КОМПЛЕКСНАЯ ПРОГРАММА ФОРМИРОВАНИЯ У ШКОЛЬНИКОВ ОСНОВ ЦИФРОВОЙ И ФИНАНСОВОЙ БЕЗОПАСНОСТИ

«Цифровой Я»

Материалы для проведения интерактивного урока

«Осторожно, кибермошенники!»

Время проведения: 40—45 минут.
Оптимальное число участников: 25—35 человек.
Виды деятельности: рассказ, обсуждение (обмен мнениями, выполнение заданий.
Задачи:
1. Дать ученикам первоначальные представления о финансовых мошенничествах в цифровом мире.
2. Познакомить с основными видами финансовых мошенничеств.
3. Обсудить необходимость защиты своих данных и финансовых инструментов.
4. Подвести детей к выводу о важности ответственного распоряжения финансами.
5. Учить детей работать с информацией, анализировать материал, принимать финансовые решения и оценивать свою работу.

Методические рекомендации
Методическая разработка рекомендуется для проведения урока «Мошенники в цифровом мире» в 5 – 11 классах. Класс может быть выбран на усмотрение организаторов.
Перед проведением урока организаторам урока, ученикам старших (8 – 11) классов, рекомендуется ознакомиться со структурой и содержанием разработки, а также проверить техническое оснащение кабинета.

Технические требования:
Компьютер, проектор, средство просмотра PowerPoint (или PDF).
Особенности воспроизведения презентации к уроку:
Основной этап урока построен в виде квеста и состоит из 4 контрольных вопросов.

Структура урока:

№	Этап (содержание)	Примерное время
1	Организационный	5 минут
2	Вводный (Актуальность проблемы, цифровизация мира, предпосылки увеличения числа мошенничеств, социальная инженерия)	10 минут
3	Основной (Мошенники в цифровом мире, телефонное и смс-мошенничество, фишинг, снифферинг, симминг)	25 минут
4	Завершающий (Подведение итогов, домашнее задание)	5 минут

Сценарий урока «Осторожно, кибермошенники!»

Организационный этап

ВЕДУЩИЙ

Здравствуйте, ребята!

Предлагаю вам стать участниками акции «Финансовая грамотность в цифровом мире».

Тема сегодняшнего урока – Мошенники в цифровом мире.

Задачей нашего сегодняшнего урока будет разобраться какие виды мошенничества развиты в цифровом мире и как от них защититься. (Слайд 2)

Вводный этап

ВЕДУЩИЙ

Для начала предлагаю понять, почему сегодня мы называем наш мир цифровым? (Слайд 3)

Посмотрите на схему развития цифрового общества. Какие главные тенденции в изменении мира вы наблюдаете?

Ответы учащихся.

ВЕДУЩИЙ

Действительно, цифровые технологии уже играют огромную роль в развитии человечества. Какое влияние на людей оказывает повсеместная цифровизация?

Ответы учащихся.

ВЕДУШИЙ

Представленный прогноз вам кажется реалистичным? Приведите аргументы, подтверждающие вашу точку зрения.

Ответы учащихся.

ВЕДУЩИЙ

С какими трудностями могут столкнуться люди в ближайшие два десятилетия?

Ответы учащихся.

ВЕДУЩИЙ

Цифровизация затрагивает все сферы жизни общества, и особенно ярко мы видим изменения в финансовой среде. (Слайд 4)

Подумайте и проанализируйте свои действия:

Имеете ли вы карманные деньги (или заработанные)? Как вы их храните?

При совершении покупок, вы используете наличные деньги или банковскую карту?

Совершаете ли вы покупки в интернете?

На что вы обращаете внимание при выборе онлайн магазинов?

Ответы учащихся.

ВЕДУЩИЙ

Ваши ответы – доказательство тому, что финансы действительно сосредоточены в цифровой среде. Пользоваться банковскими продуктами становятся проще. И здесь надо отметить, что цифровой мир непреднамеренно создаёт условия и для существования в нём мошенников.

Давайте рассмотрим причины увеличения числа мошенников в финансовой среде. (Слайд 5)

С развитием технологий мошенникам становится всё сложнее взламывать финансовые системы. Сейчас их задача «выудить» персональные данные у человека. Так работает социальная инженерия. (Слайд 6)

Обсуждение тезисов со слайда 6.

Основной этап

ВЕДУЩИЙ

Итак, давайте узнаем об основных видах современных мошенничеств. Мы пройдём квест: «Опасны ли вам финансовые мошенники?». (Слайд 7) После разбора каждого вида мошенничества вам будет предложен вопрос-ситуация, где нужно определить правильный

вариант действий. Что бы перейти к следующему пункту, необходимо правильно ответить на контрольный вопрос.
Итак, давайте посмотрим, с какими видами деятельности в цифровом мире может быть связана мошенническая деятельность. (Слайд 8)
Примеры, которые вы видите на слайде в большинстве своём представляют финансовые пирамиды. Вы наверняка про них слышали, но вероятно думали, что они остались в прошлом. К сожалению, это не так. Финансовые пирамиды тоже перешли в цифровой мир. К основным факторам их популярности относят анонимность организаторов и простоту запуска и рекламы. Для них главное создать сайт и придумать «легенду» проекта. Такие проекты всегда подстраиваются под общие тенденции. Например, в 2016-17 гг. они занимались торговлей криптовалютами.
Предлагаю рассмотреть ситуации. Что вам кажется подозрительным в каждой из них? На что бы вы обратили внимание в первую очередь?
Ответы учащихся.
ВЕДУЩИЙ
Отлично. Теперь предлагаю перейти к контрольной ситуации. (Слайд 9)
Учащиеся выбирают правильный ответ.
ВЕДУЩИЙ
Вы справились с первым контрольным вопросом, идём дальше. Один из самых распространённых видов – телефонное мошенничество. (Слайд 11)
Задача мошенников в этом случае – узнать у человека любым способом реквизиты его карты. Поступает звонок или приходит SMS-сообщение с предложением под разными предлогами сообщить нужные данные. Доверять звонкам с такими предложениями нельзя, ведь злоумышленники могут позвонить с любого номера вашей телефонной книги. Это позволяют сделать технологии IP-телефонии. Лучший способ проверить звонок со «знакомого» номера – перезвонить.
Также необходимо обращать внимание на подозрительные сообщения, например могут быть «кривые» номера и некорректная информация в тексте сообщения.
Давайте рассмотрим примеры ситуаций.
Кейс 1
Вам поступил звонок на мобильный телефон с незнакомого номера. В начале разговора человек называет своё имя и представляется сотрудником банка, в котором у вас есть открытые продукты. После этого он сообщает, что на ваш банк была совершена хакерская атака. Для того чтобы обезопасить ваши финансы, он предлагает сменить PIN-код на вашей карте. Для этого нужно назвать старый PIN-код и придумать новый. Как вы поступите?
Ответы учащихся.
Кейс 2
Вам пришло сообщение в одном из мессенджеров от вашей дальней знакомой, с просьбой проголосовать за её. Родственника, который участвует в конкурсе. В конце сообщения ссылка: http://Qbaozkx.ru. Как вы поступите?
Ответы учащихся.
ВЕДУЩИЙ
Вижу, что вы правильно размышляете. Переходим к контрольному вопросу. (Слайд 12)
Учащиеся выбирают правильный ответ.
ВЕДУЩИЙ
Хороший результат. Двигаемся дальше. Незнание гражданами основ безопасности в Интернете породило еще один вид мошенничества – фишинг. (Слайд 14)
Мошенники создают поддельный сайт (практически точную копию) с целью заполучить логины и пароли пользователей. В таком случае, поможет определить подлинность сайта, наличие защищённого соединения. Проверить его можно в адресной строке сайта. Во-первых, должна стоять иконка замка. Во-вторых, в используемом протоколе должна быть буква s – https://.

Помимо сайтов, мошенники производят рассылку спама на электронную почту. Почтовые серверы их стараются сортировать в отдельную папку, но иногда всё же ненужная рассылка может оказать в главной папке. На такие письме нельзя отвечать и переходить по ссылкам, указанным в них.

Посмотрите на слайд и прочитайте задание. Стали бы вы продолжать покупку?

Ответы учащихся.

ВЕДУЩИЙ

Верное решение. А как вы поступите в таком случае? (Слайд 15)

Учащиеся выбирают правильный ответ.

ВЕДУЩИЙ

Отлично, мы почти достигли цели. Осталось разобраться с наименее распространёнными, но тем не менее, опасными видами мошенничеств.

Первое явление – снифферинг. Опасность здесь представляют общественные wi-fi сети. При подключении к таким сетям не рекомендуется совершать финансовые операции. Дело в том, что при таком незащищённом соединении возможен перехват данных о банковской карте или электронном кошельке. А владелец может этого даже не заметить.

Представьте ситуацию: при встрече в кафе с друзьями вы заметили, что они все подключились к Wi-Fi сети. Подумайте, какие действия вы посоветуете друзьям не совершать, используя подобные сети? (Слайд 17)

Второе явление – дропперство, связано с переводами и обналичиванием денег. Суть его заключается в том, что банковские карты человека используют для мошеннических схем. Подросткам за вознаграждение предлагают обналичить денежные средства и передать «заказчику». Или при «случайном» переводе денег на карту, просят их вернуть.

Рассмотрите ситуацию. Вам на банковскую карту пришёл перевод от неизвестного человека на 15 000 рублей. Через несколько минут приходит такое сообщение. (Слайд 18)

Учащиеся выбирают правильный ответ.

ВЕДУЩИЙ

Отлично! Поздравляю, вы справились со всеми заданиями. Мошенникам будет сложно подобраться к вашим финансам. Но помните, мошенники постоянно придумывают новые способы обмана. Следите за новостями финансового мира.

Завершающий этап

Предлагаю подвести итоги урока. Наш вывод – совет: при подозрительных контактх всегда берите паузу, перед тем как что-либо сделать или сказать.

Продолжите фразы:

На уроке я узнал(а) …

На уроке я научился(ась) …

Это мне обязательно пригодится, когда я …

Учащиеся выполняют задание.

ВЕДУЩИЙ

Как вы считаете, все ли люди из вашего окружения знакомы с особенностями деятельности финансовых мошенников? В качестве домашнего задания предлагаю разработать чек-лист для проверки финансовой ситуации.

Необходимо разработать алгоритм проверки ситуации на возможные угрозы социальной инженерии. Используйте материалы всего урока.

Пользуясь различными средствами оформления представьте результат своей деятельности. Покажите его своим родственникам и друзьям.