
Преподаватель.

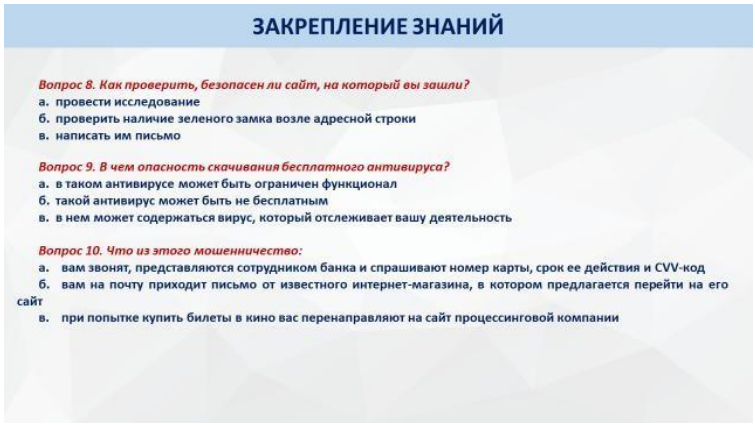
Для закрепления пройденного материала предлагаю вам выполнить тестовые задания (Приложение 2).

Демонстрация слайда 15-18









После выполнения тестовых заданий эталоны ответов демонстрируются на слайде, студенты проводит самооценку выполненных заданий.

Демонстрация слайда 19

РЕФЛЕКСИЯ

Предлагает обучающимся поднять стикеры (в зависимости от достигнутой цели занятия) соответствующего цвета:

зеленый стикер - знаю общие сведения кибермошенничестве;

желтый стикер – в основном уверен в том, что меня не обманут кибермошенники;

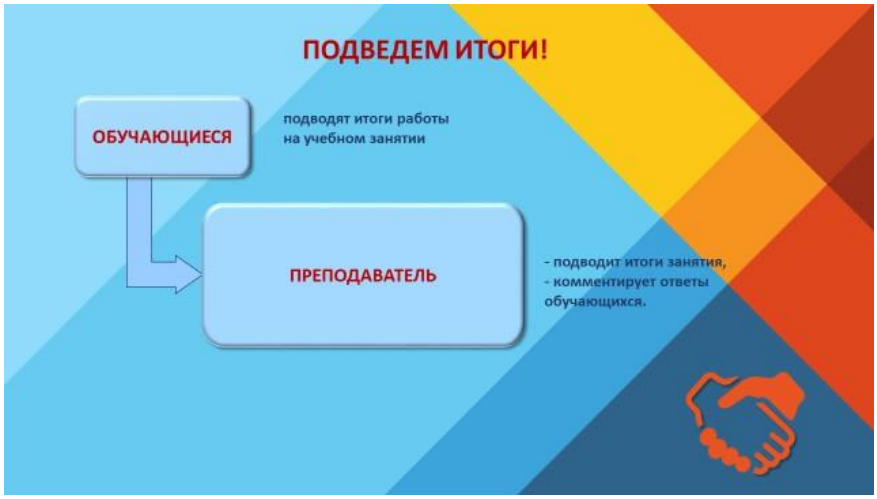
красный стикер - уверен в своих знаниях и в себе, меня не обмануть кибермошенникам!

Демонстрация слайда 20

ПОДВЕДЕНИЕ ИТОГОВ ЗАНЯТИЯ

Мы рассмотрели кибермошенничество как потенциальную угрозу современному информационному обществу. Результаты показали, что эта проблема является острой и требует большого внимания со стороны граждан любого возраста. Уважаемые обучающиеся! Посмотрите на слайды и скажите, все ли задачи, поставленные в начале занятия, мы решили, достигли ли мы цели занятия?

Демонстрация слайда 21



ВЫДАЧА ДОМАШНЕГО ЗАДАНИЯ

Преподаватель предлагает студентам найти в Интернете сайты, защищающие их от «опасной» информации.

Демонстрация слайда 22

Всем спасибо! До свидания!

ПРИЛОЖЕНИЕ 1

КАРТОЧКИ-ЗАДАНИЯ С ОПИСАНИЕМ СИТУАЦИИ

Карточка1

На мобильный телефон: «Добрый день! Хочу предложить тебе интересную, высокооплачиваемую работу. Предлагаю тебе размещать посты о нашей компании в интернете. Оплата 500 долларов США в месяц. Торопись, друг, подобное письмо я направил еще нескольким парням, кто первый из вас перейдет по ссылке, тот и получит работу своей мечты!» ВАШИ ДЕЙСТВИЯ

Карточка 2

Вы получили сообщение от друга через социальную сеть с просьбой одолжить денег: «Привет, срочно нужно 500 рублей, перекинь на номер _,_ _ _, _ _ _, _ _, _ _ я все объясню позже».

ВАШИ ДЕЙСТВИЯ

Карточка 3

На мобильный телефон вам пришло сообщение: «Поздравляем, вы выиграли современный телефон! Это не розыгрыш, перешлите на указанный номер -,---,---,--,-- фото своего паспорта, номер телефона, мы Вам перезвоним для отправки приза».

ВАШИ ДЕЙСТВИЯ

Карточка 4

На вашу электронную почту приходит письмо с адреса известной платежной системы: «Мы подвели итоги лотереи держателей карт нашей платежной системы. Поздравляем вас с победой в конкурсе! Перейдите по ссылке для получения приза». Вы перешли по ссылке и видите знакомую вам страницу сайта, правда (логотип платежной системы какой-то нечеткий. Перед вами форма для заполнения информации по вашей карте, куда вам перечислят деньги.

ВАШИ ДЕЙСТВИЯ

Карточка 5

На ваш мобильный телефон пришло сообщение: «Вам поступил платеж 200 рублей». При этом вы не пополняли счет своего телефона. Вы удивлены. Через некоторое время приходит новое сообщение: «Простите, по ошибке перевела 300 рублей на ваш счет. Пожалуйста, верните деньги на мой номер -. - - -,---,--,--. Лиза».

ВАШИ ДЕЙСТВИЯ

Карточка 6.

На мобильный телефон вам звонит человек и, представляясь сотрудником банка, сообщает, что по вашей банковской карте была проведена сомнительная операция, из-за чего банк заблокировал карту. Для разблокировки вам необходимо сейчас сообщить всю важную информацию: ФИО, номер карты, ПИН-код, трехзначный код на оборотной стороне карты.

ВАШИ ДЕЙСТВИЯ

ПРИЛОЖЕНИЕ 2

ТЕСТОВОЕ ЗАДАНИЕ ДЛЯ ЗАКРЕПЛЕНИЯ ПОЛУЧЕННЫХ ЗНАНИЙ

1. Что вы будете делать, если в социальной сети вам пришло сообщение от службы безопасности банка с уведомлением о блокировке вашей карты?

а. Перейду по ссылке, которую мне указали в сообщении, чтобы разблокировать карту.

б. *Не буду ничего делать, так как настоящая служба безопасности банка не рассылает сообщения через социальные сети.*

в. Не буду паниковать, но позвоню в банк и заблокирую карту.

2. В социальной сети вам пришло сообщение от лучшего друга с просьбой срочно перевести 400 рублей на незнакомый номер. Каковы ваши действия?

а. *Прежде чем перевести деньги, созвонюсь с другом и уточню, действительно ли он прислал мне данное сообщение?*

б. Мне ничего не жалко для друга, обязательно переведу.

в. Зачем звонить и уточнять, переведу без разговоров, сумма небольшая.

3. Вам пришло СМС с известного сайта с поздравлением с выигрышем, так как именно вы стали тысячным посетителем. Какая удача! Чтобы получить заветный выигрыш — новый телефон, необходимо переслать на указанный в СМС адрес копию всех страниц своего паспорта. Как вы поступите?

а. Ура, я выиграл телефон! Конечно, перешлю копию паспорта.

б. Копия паспорта нужна, иначе как доказать, что я победитель? Не очень хочется пересылать, но телефон этого стоит.

в. Пересылать копию паспорта не буду. Просто так новые телефоны никому не раздают. А паспортными данными могут воспользоваться мошенники.

4. Вам ошибочно зачислили 300 рублей на телефон. Просят вернуть на указанный номер. Ваши действия?

а. Я честный, верну без разговоров.

б. *А почему не было СМС от сотового оператора о зачислении средств?*

в. Нет, явно деньги мне не поступали, свои отдавать не собираюсь.

г. Подумаю, но, скорее, верну. Вдруг я попаду в подобную ситуацию?

5. Вы решили проверить баланс своей карты через интернет. Зашли на страницу сайта банка, но на первый взгляд показалось, что сайт выглядит необычно: расплывчатый логотип, в строке браузера указано не название банка, а какое-то другое слово, не все ссылки открываются. Будете ли вы вводить логин и пароль для входа в систему?

а. *Не буду, так как есть риск отправить свои данные мошенникам.*

б. Введу, просто интернет барахлит.

в. Возможно, на сайте банка ведутся работы, ничего страшного, введу и логин, и пароль.

6. Как часто нужно менять пароли в онлайн-сервисах, чтобы не стать жертвой взлома?

а. каждые 2 месяца

б. каждые 6 месяцев

в. каждые 12 месяцев

7. Как выглядит безопасный веб-сайт?

а. он начинается с shttp://

б. *он начинается с https://*

в. он начинается с httpp://

8. Как проверить, безопасен ли сайт, на который вы зашли?

а. провести исследование

б. проверить наличие зеленого замка возле адресной строки

в. написать им письмо

9. В чем опасность скачивания бесплатного антивируса?

а. в таком антивирусе может быть ограничен функционал такой антивирус может быть не бесплатным

б. в нем может содержаться вирус, который отслеживает вашу деятельность

10. Что из этого мошенничество:

а. вам звонят, представляются сотрудником банка и спрашивают номер карты, срок ее действия и CVV-код

б. вам на почту приходит письмо от известного интернет-магазина, в котором предлагается перейти на его сайт

в. При попытке купить билеты в кино вас перенаправляютна сайт процессинговой компании

Оценка ответов:

10 правильных ответов – УРА! МЕШЕННИКАМ ТЕБЯ НЕ ОБМАНУТЬ!

8-9 правильных ответов – БУДЬ ОСТОРОЖЕН! ТЕБЯ МОЖНО ОБМАНУТЬ!

7 и менее правильных ответов – ТЫ ЛЕГКАЯ МИШЕНЬ ДЛЯ КИБЕРМОШЕННИКОВ! НЕОБХОДИМО ПОВЫСИТЬ ТВОЮ ФИНАНСОВУЮ ГРАМОТНОСТЬ!