**В МБОУ Лысогорской СОШ проведен тематический урок финансовой грамотности в 8 и 10 класах.**

**Цель :** выработка личной стратегии грамотного поведения в ситуации мошеннических действий.

**Задачи:**

1. Дать определение понятию «мошенничество»

2. Рассмотреть основные виды мошенничества и методы финансовых мошенников

3. Выявить «зоны риска» встречи с финансовыми мошенниками

4. Выстроить собственную линию поведения, чтобы не стать жертвой мошенников.

**Предметные образовательные результаты:**

- дать определение финансового мошенничества,

- изучить наиболее распространенные виды финансовых мошенничеств: фишинг, скимминг, смишинг и др.

- выработать способы защиты от мошенничества.

**Метапредметные:**

- уметь самостоятельно определять цель и составлять план деятельности,

- владеть навыками учебно-исследовательской деятельности, разрешения проблем,

- уметь работать в группе.

**Личностные:**

- знать причины возникновения финансовых рисков,

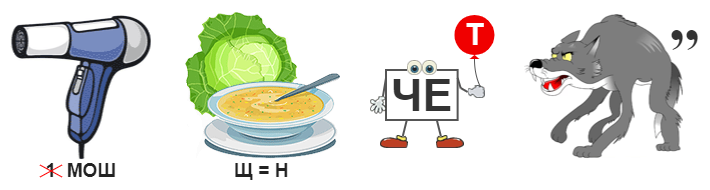
- уметь проверять поступающую из различных источников информацию,

- соблюдать осторожность в финансовой сфере.

**Организационный момент (приветствие)**

**Актуализация знаний**

Ребята! Вашему вниманию предлагается ребус. После того, как его разгадаете, вы узнаете, о чем пойдет речь сегодня на классном часе.



мошенничество.

Сегодня мы поговорим о мошенничестве.

Знаете ли вы, кто такие мошенники?

Сталкивались ли вы или ваши родственники с мошенническими действиями. Если да, то с какими?

**Ответы учащихся.**

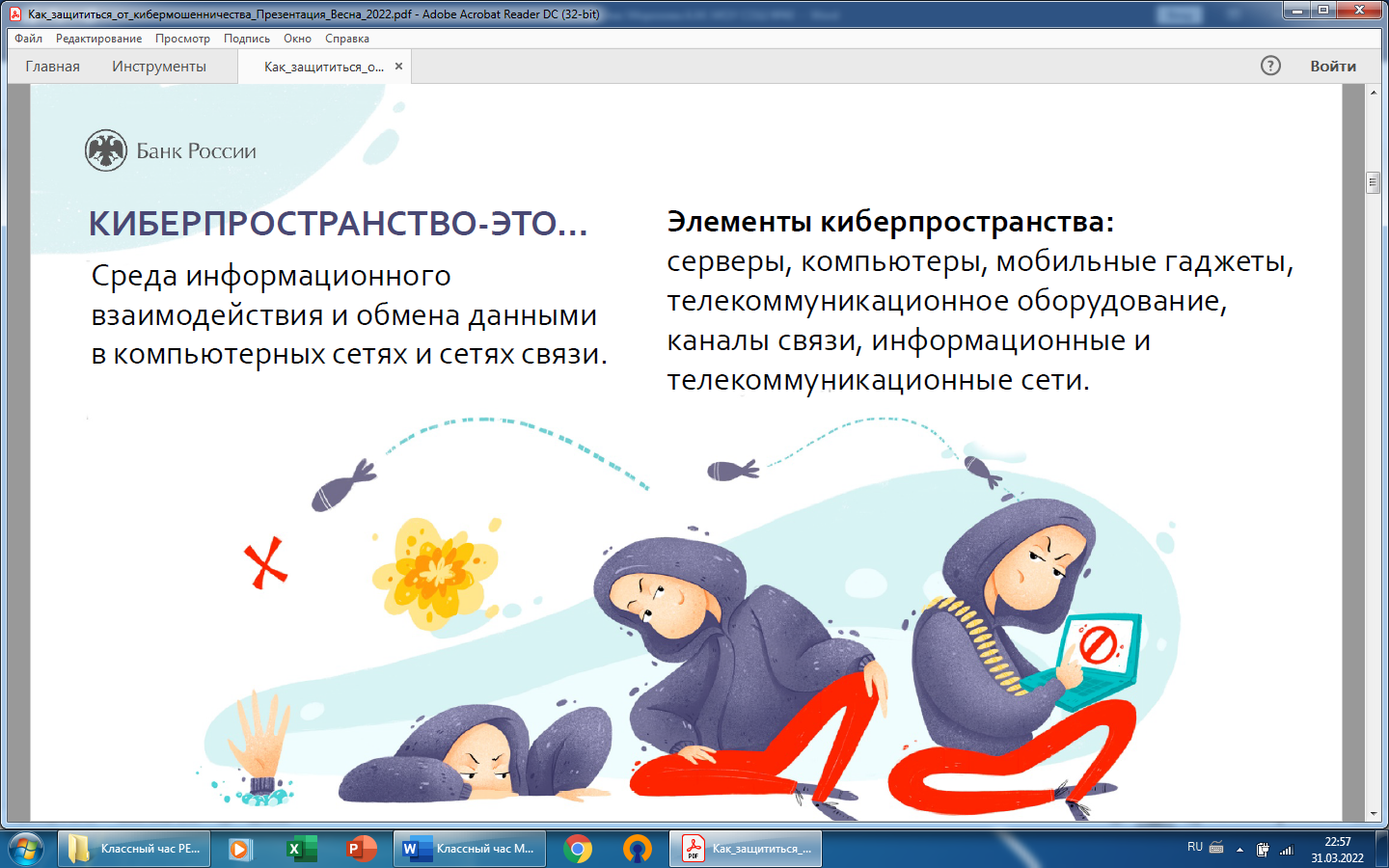
**Постановка цели и выработка задач занятия – с опорой на документ (см. ссылку)**

<http://www.consultant.ru/document/cons_doc_LAW_10699/8012ecdf64b7c9cfd62e90d7f55f9b5b7b72b755/>

**Финансовое мошенничество** — совершение противоправных действий в сфере денежного обращения путём обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

Существует много видов мошенничества. На сегодняшний день наиболее распространены мошеннические действия в киберпространстве. Кто скажет, что такое киберпространство?

**Ответы учащихся.**

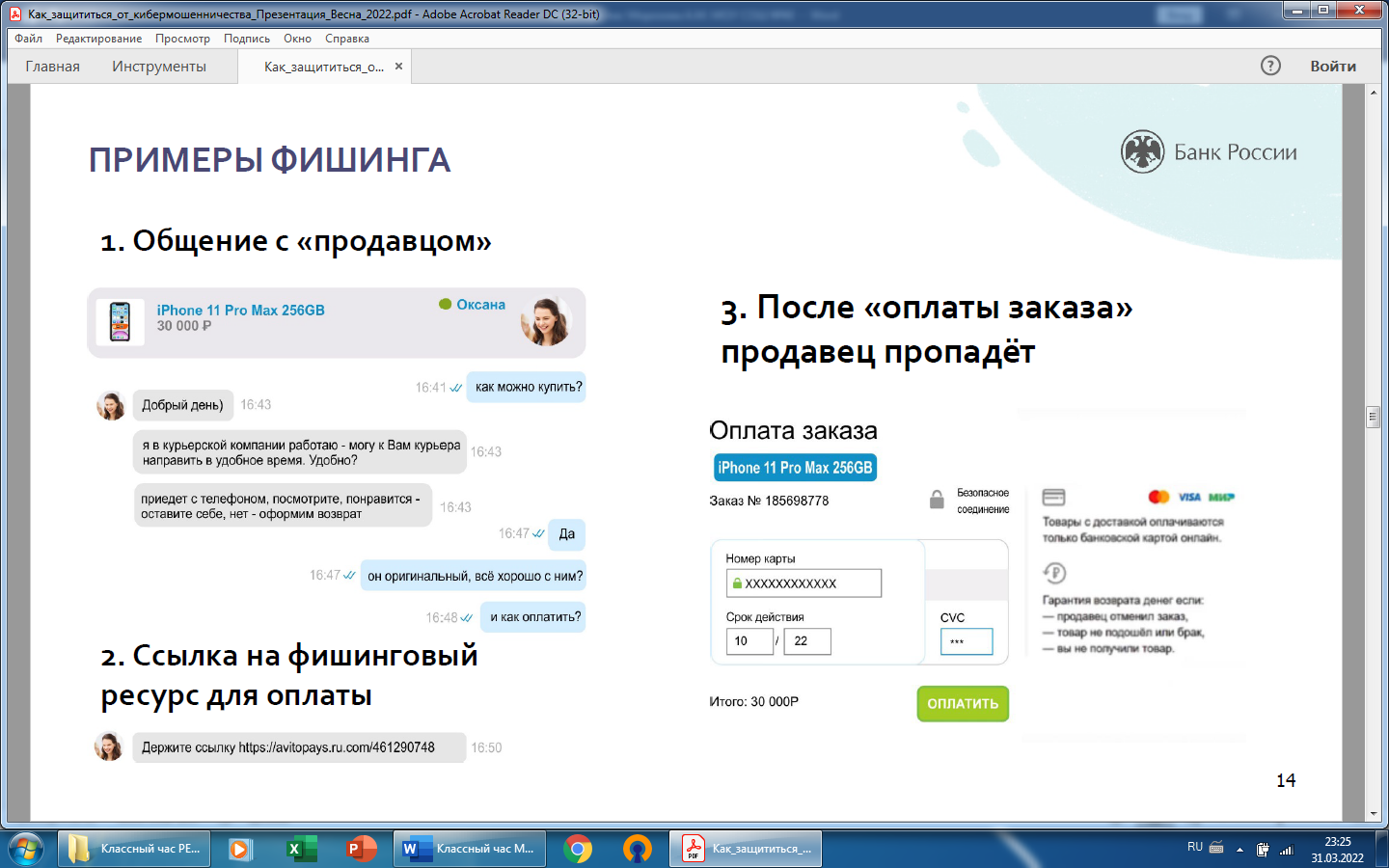


**Реализация**

Какие виды мошенничеств в интернете вы знаете? Может быть, кто-то из вас уже сталкивался с чем-то подобным?

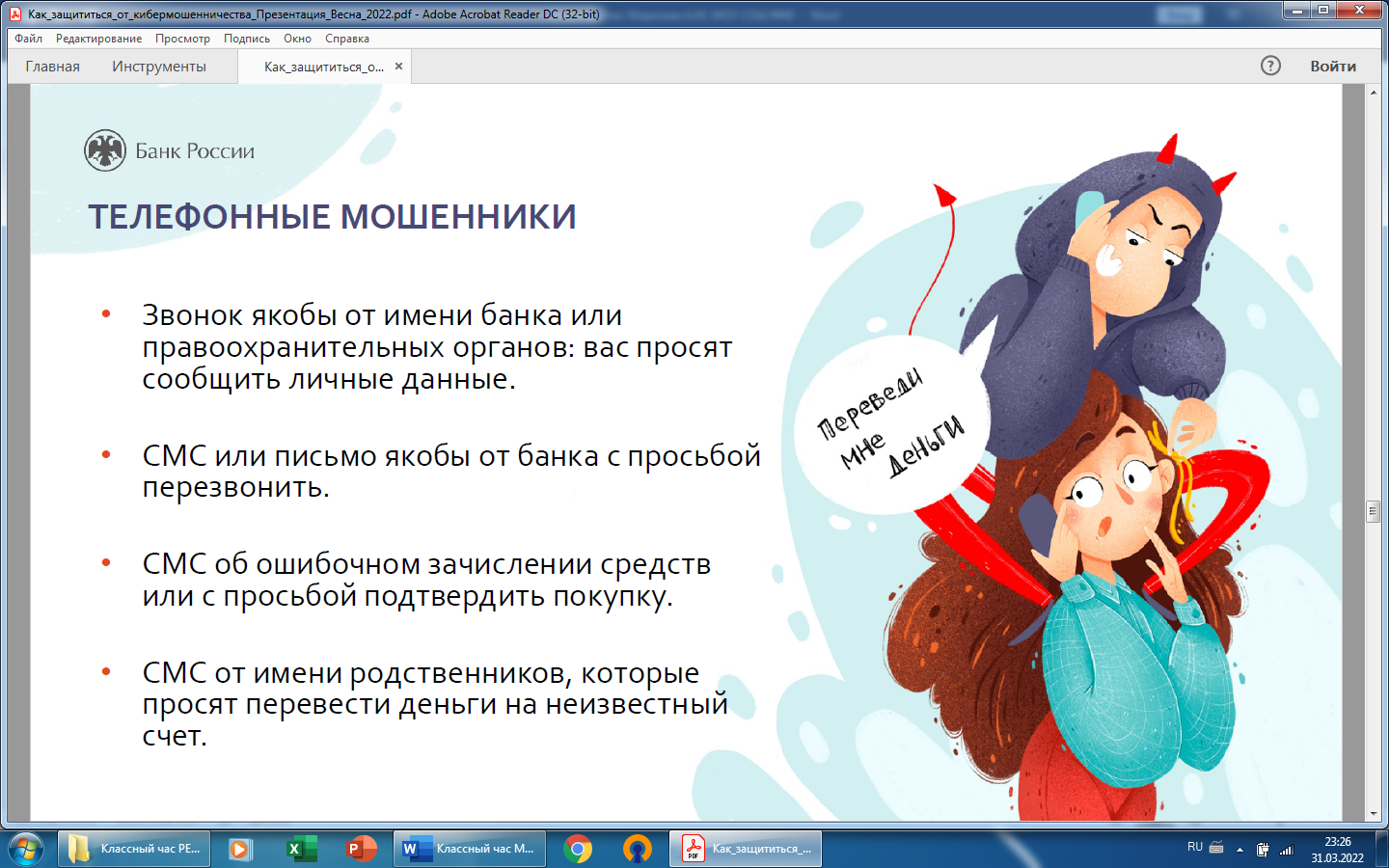
Классный руководитель принимает **ответы от учащихся**. При необходимости может дополнить их из списка ниже. Данный список не исчерпывает все возможные варианты ответов: классный руководитель должен самостоятельно определить являются ли варианты, предложенные школьниками, правильными.

1. **Фишинг** – получение персональных данных любым доступным способом. В основном, используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих. Вам могут прислать письмо якобы от вашего банка или почтового сервера, которым вы пользуете, и сообщить, что произошли какие-то изменения (вас добавили в черный ящик, заблокировали карту, кто-то завладел вашим паролем и т.п.). При клике на ссылку вы переходите на сайт, которые внешне почти ничем не отличается от сайта реальной компании, но если присмотреться, то можно заметить отличия. Например, использовано старое изображение логотипа, и в адресной строке вместо реального названия сайта банка другие вариации его написания (не «online.sberbank.ru», а «onllinesberbank.ru», без точек в одно слово). Вы переходите на такой сайт, вводите ваши персональные данные, и они оказываются у мошенников, которые затем крадут деньги с банковской карты.



2. **Смишинг** - выманивание данных карты мошенниками при обращении в социальных сетях. К вам обращаются от лица вашего друга или родственника, взломав его страницу, и просят одолжить деньги или сказать код-пароль, который пришел в sms на ваш телефон.

3. Также есть такие мошенники, которые звонят пожилым людям и разыгрывают спектакль, что якобы их дети или внуки попали в аварию и просят передать через 3-е лицо крупную сумму денег, иначе им не сделают вовремя медицинскую операцию или посадят в тюрьму.

Давайте прямо сейчас проверим, легко ли вас обмануть по телефону? Предлагаю всем пройти тест:

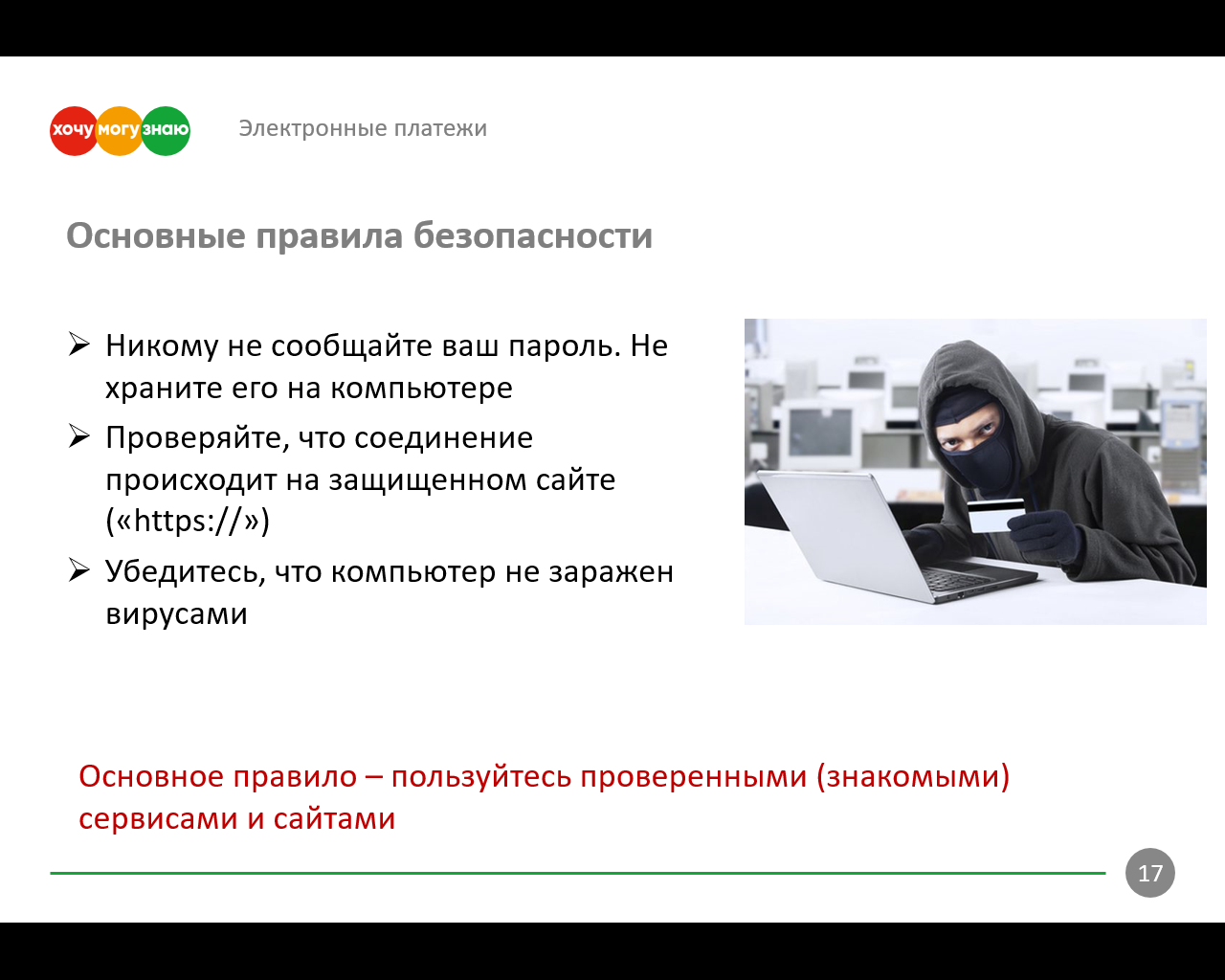
<https://news.rambler.ru/community/42231690-test-legko-li-vas-obmanut-po-telefonu/>

Надеюсь, что к окончанию классного часа, людей, которых оказалось обмануть легко, вовсе не осталось.

3. Ненадежные интернет-магазины. Мошенники могут создать сайт несуществующего интернет-магазина (или скопировать реальный сайт). Вы оплачиваете свои покупки, а товар не получаете.

4. Мошенничества на сайтах объявлений продажи товаров (типа «Авито»). Вы выставляете на сайте объявление о продаже товара. С вами связывается «Покупатель» и просит сообщить ему данные карты (код CVV2/CVC2, срок действия, ФИО владельца), чтобы зачислить на нее деньги.

Учитель напоминает школьникам, что за безопасность средств на своей банковской карте, в первую очередь, отвечают они сами. Если по неосторожности разгласить важную информацию о своей карте, то банк, скорее всего, не будет возмещать средства, поэтому нужно быть бдительным и помнить о правилах безопасности.



5. **Скимминг** – вид мошенничества, при котором третьи лица завладевают электронными данными карты и пин-кодом с помощью технических приборов, расположенных на банкомате (накладная клавиатура, накладка на картоприемник и прочее).

Как вы думаете, на что следует обращать внимание при пользовании банкоматом?

**Ответы ребят:** следует проверить нет ли в банкомате дополнительных накладок.

- Убедитесь в исправности банкомата. Если по каким-то признакам, вы видите, что банкомат работает неисправно, не рискуйте. Неисправный банкомат может задержать вашу банковскую карту/провести операцию и не выдать наличные и т.п.

- Посмотрите, нет ли такой накладки на отверстие, в которое вставляется карта. При установке своих устройств мошенники должны спешить и могут оставить следы: щели, клеевые подтеки и сколы. Лишние панели, криво прикрепленные детали.

Мошенники делают панели, монтируют в них видеокамеры для записи момента ввода ПИН-кода, а потом незаметно крепят к банкомату: на лотки для рекламы, под козырек, под экран.

Отличающаяся по тону или текстуре деталь.

Если банкомат старый, со сколами и затертыми панелями, а какая-то деталь (например, клавиатура) выглядит как новая — это плохой знак. Также подобрать краску для поддельных деталей тон-в-тон довольно сложно.

- Не забудьте забрать ваши деньги и банковскую карту. Современные банкоматы могут задержать ваши деньги и карту, если вы не успели их забрать в течение определенного времени.

- Проверьте, нет ли рядом подозрительных личностей, которые могут подсмотреть ваш пин-код, отнять карту и так далее, лучше отложить задуманные вами действия с картой и провести их в более безопасном месте.

В настоящее время при оплате банковской картой терминал не всегда запрашивает у вас ввести пин-код от карты (это зависит от настроек самого терминала), поэтому если вы ее потеряете, мошенники смогут совершать покупки в некоторых магазинах. Чтобы деньги на банковской карте были в безопасности, с картой надо обращаться аккуратно. Надо позаботиться, чтобы карта вместе с ПИН-кодом не могла попасть в чужие руки. Поэтому его нельзя записать на листочке и хранить в том же кошельке, что саму карту. Лучше всего хранить его только в памяти, а это непросто, если карт у вас несколько.



В любой ситуации, когда данные вашей карты или она сама могут оказаться в руках мошенников, следует обратиться в банк и заблокировать карту. В случае неисправной работы терминалов оплаты или банкоматов, из-за чего у вас возникли проблемы, также нужно обращаться в ваш банк.

К сожалению, данные клиентов банков могут попасть в чужие руки. Поэтому в разговоре мошенники могут очень убедительно представляться сотрудниками банка, «подтверждая» свой статус информацией, которой они знать не должны.

Способы выманивая информации у держателей карт меняются и становятся все изощреннее – иногда может казаться, что информацию, которую вас просят сообщить, безобидна. Наилучший вариант - не рассказывать ничего, как можно быстрее связаться с банком самостоятельно, для надежности заблокировать карту, часть данных о которой уже стала известна злоумышленникам.

А теперь я предлагаю вам поработать в группах, чтобы на практике понять, с каким видом мошенничества вы столкнулись и найти пути выхода из сложившейся ситуации.

для ввода данных карты. Не раздумывая, Катя сделала все необходимое. После этого с ее карты начали списываться деньги. Что нужно сделать Кате?

Правильный ответ: не переходить по ссылке и не вводить никаких данных. Проверить состояние карты или ее заблокировать через интернет-банк или позвонить в банк.

Катя пострадала от «фишинга» (разнообразные приемы для получения данных пользователей).

определенную сумму денег за его вызволение. В последнем случае суммавыкупа может исчисляться десятками тысяч рублей. Ваши действия?

Правильный ответ: не предпринимать никаких действий, лично не убедившись, что ваш родственник или знакомый точно попал в затруднительную ситуацию. Самое простое – просто позвонить ему.

«Какие самые новейшие «разработки» мошенников вам известны?»

**Возможные ответы:** приехать на дом и сделать прививку от коронавируса.

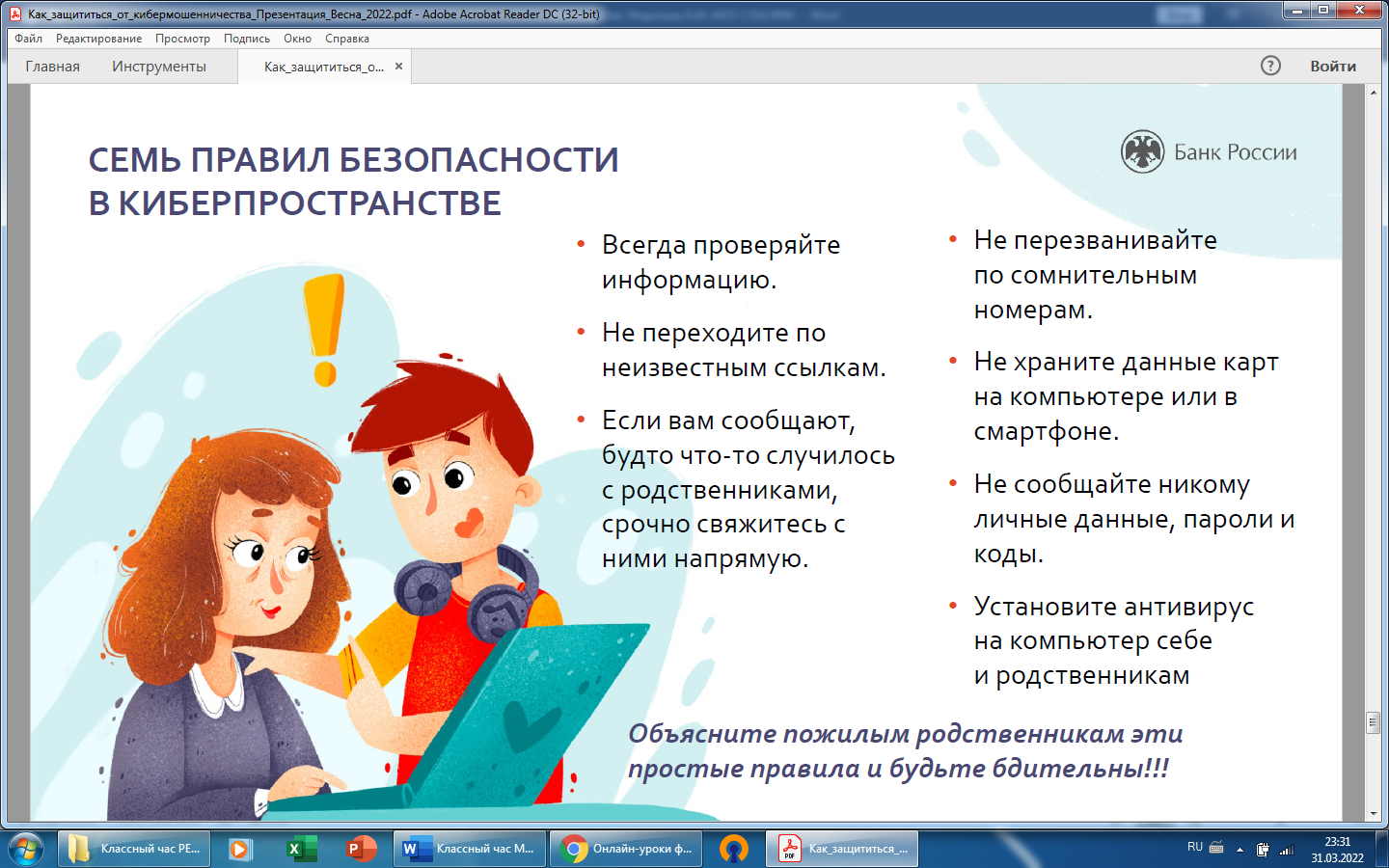
Давайте все вместе разработаем правила, которые помогут нам не стать жертвами мошенников.

**Основные правила безопасности:**

1. Никогда никому не сообщать свой пароль, включая сотрудников платежных систем. Никогда не сохранять информацию о своем пароле на любых носителях, в том числе и на компьютере. Если есть подозрения, что кто-либо получил доступ к личному кабинету, сменить пароль или заблокировать свой счет/аккаунт.

2. Проверить, что соединение действительно происходит в защищенном режиме SSL. При использовании технологии шифрования данных адрес сайта начинается на «https://», а не «http://». В правом нижнем углу вашего браузера должен быть виден значок закрытого замка. Нельзя вводить данные карты на сомнительных сайтах

3. Убедиться, что компьютер не поражен какими-либо вирусами. Установить и активизировать антивирусные программы. Стараться их постоянно обновлять, так как действие вирусов может быть направлено на передачу третьим лицам информации о вашем пароле.



**Если вдруг случилась беда, куда обращаться за помощью?**

Нужно идти в отделение полиции с паспортом, сообщить дежурному о факте мошенничества и написать заявление.

**Подведение итогов**

**Будьте внимательны, мошенники с каждым годом становятся все изощреннее в своих способах отъема денег. Наивно полагать, что они способны обхитрить только пожилых людей или несовершеннолетних детей. В их арсенале полно уловок! «Ключики» можно подобрать и к молодой маме, и к студенту, и к зрелому мужчине. Главное, не поддаваться первому порыву, все обдумать или лучше всего все рассказать и посоветоваться со взрослыми.**

**Учитель истории и обществознания Дадукина Г.В.**