Рекомендации по работе с презентацией тематического занятия «Финансовая безопасность» для обучающихся 8-10 классов

Цель: формирование у обучающихся базовых представлений о различных видах финансового мошенничества и основных правилах финансовой безопасности.

Задачи:

- сформировать убежденность учащихся в том, что финансовая грамотность и личная финансовая безопасность – основа финансового благополучия;
- заложить у старшеклассников установки грамотного финансового поведения, закрепить базовые финансовые понятия, предупредить о рисках;
- сформировать у школьников представление об основных видах финансового мошенничества и о способах противодействия им.

Методический материал носит рекомендательный характер; учитель, принимая во внимание особенности каждого класса, может варьировать задания, их количество, менять этапы занятия.

Слайд	Комментарий для учителя
 СЛАЙД 1	*Многие старшеклассники уже сейчас задумываются о взрослой жизни, о том, как выбрать хорошую профессию, реализовать свои планы и мечты. А для этого не в последнюю очередь важно достичь финансовой независимости и уметь грамотно обращаться со своими деньгами. Финансы окружают нас повсюду, и знать базовые правила их безопасного использования жизненно необходимо каждому из нас.* *По данным Национального агентства финансовых исследований 82% россиян владеют хотя бы одной банковской картой: чаще всего это карты для получения заработной платы (50%), реже – дебетовые (32%) и кредитные карты (20%), а также социальные карты (27%). Треть владельцев карт в России (31%) сталкивались с мошенничеством: это были попытки узнать конфиденциальные данные карты по телефону и просьбы предоставить данные для денежного перевода (например, для ложной помощи знакомым или оформления несуществующего выигрыша). Также держатели карт получали сообщения или письма с вирусами или вредоносными ссылками, сообщения о подтверждении или отмене операций по карте, которые они не совершали.* *Чаще других атакам мошенников подвергались россияне в возрасте от 25 до 34 лет (35%), люди, занимающие руководящие посты (41%). Реже о попытках*

СЛАЙД 2

СЛАЙД 3

мошенничества сообщали люди старшего возраста (26% против 31% в среднем среди возрастных групп), при этом они в целом пользуются картами менее активно. Способность распознать мошенничество свидетельствует о высоком уровне финансовой грамотности человека. Часть данных карты безопасно сообщать, например, сотруднику банка: это шестнадцатизначный номер карты, имя и фамилия держателя карты. Срок действия карты, а также трехзначный код с обратной стороны карты передавать никому нельзя.

Только 10% россиян, имеющих банковские карты, дали верные ответы на вопрос о том, какие данные карты можно сообщать сотруднику банка (номер карты, имя и фамилия держателя). Большинство россиян (63%) не готовы передавать никакие данные карт по телефону. Четверть россиян (27%) находятся в «группе риска»: они могут стать жертвами мошенников, поскольку готовы сообщить сотруднику банка по телефону данные карт, которые сообщать нельзя (срок действия, трехзначный код безопасности с обратной стороны, код из смс-сообщения).

Статистика РБК:

В России в период самоизоляции резко, на 76%, выросло число дел о телефонном и интернет-мошенничестве. Помимо фишинга злоумышленники использовали стремление россиян обеспечить себе дополнительный заработок или получить соцвыплаты.

За время действия ограничений, связанных с эпидемией коронавируса, в России резко выросло число зарегистрированных случаев мошенничества. Об этом свидетельствует статистика Генпрокуратуры, проанализированная РБК. При этом рост произошел исключительно за счет телефонного и интернет-мошенничества — за шесть месяцев 2020 года число случаев такого мошенничества выросло на 76% по сравнению с первым полугодием 2019 года.

Мошенничество — одно из самых частых совершаемых в России преступлений, чаще регистрируются только кражи. Если последних за время самоизоляции стало меньше на 9%, то случаев мошенничества в совокупности — значительно больше, на 36% (ст. 159–159.6 УК РФ).

По сравнению с прошлым годом в Санкт-Петербурге число зарегистрированных случаев мошенничества выросло вдвое, в Москве — на 76%, в Свердловской области — на 60%.

Источник: https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d

За 2020 год ФинЦЕРТ направил на блокировку операторам связи около 26,4 тыс. телефонных номеров, что превышает показатель предыдущего года на 86%, причем в большинстве случаев (71%) мошенники использовали городские номера, что создает большую иллюзию, что звонок поступает именно из банка или госучреждения.

Порядка 80% звонивших злоумышленников выступали якобы от лица представителей финансовых организаций, при этом использовались технологии

	подмены телефонных номеров. Это подтверждает почти четырехкратный рост количества заблокированных городских телефонных номеров в первом полугодии 2020 года. **<u>Задание 1</u>** Проанализируйте данные диаграмм и ответьте на вопросы. 1. Какие выводы можно сделать из информации, приведенной на слайде №2? 2. Кто из вас пользуется банковской картой? Знаете ли вы, какие данные карты допустимо сообщать другим людям? 3. Прокомментируйте данные диаграмм на слайде №3. 4. Нужно ли современному человеку учиться финансовой безопасности? 5. Что такое личная финансовая безопасность и почему она важна? 6. Как финансовая грамотность связана с финансовой безопасностью? Обоснуйте свой ответ.
 СЛАЙД 4	*Финансовая безопасность – понятие, включающее комплекс мер, методов и средств по защите экономических интересов государства на макроуровне, корпоративных структур, финансовой деятельности хозяйствующих субъектов на микроуровне. Из определения данного понятия мы можем выделить уровни финансовой безопасности:* • *Национальный, то есть финансовая безопасность всего государства;* • *Региональный – безопасность отдельных частей государства: республик, краев, областей, автономных округов и автономной области;* • *Корпоративный, то есть финансовая безопасность организаций;* • *Личный – финансовая безопасность отдельно взятого индивида, или личная финансовая безопасность.* *Личная финансовая безопасность – это социально-экономическая возможность человека, иметь финансовую независимость для удовлетворения своих материальных и духовных потребностей, как индивидуально, так и внутри общества, а также сохранение этой независимости в перспективе и её дальнейшее преумножение.* *Иными словами, финансовая безопасность личности означает независимость и стабильность – и именно поэтому так важно знать, как ее обеспечить каждому из нас.* *Финансовое мошенничество – это совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.* *Среди видов финансового мошенничества выделяют:* • *мошенничество с использованием банковских карт;* • *мошенничество в сети Интернет;* • *мошенничество с использованием мобильных телефонов;* • *мошенничество с финансовыми пирамидами;*

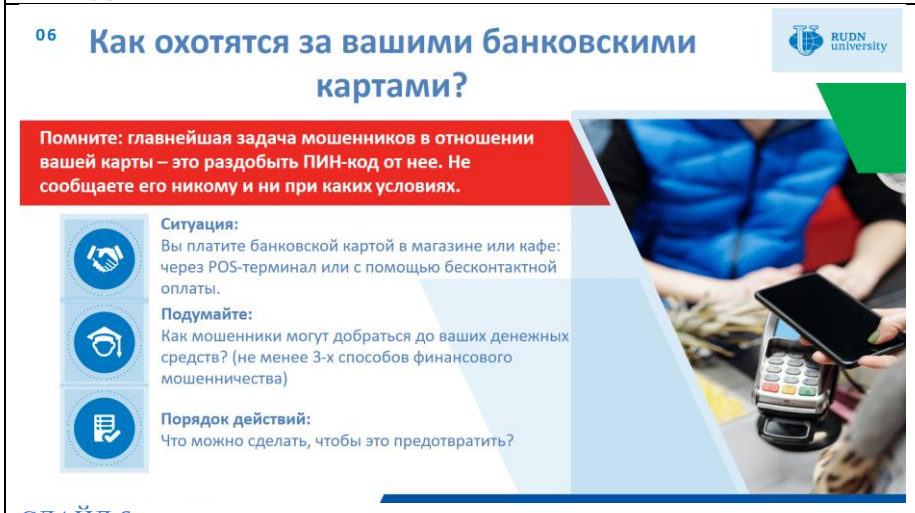
СЛАЙД 5

- *мошенничество на рынке Форекс.*

Задание 2

Внимательно изучите слайд №5 и ответьте на вопросы:

1. Как вы думаете, что подразумевается под приведенными видами финансового мошенничества?
2. Приведите примеры каждого из видов мошенничества.
3. Можете ли вы назвать еще какие-либо виды финансового мошенничества, помимо представленных на слайде?



СЛАЙД 6

1. *Мошенничество с банковскими картами бывает различных типов, среди которых можно выделить:*

- *«Магазинные мошенничества» – данные карты могут быть считаны, сфотографированы или иным образом зафиксированы ручным скиммером, сама карта может быть украдена. Данный вид мошенничества также распространен в отношении банковских карт с функцией бесконтактной оплаты: с помощью специального терминала, прислоненного к карману или сумке жертвы, мошенники могут украсть денежные средства с карты.*
- *Траппинг – на банкомат устанавливаются устройства, которые блокируют карту. На помощь человеку приходит мошенник, который подглядывает ПИН-код и после ухода человека достает карту из банкомата.*
- *Фишинг – рассылка электронных писем о якобы производимых изменениях в системе безопасности банка. Мошенники просят дать информацию о карте, в том числе указать номер кредитки и ее ПИН-код, отправив ответное письмо или заполнив анкету на сайте, похожем на сайт банка-эмитента.*
- *Вишинг (голосовой фишинг) – сбор информации о номерах карт и счетов при помощи моделирования звонка автоинформатора.*
- *Звонки мошенников с просьбой погасить задолженность по кредиту, в ходе разговора пытаются выяснить данные банковской карты. Банки не присылают писем и не звонят на телефоны своих клиентов с просьбой*

предоставить им данные счетов. Если такая ситуация произойдет, вас попросят приехать в банк лично.

Как противостоять?

- ✓ *Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому и не вводите ПИН-код при работе в Интернете. Помните, что ПИН-код не может быть затребован ни банком, ни любой другой организацией ни при каких условиях.*
- ✓ *Сохраняйте документы до окончания проверки правильности списанных сумм*
- ✓ *Сообщайте банку актуальные контактные данные. Если у банка будут устаревшие данные, он не сможет оперативно связаться с вами для подтверждения подозрительных операций или при возникновении спорных ситуаций.*
- ✓ *Всегда имейте при себе телефон службы поддержки держателей карт вашего банка — это позволит вам оперативно получать информацию о состоянии вашей карты и решать все возникающие при использовании карты вопросы.*
- ✓ *Перед снятием денег в банкомате осмотрите его. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.*

Задание 3

Решите ситуационную задачу.

Место действия: магазин или кафе

1. Вы платите обычной банковской картой

Злоумышленником может оказаться работник сферы торговли и услуг. Официант, кассир или продавец, принимая для расчета вашу банковскую карту, может сфотографировать нужные данные (номер карты, срок действия, имя владельца и код на обратной стороне), а после расплатиться ей в интернете.

Как предотвратить?

Рассчитываясь, постарайтесь не упускать из вида свою карту. И вводите ПИН-код так, чтобы он не был виден посторонним.

2. Вы платите через терминал, но оплата не проходит

В кафе официант приносит вам POS-терминал (на картинке), вы расплачиваетесь, но тут официант говорит, что оплата не прошла, и просит повторно ввести ПИН-код. Делая это, вы рискуете заплатить дважды.

Как предотвратить?

Подключите смс-уведомления о платежах. Обязательно попросите чек с уведомлением о сбое или отказе от операции (POS-терминал всегда печатает такой).

	3. Вы платите картой с системой бесконтактной оплаты Картами с системой бесконтактной оплаты можно расплачиваться мгновенно, в одно касание, если ваш платеж не превышает определенный лимит. ПИН-код при этом вводить не нужно. Злоумышленники могут похитить деньги с такой карты, прислонив считыватель или POS-терминал к сумке. <u>Как предотвратить?</u> Чтобы бесконтактная оплата не проходила без вашего ведома, карту лучше хранить в экранирующем отсеке кошелька, сумки или специальном чехле для банковских карт.
 СЛАЙД 7	*Скимминг – это вид финансового мошенничества; предполагает установку специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте. Это устройство копирует данные с магнитной полосы карты. Могут украсть и ПИН-код, установив на банкомат скрытую камеру или накладную клавиатуру. Поддельную клавиатуру ставят прямо поверх оригинальной, и сам банкомат реагирует на нажатия как обычно — человек даже не заметит, что что-то идет не так. Злоумышленники, используя украденные данные, могут изготовить копию карты.* *<u>Как не стать жертвой скиммеров:</u>* ✓ *Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.* ✓ *Перед пользованием банкоматом внимательно осмотрите его на предмет наличия посторонних предметов; клавиатура не должна шататься.* ✓ *В случае потери карты или утраты ПИН-кода немедленно обратитесь в ваш банк для ее блокирования.* ✓ *Подключите услугу SMS- уведомлений, это позволит вам оперативно получать информацию о проводимых по вашей карте операциях: оплате товаров/услуг, просмотре баланса в банкомате, снятии наличных. Следите за тем, чтобы в выписке, SMS-уведомлениях или мобильном приложении были отражены ваши реальные операции. Если вы заметили несоответствие — обратитесь в банк.* ✓ *Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.* ✓ *При бесконтактной оплате банковской картой или с помощью технологии NFC для смартфонов придерживайтесь лимитов, при превышении которых требуется ПИН-код для подтверждения транзакции (в России такой лимит составляет 999 рублей, все более крупные денежные операции требуют подтверждения ПИН-кодом). Кроме того, пользователям бесконтактной оплаты стоит ограничить размер ежедневных, еженедельных или ежемесячных расходов с учетом личного бюджета, связавшись с банком, осуществляющим обслуживание карты.* **Задание 4**

СЛАЙД 8

Изучите информацию на слайде и ответьте на вопросы:

- ✓ Пользуетесь ли вы банковскими картами? Если да, то как часто?
- ✓ Слышали ли вы ранее о таком способе мошенничества как скримминг?
- ✓ Как, по вашему мнению, можно защититься от такого вида финансового мошенничества?
- ✓ Изучите информацию на слайде №8. Обсудите: знали ли вы о необходимости осматривать банкомат перед использованием?

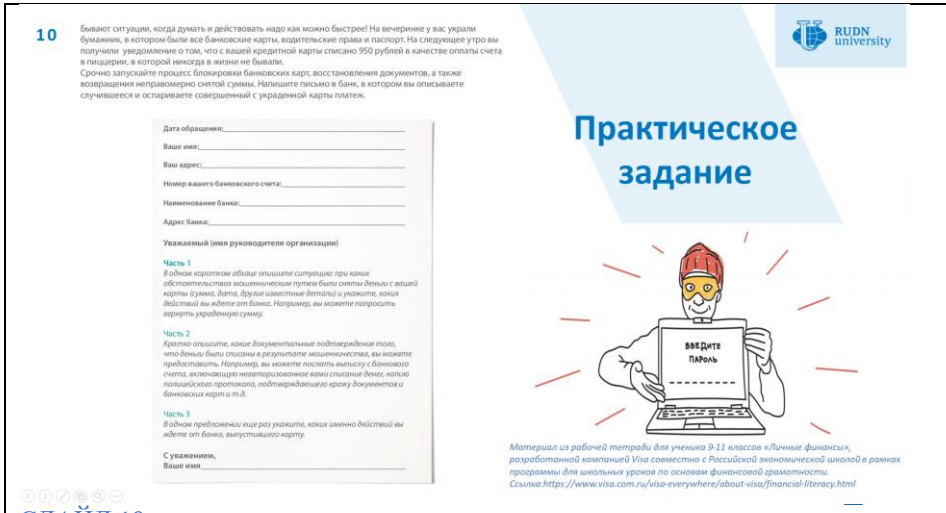
СЛАЙД 10

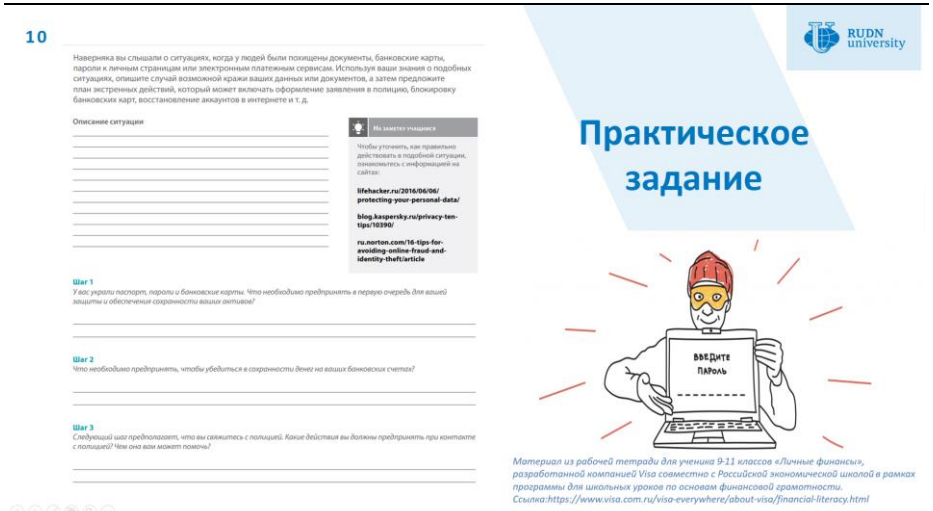
Задание 5. Практическое задание

1. Случалось ли вам или вашим родным терять банковскую карту? Предложите порядок действия в такой ситуации. Сравните предложенный вами порядок с представленным на слайде №9. Все ли варианты действий были названы?
2. Изучите ситуацию, представленную на слайде №10. По образцу напишите письмо в банк, в котором вы описываете случившееся и оспариваете совершенный с украденной карты платеж.

ПРИМЕЧАНИЕ:

- ***Практическое задание на слайде №10 представлено в двух вариантах: педагог может выбрать один из них, либо выбрать оба, учитывая особенности своих классов / групп обучающихся.***
- ***Практическое задание, приведенное на слайде №10, педагог может раздать обучающимся в печатном виде. Раздаточный материал для распечатки можно найти в Приложении №1 и Приложении №2 к Методическим рекомендациям по подготовке и проведению Всероссийского тематического урока на тему «Финансовая безопасность» (стр. 14-15).***

<table>
<tr>
<td>


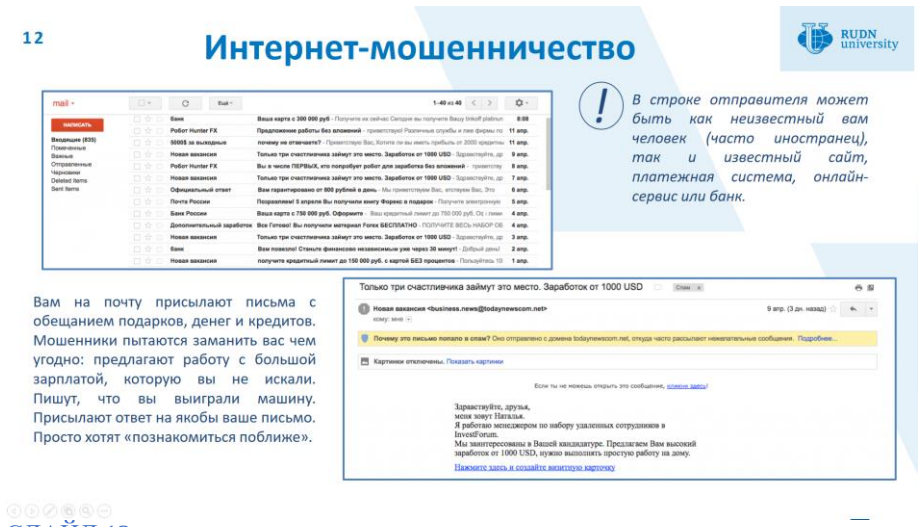
СЛАЙД 10


СЛАЙД 10
</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Среди типов финансового мошенничества в Интернете можно назвать:

Покупки через интернет. Продавец просит оплатить товар через систему денежных переводов, используя фальшивое или недействительное удостоверение личности. Получая деньги, он исчезает.

</td>
</tr>
</table>

СЛАЙД 11



СЛАЙД 12

- *Составление гороскопа. Пользователю предлагается заполнить анкету, после чего на электронный адрес отправляется не сам гороскоп, а письмо с указанием отправить по указанному номеру СМС-сообщение. Стоимость такого сообщения может составлять несколько сотен рублей.*
- *Письма платежных систем, к которым прилагается вирус, замаскированный под вложение – файл или ссылку. Его задача – собрать данные о ваших аккаунтах в платежных системах и данные банковских карт.*
- *Нигерийские сюжеты. Некое высокопоставленное лицо из африканской страны просит помочь в выводе значительной суммы денег за процент. При этом клиента просят перечислять незначительные суммы для оформления перевода и других действий, пока клиент не осознает, что его обманули.*

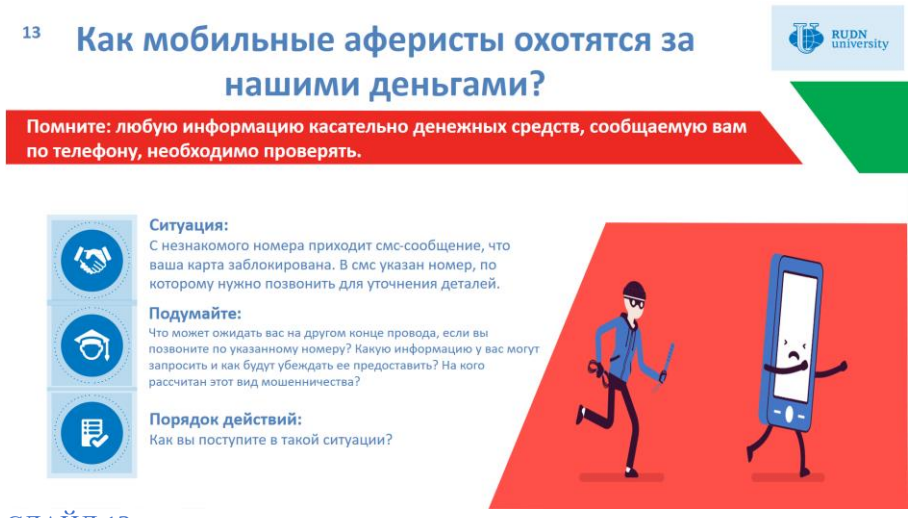
Способы защиты:

- ✓ *Не открывайте сайтов платежных систем по ссылке в письмах, проверяйте URL в адресной строке, посмотрите, куда ведет ссылка. Даже если ссылка кажется надежной, всегда сверяйте адреса с доменными именами официальных сайтов организаций*
- ✓ *Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах.*
- ✓ *Не сообщайте ваши пароли, вводите их только на сайтах платежных систем.*
- ✓ *Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации, делайте несколько копий таких файлов.*
- ✓ *Не оплачивайте никаких взносов, при трудоустройстве на удаленную работу.*
- ✓ *Установите на компьютер антивирус — и себе, и родственникам.*
- ✓ *Всегда обращайте внимание на адресную строку браузера: на сайте-клоне будет допущена ошибка.*
- ✓ *Оплачивайте покупки только через сайты с защищенным соединением и значком платежной системы.*
- ✓ *Внимательно изучите и содержание сайта — злоумышленники часто невнимательно относятся к наполнению сайта.*
- ✓ *Добавьте в закладки сайты, которыми часто пользуетесь, чтобы не набирать адрес вручную — так вы не ошибетесь в названии и попадете на нужный вам сайт.*

Задание 6

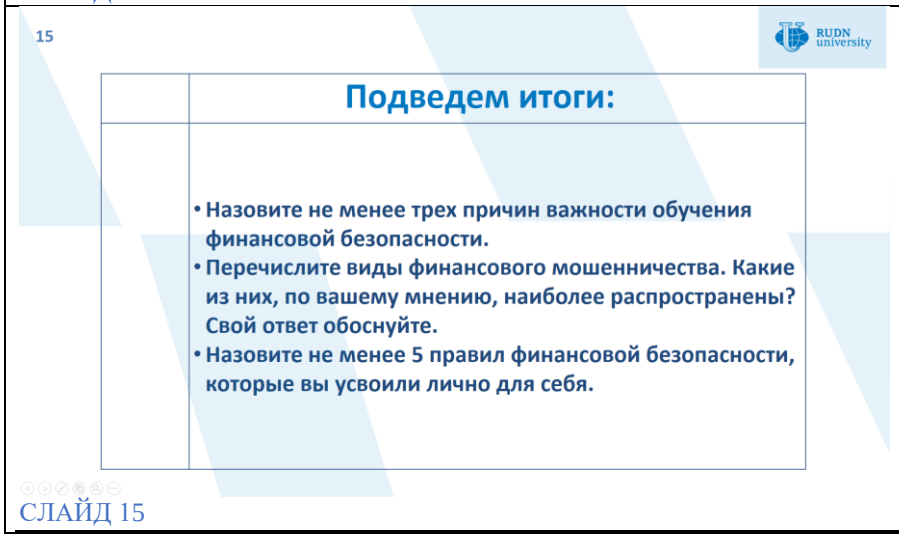
Изучите информацию на слайде.

1. Как часто вы совершаете покупки в Интернете?

	2. Считаете ли вы разумными правила, предложенные на слайде №11? Обоснуйте свой ответ. 3. Случалось ли вам получать электронные сообщения от мошенников? Можно ли открывать такие сообщения? Как не стать жертвой мошеннических писем в электронной почте?
 СЛАЙД 13	*Мобильные мошенничества – характеризуются либо использованием распространенных сюжетов-клише, с помощью которых можно заставить жертву совершить определенные действия, либо специализированных технических средств:* • *«Вы выиграли приз». Мошенник привлекает жертву дорогим подарком, который он «выиграл», или звонит с предложением получить компенсацию за приобретенные ранее БАДы, денежный выигрыш, потерянные при обмене денег сбережения и т. п. При этом просит прислать подтверждающую СМС, внести регистрационный взнос и т.п. Получив деньги, мошенник исчезает.* • *«Мама, я попал в аварию». Мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета мошенников.* • *«Ваша карта заблокирована». На мобильный телефон приходит соответствующее СМС-сообщение с указанием телефона для разблокировки, по которому мошенник предлагает жертве совершить несколько операций с банкоматом под диктовку. Деньги с карты перейдут на счет мошенников.* • *Вирус. Он помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.* *<u>Чтобы не стать жертвой мобильных аферистов:</u>* ✓ *Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов.* ✓ *При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию.* ✓ *Не отправляете СМС на короткие номера, заранее не узнав его стоимости.* ✓ *Не сообщайте никаких персональных данных. Попросите представиться, назвать ФИО, звание должность, наименование организации, узнайте телефон этой организации в справочных базах и перезвоните.* ✓ *Если вам сообщают, что ваш родственник или знакомый попал в беду и за него нужно внести деньги - позвоните ему напрямую.* ✓ *Ценную информацию не храните только в телефоне, дублируйте ее в бумажном блокноте или в компьютере.* **Задание 7** 1. Изучите ситуационную задачу на слайде №13 и ответьте на вопросы.

СЛАЙД 14

2. Обоснуйте, почему представленная на слайде №14 информация полезна.



СЛАЙД 15

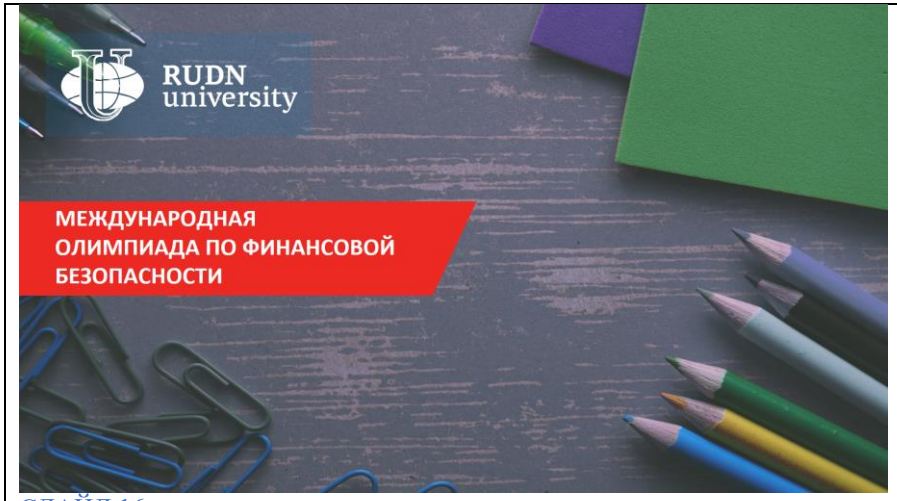
Задание 8. Подведение итогов

Посмотрите обобщающее видео.

1. Назовите не менее трех причин важности обучения финансовой безопасности.
2. Перечислите виды финансового мошенничества. Какие из них, по вашему мнению, наиболее распространены? Свой ответ обоснуйте.
3. Назовите не менее 5 правил финансовой безопасности, которые вы усвоили лично для себя.

Ознакомление обучающихся с возможностью принять участие в Международной олимпиаде по финансовой безопасности.

ПРИМЕЧАНИЕ: Слайд №19 представлен в восьми различных вариациях – для каждого федерального округа. Учитель должен ознакомить учащихся с информацией о площадках проведения отборочного этапа соответствующего округа, удалив лишние слайды №19.



СЛАЙД 16

СЛАЙД 17

18

Маршрут Олимпиады

- ✓ Всероссийский урок по финансовой безопасности
  - o I этап Олимпиады (вузовский, отборочный)
  - o II этап Олимпиады (финальный)

I ЭТАП ОЛИМПИАДЫ (отборочный)

- проводится на площадках вузов – участников Международного сетевого института в сфере ПОД/ФТ
- участники – обучающиеся 8-10 классов и студенты российских вузов
- срок проведения – с 17 по 21 мая 2021 года
- победители получают право участия во II этапе Олимпиады

II ЭТАП ОЛИМПИАДЫ (финальный)

- проводится на федеральной территории «Сириус» (г. Сочи, Россия)
- срок проведения – с 3 по 9 октября 2021 года

СЛАЙД 18

19

Отборочный этап (Центральный федеральный округ)

Субъекты	Университет	Направления олимпиады
Москва Московская область Белгородская область Брянская область Владимирская область Воронежская область Ивановская область Калужская область Костромская область Курская область Липецкая область Московская область Орловская область Рязанская область Смоленская область Тамбовская область Тверская область Тульская область Ярославская область	Российский университет дружбы народов	Обществознание и право
	Национальный исследовательский ядерный университет «МИФИ»	Математика и информатика (IT, программирование и искусственный интеллект)
	Российский экономический университет имени Г.В. Плеханова	Экономика

СЛАЙД 19


Приглашаем принять участие:
• российских школьников и студентов,
• а также студентов образовательных организаций – участников Международного сетевого института в сфере ПОД/ФТ из Беларуси, Казахстана, Кыргызстана, Таджикистана, Туркменистана, Узбекистана
RUDN university
Более подробная информация:
www.fedsfm.ru - Росфинмониторинг
www.mumcfm.ru – МУМЦФМ
www.rudn.ru - РУДН
E-mail: olimpiada@mumcfm.ru

СЛАЙД 20