Международная олимпиада по финансовой безопасности для учащихся 8-10 классов общеобразовательных организаций

Федеральная служба по финансовому мониторингу проводит Международную олимпиаду по финансовой безопасности для учащихся 8-10 классов общеобразовательных организаций (далее – Олимпиада).

Цель Олимпиады - повышение информационной, финансовой иправовой грамотности детей и молодежи.

Олимпиада проводится в два этапа:

- первый (отборочный) этап проводится с 17 по 21 мая 2021 г. Для учащихся общеобразовательных организаций Сибирского Федерального округа отборочный этап пройдет на базе Сибирского федерального университета и Новосибирского государственного университета экономики и управления «НИНХ». Порядок проведения отборочного этапа размещен на официальных сайтах университетов и по ссылке https://fedsfm.ru/olympiad/geography.

- второй (финальный) этап проводится с 3 по 9 октября 2021 года на федеральной территории «Сириус» (г. Сочи, Россия).

Координатором проведения Олимпиады является Международный учебно-методический центр финансового мониторинга (e-mail: olimpiada@mumcfm.ru).

В целях подготовки проведения Олимпиады рекомендуется до 15 мая 2021 г. провести для учащихся 8-10 классов Всероссийский тематический урок «Финансовая безопасность» согласно прилагаемым методическим материалам.

Приложения:

1. Методические рекомендации по подготовке и проведению Всероссийского тематического урока «Финансовая безопасность».
2. Презентация «Финансовая безопасность» в формате PDF.
3. Рекомендации по работе с презентацией «Финансовая безопасность».

Федеральное государственное автономное учреждение высшего образования
«Российский университет дружбы народов»

Методические рекомендации

по подготовке и проведению
Всероссийского тематического урока на тему
«Финансовая безопасность»

Москва, 2021

Аннотация

Методические рекомендации подготовлены в помощь педагогам образовательных организаций и ориентированы на оказание методической помощи педагогам начального общего, основного общего, среднего (полного) общего и дополнительного образования по организации и проведению тематического урока, посвященного основам финансовой грамотности и финансовой безопасности. В методических рекомендациях предлагаются концептуальные, содержательные, методические и технологические подходы к проведению.

В Рекомендациях раскрывается комплекс вопросов, связанных с проведением данного мероприятия. Предлагаемые материалы носят рекомендательный характер, поэтому педагог может провести занятие, опираясь на данные разработки, исходя из собственного опыта, учитывая возрастные особенности, уровень подготовки обучающихся, а также традиции региона.

Рекомендации рассчитаны на максимальный охват существующих видов финансового мошенничества и способов защиты от них. Учитывая ограниченность времени, отведенного на урок, педагог может по своему усмотрению сконцентрироваться на тех или иных видах мошенничества в зависимости от возраста обучающихся и/или иных критериев выбора.

Пояснительная записка

Финансовое образование молодежи способствует принятию грамотных решений, минимизирует риски и, тем самым, способно повысить финансовую безопасность молодежи. Низкий уровень финансовой грамотности и знаний в области финансовой безопасности может привести не только к банкротству, но и к неграмотному планированию выхода на пенсию, уязвимости к финансовым мошенничествам, чрезмерным долгам и социальным проблемам, включая депрессию и прочие личные проблемы.

Цель – создание условий для формирования 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 школьников 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.

По данным Национального агентства финансовых исследований (опрос проведен Аналитическим центром НАФИ в июле 2020 г.) 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 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).

Раскрытие основной темы урока направлено на формирование основ финансовой культуры обучающихся старших классов, воспитание понимания школьниками важности приобретения базовых знаний и навыков обеспечения финансовой безопасности.

Основой урока станет ответ на вопрос: «Почему важно учиться финансовой безопасности?», а также усвоение учащимися минимальных правил финансовой безопасности.

В рамках подготовки к уроку можно задействовать информационные видеоролики, комиксы и брошюры, посвященные финансовой безопасности.

Обучающимся можно предложить решить ситуационные задачи, связанные со случаями финансового мошенничества – изучить ситуацию и составить план действий по ее предотвращению или предотвращению ее негативных последствий.

В ходе подготовки к проведению урока учителя могут обратиться к порталу Национального агентства финансовых исследований (https://nafi.ru/analytics/27-derzhateley-bankovskikh-kart-mogut-stat-zhertvami-moshennikov/), видеоурокам финансовой грамотности, размещенным на

видео-хостинге YouTube (https://www.youtube.com/watch?v=kK5vp_uzY6Q) и информационно-просветительскому ресурсу Центрального банка Российской Федерации «Финансовая культура». (https://fincult.info/articles/ostorozhno-moshenniki/).

Особенности организации учебной деятельности

Важным условием достижения педагогических задач является организация урока таким образом, чтобы фронтальная, групповая и индивидуальная работа взаимно дополняли друг друга. При подготовке и проведении занятия необходимо учитывать возрастные и образовательные возможности обучающихся.

Основные тезисы урока

Многие школьники 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. Ведь во взрослой жизни придется самостоятельно принимать множество финансовых решений, будь то оплата образования, покупка автомобиля и недвижимости для будущей семьи и даже управление пенсионными накоплениями. Как накопить деньги и не попасть в финансовые ловушки, как взять кредит или инвестировать свои средства – уже скоро сегодняшним школьникам предстоит решать эти непростые вопросы.

Финансы окружают нас повсюду, и знать базовые правила их безопасного использования жизненно необходимо каждому из нас.

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.

Для того, чтобы эффективно противостоять финансовому мошенничеству, которое угрожает нашей личной финансовой безопасности, необходимо, в первую очередь, разобраться с тем, что оно из себя представляет и каким бывает.

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;
- ✓ мошенничество на рынке Форекс.

Разберемся с основными способами защиты от финансовых мошенников, с которыми можно столкнуться уже в подростковом возрасте.

1. **Мошенничество с банковскими картами** бывает различных типов, среди которых можно выделить:
   - Скимминг – это установка специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте. Это специальное устройство, которое 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. Перед пользованием банкоматом внимательно осмотрите его на предмет наличия посторонних предметов.
   - «Магазинные мошенничества». Данные карты могут быть считаны и зафиксированы ручным скиммером. Поэтому не передавайте карту или ее данные посторонним, требуйте проведения операций с картой только в личном присутствии. Данный вид мошенничества также распространен в отношении банковских карт с функцией бесконтактной оплаты: с помощью специального терминала, приложенного к карману или сумке жертвы, мошенники могут украсть денежные средства с карты.
   - Траппинг. На банкомат устанавливаются устройства, которые блокирует карту. На помощь человеку приходит мошенник, который подсматривает ПИН-код и после ухода человека достает карту из банкомата. При вводе ПИН-кода закрывайте рукой клавиатуру.

- 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. Самая сложная задача мошенника — узнать ваш ПИН-код. Никому не сообщайте его.
- Вишинг (голосовой фишинг). Сбор информации о номерах карт и счетов при помощи моделирования звонка автоинформатора.
- Звонки мошенников с просьбой погасить задолженность по кредиту. Когда гражданин сообщает, что кредит он не брал, ему предлагается уточнить данные его 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 не стать жертвой таких мошенников?

- ✓ 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, в том числе при оплате товаров/ услуг через Интернет и иные информационные сети.
- ✓ В случае потери карты или утраты ПИН-кода немедленно обратитесь в ваш банк для ее блокирования.
- ✓ 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.
- ✓ 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.
- ✓ 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.
- ✓ 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.

В случае мошеннической или ошибочной операции по карте обратитесь в отделение банка и попросите выписку по счету. Напишите заявление о несогласии с операцией. Сохраните экземпляр заявления с отметкой банка о приеме. Обратитесь в правоохранительные органы с заявлением о хищении.

2. 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.
   - 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.

3. **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.

Чтобы не стать жертвой мобильных аферистов:

- ✓ 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.

Приложение

Глоссарий

Платежеспособность – характеристика финансового состояния человека (или компании), описывающая его возможность обеспечивать свои текущие расходы и обязательства.

Финансовая безопасность – понятие, включающее комплекс мер, методов и средств по защите экономических интересов государства на макроуровне, корпоративных структур, финансовой деятельности хозяйствующих субъектов на микроуровне.

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.

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

Скимминг – это установка специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте.

Фишинг – рассылка электронных писем о якобы производимых изменениях в системе безопасности банка.

Вишинг (голосовой фишинг) – сбор информации о номерах карт и счетов при помощи моделирования звонка автоинформатора.

CVV (CVC-код) – трехзначный код проверки подлинности банковской карты, расположенный на ее обороте (обычно используется для подтверждения финансовых операций в интернете).

Документы

1. Указ Президента РФ от 01.07.1996 № 1008 (ред. от 16.10.2000) «Об утверждении Концепции развития рынка ценных бумаг в Российской Федерации» и Концепция развития рынка ценных бумаг в Российской Федерации
2. Распоряжение Правительства РФ от 05.02.2016 № 164-р «Об утверждении Стратегии действий в интересах граждан старшего поколения в Российской Федерации до 2025 года» и Стратегия действий в интересах граждан старшего поколения в Российской Федерации до 2025 года
3. Распоряжение Правительства РФ от 25.09.2017 № 2039-р «Об утверждении Стратегии повышения финансовой грамотности в Российской Федерации на 2017 - 2023 годы» и Стратегия повышения финансовой грамотности в Российской Федерации на 2017 - 2023 годы
4. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств (I и II кварталы 2019/2020 года), подготовленный Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России. URL:

https://www.cbr.ru/analytics/ib/review_1q_2q_2020/ (дата обращения: 26.03.2021).
5. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств (III квартал 2019/2020 года), подготовленный Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России. URL: https://www.cbr.ru/analytics/ib/review_3q_2020/ (дата обращения: 26.03.2021).

Литература и источники по финансовой безопасности:

1. *Горяев* А., *Чумаченко* В. Основы финансовой грамотности. 8-9 классы. Учебник // М.: Просвещение, 2019. 272 с.
2. *Горяев* А., *Чумаченко* В. Основы финансовой грамотности. 8-9 классы. Методические рекомендации // М.: Просвещение, 2020. 106 с.
3. *Горяев* А., *Чумаченко* В. Основы финансовой грамотности. 8-9 класс. Рабочая тетрадь // М.: Просвещение, 2019. 64 с.
4. *Горяев* А., *Чумаченко* В. «Финансовая грамота» // Российская экономическая школа, 2009. URL: https://www.visa.com.ru/dam/VCOM/regional/cemea/russia/media-kits/documents/FinGramota.pdf
5. *Горяев* А., *Чумаченко* В. «Финансовая грамота для школьников» // Российская экономическая школа, 2010. URL: https://www.visa.com.ru/dam/VCOM/regional/cemea/russia/media-kits/documents/Fingramota2.pdf
6. *Макаров* С., *Смирнова* Н., *Дедова* В., *Блискавка* Е., *Васильева* А. «Банковская карта: инструкция по безопасному и эффективному применению» // Брошюра Института Финансового Планирования. URL: https://www.visa.com.ru/dam/VCOM/regional/cemea/russia/media-kits/documents/bankcard.pdf
7. *Макаров* С., *Смирнова* Н., *Дедова* В., *Блискавка* Е., *Васильева* А. «Кредитные карты: инструкция по применению» // Брошюра Института Финансового Планирования. URL: https://www.visa.com.ru/dam/VCOM/regional/cemea/russia/media-kits/documents/credit-n.pdf
8. *Макаров* С., *Смирнова* Н., *Дедова* В., *Блискавка* Е., *Васильева* А. «Зарплатные карты: инструкция по применению» // Брошюра Института Финансового Планирования. URL: https://www.visa.com.ru/dam/VCOM/regional/cemea/russia/media-kits/documents/salary.pdf
9. Личные финансы // Методическое пособие для учителя 9-11 классов. URL: https://www.visa.com.ru/dam/VCOM/regional/cemea/russia/media-kits/documents/teacher-9-11-rus.pdf
10. Личные финансы // Рабочая тетрадь для ученика 9-11 классов. URL: https://www.visa.com.ru/dam/VCOM/regional/cemea/russia/media-kits/documents/child-9-11-rus.pdf

11. Риски и финансовая безопасность // Материалы VВсероссийской недели финансовой грамотности для детей и молодежи, 2019. URL: http://fingram.rkomi.ru/uploads/documents/lichnaya_finansovaya_bezopasnost_pdf_2019-06-09_08-29-38.pdf
12. Учебно-методические комплекты по финансовой грамотности в формате электронного учебника // https://школа.вашифинансы.рф (УМК для 10-11 классов, Модуль 6).
13. Электронное учебное пособие по финансовой грамотности Экономического факультета МГУ// https://finuch.ru/ (раздел 5.5.).

Интернет-ресурсы *(дата обращения: 24.03.2021)*

1. Интернет-портал Национального агентства финансовых исследований. URL: https://nafi.ru/analytics/27-derzhateley-bankovskikh-kart-mogut-stat-zhertvami-moshennikov/
2. Единый государственный реестр Юридических лиц. URL: https://egrul.nalog.ru/index.html
3. Справочник финансовых организаций. URL: https://www.cbr.ru/fmp_check/
4. Аналитика Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России. URL: https://www.cbr.ru/information_security/analitics/
5. Информационно-просветительский ресурс Центрального банка Российской Федерации «Финансовая культура». URL: https://fincult.info/articles/ostorozhno-moshenniki/
6. КиноПАКК: учебные фильмы по финансовой грамотности для УМК // https://edu.pacc.ru/kinopacc/. Фильм «Сообщите ваш пароль» (https://www.youtube.com/watch?v=HYQNjRJBkCk&t=220s). Фильм «Письмо счастья» (https://www.youtube.com/watch?v=ILvYbw96-5k&t=51s)
7. Образовательные проекты ПАКК: анимированные презентации для УМК по финансовой грамотности // https://edu.pacc.ru/informmaterialy/articles/presenations/. Анимированная презентация «Финансовое мошенничество» (https://www.youtube.com/watch?v=p9xgtCbbYo0&t=311s).
8. Образовательный портал «ХочуМогуЗнаю»: фильм «Цифровые финансовые услуги» (Цифровые финансовые услуги | ХочуМогуЗнаю (xn--80afmshcb2bdox6g.xn--p1ai); Фильм «Финансовая безопасность в интернете. Советы родителям» https://www.youtube.com/watch?v=y7UNy1OEKAQ&t=3s.
9. Официальный сайт Министерства финансов Российской Федерации. URL: https://minfin.gov.ru/ru/om/fingram/directions/strategy/
10. Портал Некоммерческого партнерства «Институт образования и науки» (НП «ИОН»). URL: https://profin.top/literacy/lichnye-finansy/base.html
11. Видеоуроки финансовой грамотности для школьников. URL: https://www.youtube.com/watch?v=kK5vp_uzY6Q

12. Официальный сайт РБК. «Число дел о мошенничестве рекордно выросло на фоне пандемии». URL: https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d
13. Сайт «6 основных правил финансовой грамотности». URL: https://www.fingram39.ru/publications/finansy-semi/8155-.html
14. Научно-образовательный портал «IQ» Национального исследовательского университета «Высшая школа экономики». URL: https://iq.hse.ru/more/finance/neobhodimost-povishenia-finansovoj-gramotnosti

Наверняка вы слышали о ситуациях, когда у людей были похищены документы, банковские карты, пароли к личным страницам или электронным платежным сервисам. Используя ваши знания о подобных ситуациях, опишите случай возможной кражи ваших данных или документов, а затем предложите план экстренных действий, который может включать оформление заявления в полицию, блокировку банковских карт, восстановление аккаунтов в интернете и т.д.

Описание ситуации

Шаг 1

У вас украли паспорт, пароли и банковские карты. Что необходимо предпринять в первую очередь для вашей защиты и обеспечения сохранности ваших активов?

Шаг 2

Что необходимо предпринять, чтобы убедиться в сохранности денег на ваших банковских картах?

Шаг 3

Следующий шаг предполагает, что вы свяжитесь с полицией. Какие действия вы должны предпринять при контакте с полицией? Чем она вам может помочь?

Бывают ситуации, когда думать и действовать надо как можно быстрее! На вечеринке у вас украли бумажник, в котором были все банковские карты, водительские права и паспорт. На следующее утро вы получили уведомление о том, что с вашей банковской карты списано 950 рублей в качестве оплаты счета в пиццерии, в которой никогда в жизни не бывали.

Срочно запускайте процесс блокировки банковских карт, восстановления документов, а также возвращения неправомерно снятой суммы. Напишите письмо в банк, в котором вы описываете случившееся и оспариваете совершенный с украденной карты платеж.

Дата обращения: _____

Ваше имя: _____

Ваш адрес: _____

Номер вашего банковского счета: _____

Наименование банка: _____

Адрес банка: _____

Уважаемый (имя руководителя организации),

Часть 1

В одном коротком абзаце опишите ситуацию: при каких обстоятельства мошенническим путем были сняты деньги с вашей карты (сумма, дата, другие известные детали) и укажите, каких действий вы ждете от банка. Например, вы можете попросить вернуть украденную сумму.

_____
_____
_____
_____
_____
_____
_____
_____
_____

Часть 2

Кратко опишите, какие документальные подтверждения того, что деньги были списаны в результате мошенничества, вы можете предоставить. Например, вы можете послать выписку с банковского счета, включающую неавторизованное вами списание денег, копию полицейского протокола, подтверждающую кражу документов и банковских карт и т.д.

_____
_____
_____
_____
_____
_____
_____

Часть 3

В одном предложении еще раз укажите, каких именно действий вы ждете от банка, выпустившего карту.

_____
_____

С уважением,
Ваше имя _____.

Финансовая безопасность

Уберечь свои деньги стоит больших трудов, чем добыть их.

Мишель де Монтень

RUDN university

Всероссийский тематический урок

Статистика Национального агентства финансовых исследований

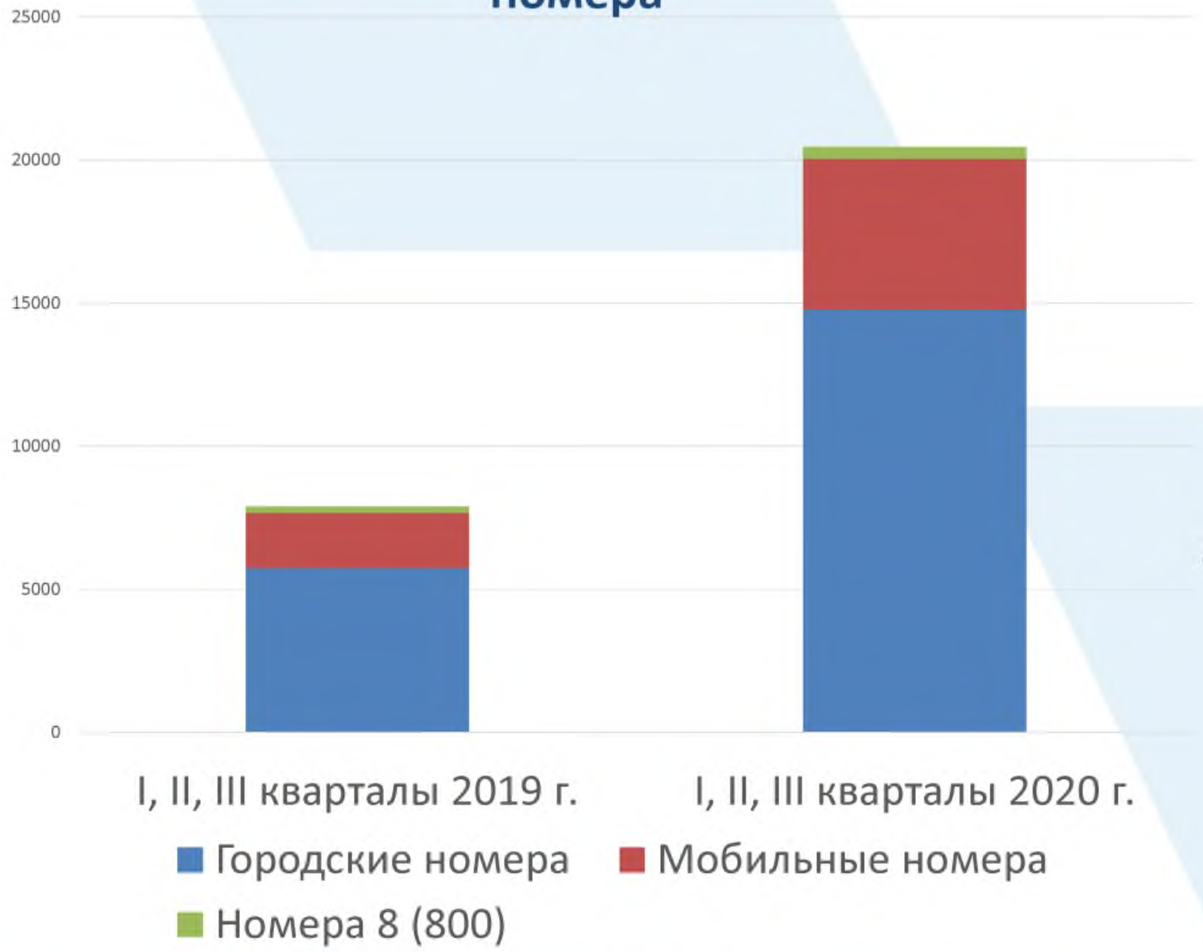
Распространенность банковских карт в России

Случаи финансового мошенничества

Всероссийский опрос проведен Аналитическим центром НАФИ в июле 2020 г. Опрошено 1600 человек старше 18 лет в 136 населенных пунктах в 50 регионах России. Выборка построена на данных официальной статистики Росстат и репрезентирует население РФ по полу, возрасту, уровню образования и типу населенного пункта. Статистическая погрешность данных не превышает 3,4%.

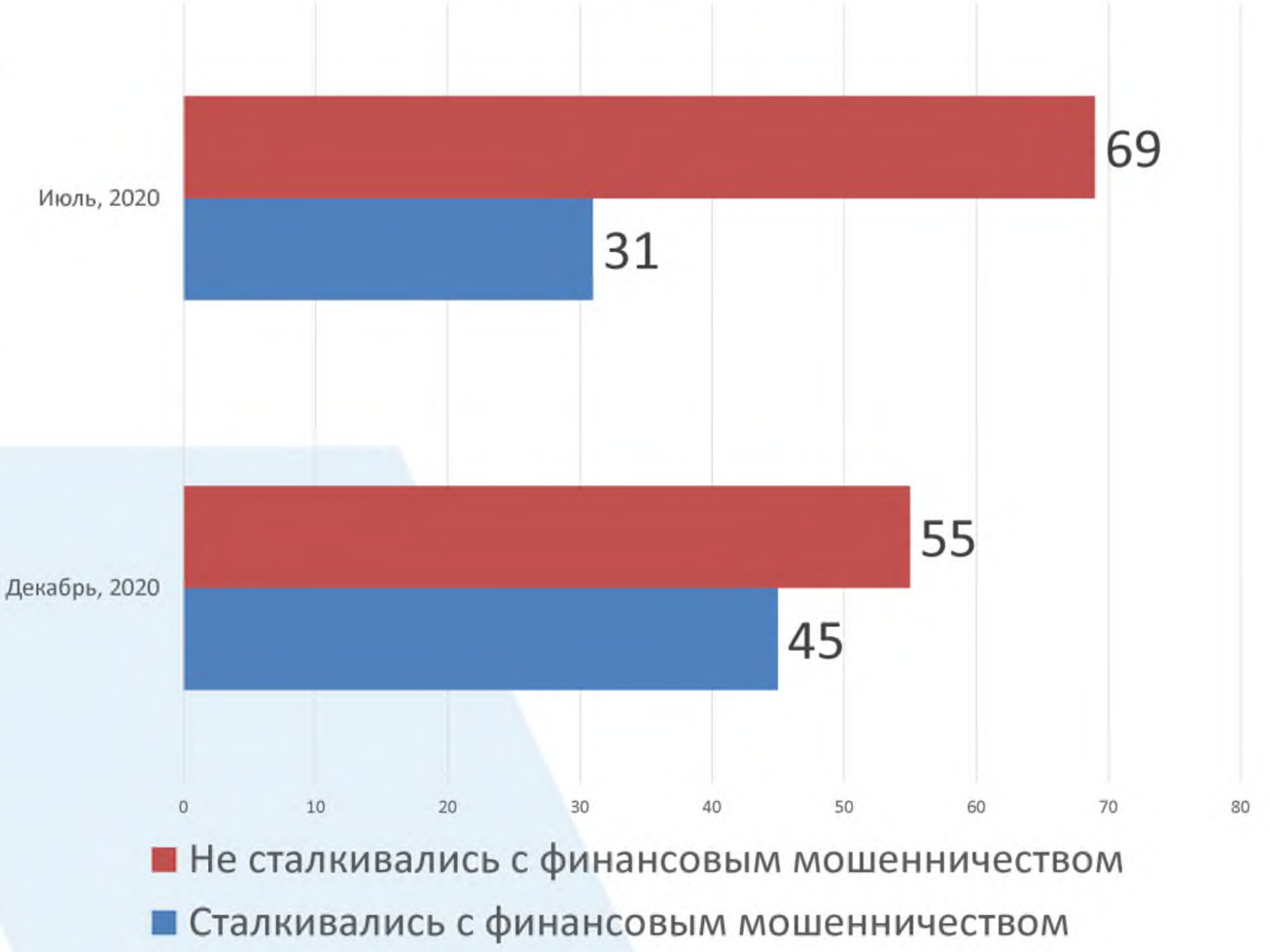
Статистика

Заблокированные по инициативе Банка России мошеннические телефонные номера



Источник: Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств, подготовленный ФинЦЕРТ за I и II кварталы 201/2020 гг. и за III квартал 2019/2020 гг.

Случаи финансового мошенничества в России в 2020 году



Источник: Аналитика от 20.01.2021 г., подготовленная Аналитическим Центром Национального агентства финансовых исследований

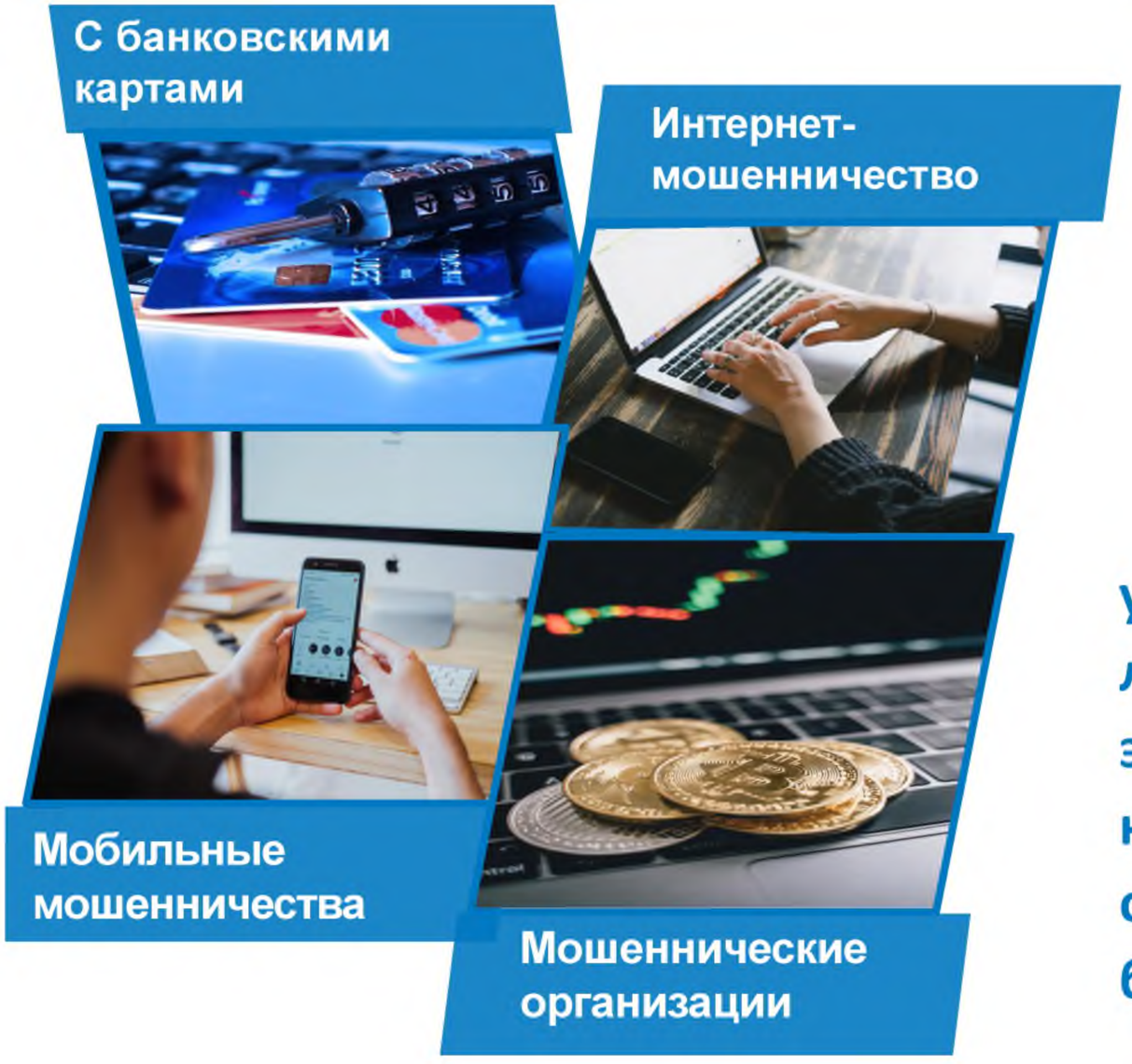
Финансовая безопасность

— понятие, включающее комплекс мер, методов и средств по защите экономических интересов государства на макроуровне, корпоративных структур, финансовой деятельности хозяйствующих субъектов на микроуровне.

Уровни финансовой безопасности:

RUDN university

Виды финансового мошенничества



Финансовое мошенничество угрожает финансовой безопасности личности. Для того, чтобы эффективно противостоять ему, необходимо разобраться с тем, что оно из себя представляет и каким бывает.

Как охотятся за вашими банковскими картами?

Помните: главнейшая задача мошенников в отношении вашей карты – это раздобыть ПИН-код от нее. Не сообщаете его никому и ни при каких условиях.

Ситуация:
Вы платите банковской картой в магазине или кафе: через POS-терминал или с помощью бесконтактной оплаты.

Подумайте:
Как мошенники могут добраться до ваших денежных средств? (не менее 3-х способов финансового мошенничества)

Порядок действий:
Что можно сделать, чтобы это предотвратить?

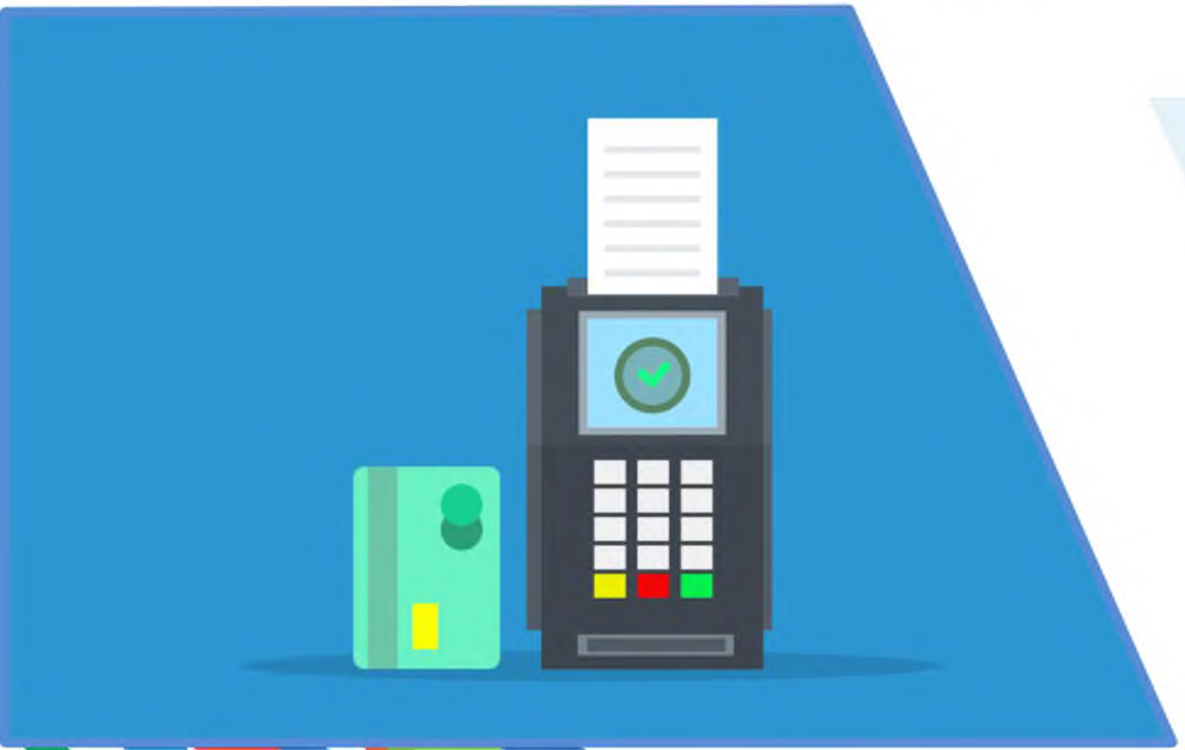
07 Мошенничество с банковскими картами: скимминг

Самый распространенный способ кражи реквизитов карты (номер, имя и фамилия владельца, срок действия) при ее использовании в банкомате — установка на банкомат скиммера. Это специальное устройство, которое 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 — вы даже не заметите, что что-то идет не так. Злоумышленники, используя украденные данные, могут изготовить копию вашей карты.

«Приехал как-то к другу в Москву, около его дома заглянул в магазин — а там только наличными оплата. Побежал к банкомату, торопился. Непримечательный такой банкомат в том же магазине нашел, рядом еще крутились двое парней-«техников» в униформе, с оборудованием, настраивали что-то...»

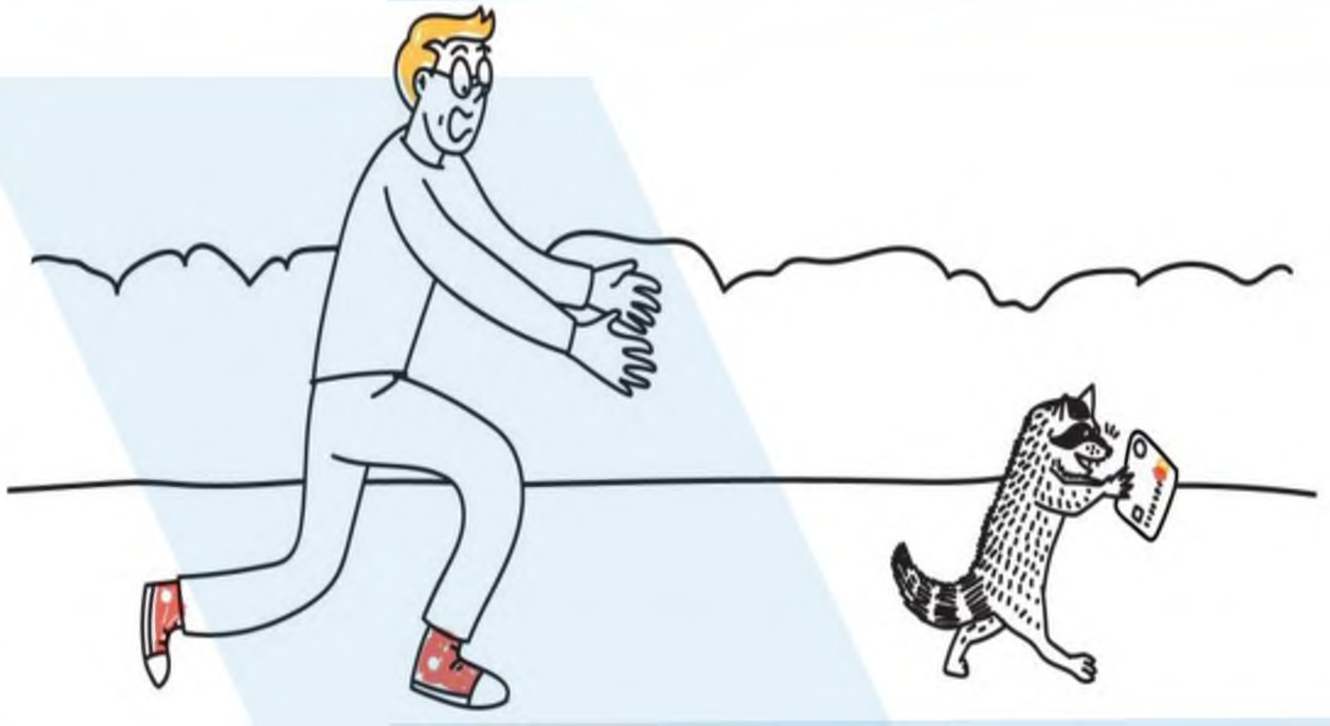
Как не стать жертвой скимминга и траппинга?

- Перед снятием денег в банкомате осмотрите его. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.
- Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.
- Старайтесь пользоваться банкоматами внутри отделений банков. Их чаще проверяют и лучше охраняют.



Карта все же попала в руки злоумышленников. Что делать?

- Позвонить в банк (номер всегда есть на обороте карты), сообщить об этом и заблокировать карту.
- Запросить выписку по счету и написать заявление о несогласии с операцией.
- Обратиться с заявлением в отдел полиции по месту жительства или отправить обращение в управление «К» МВД России.



RUDN university

Наверняка вы слышали о ситуациях, когда у людей были похищены документы, банковские карты, пароли к личным страницам или электронным платежным сервисам. Используя ваши знания о подобных ситуациях, опишите случай возможной кражи ваших данных или документов, а затем предложите план экстренных действий, который может включать оформление заявления в полицию, блокировку банковских карт, восстановление аккаунтов в интернете и т. д.

Описание ситуации

На заметку учащимся

Чтобы уточнить, как правильно действовать в подобной ситуации, ознакомьтесь с информацией на сайтах:

lifehacker.ru/2016/06/06/protecting-your-personal-data/

blog.kaspersky.ru/privacy-ten-tips/10390/

ru.norton.com/16-tips-for-avoiding-online-fraud-and-identity-theft/article

Шаг 1

У вас украли паспорт, пароли и банковские карты. Что необходимо предпринять в первую очередь для вашей защиты и обеспечения сохранности ваших активов?

Шаг 2

Что необходимо предпринять, чтобы убедиться в сохранности денег на ваших банковских счетах?

Шаг 3

Следующий шаг предполагает, что вы свяжитесь с полицией. Какие действия вы должны предпринять при контакте с полицией? Чем она вам может помочь?

Практическое задание

Материал из рабочей тетради для ученика 9-11 классов «Личные финансы», разработанной компанией Visa совместно с Российской экономической школой в рамках программы для школьных уроков по основам финансовой грамотности. Ссылка:https://www.visa.com.ru/visa-everywhere/about-visa/financial-literacy.html

Бывают ситуации, когда думать и действовать надо как можно быстрее! На вечеринке у вас украли бумажник, в котором были все банковские карты, водительские права и паспорт. На следующее утро вы получили уведомление о том, что с вашей кредитной карты списано 950 рублей в качестве оплаты счета в пиццерии, в которой никогда в жизни не бывали.
Срочно запускайте процесс блокировки банковских карт, восстановления документов, а также возвращения неправомерно снятой суммы. Напишите письмо в банк, в котором вы описываете случившееся и оспариваете совершенный с украденной карты платеж.

Дата обращения:_____

Ваше имя:_____

Ваш адрес:_____

Номер вашего банковского счета:_____

Наименование банка:_____

Адрес банка:_____

Уважаемый (имя руководителя организации)

Часть 1
В одном коротком абзаце опишите ситуацию: при каких обстоятельствах мошенническим путем были сняты деньги с вашей карты (сумма, дата, другие известные детали) и укажите, каких действий вы ждете от банка. Например, вы можете попросить вернуть украденную сумму.

Часть 2
Кратко опишите, какие документальные подтверждения того, что деньги были списаны в результате мошенничества, вы можете предоставить. Например, вы можете послать выписку с банкового счета, включающую неавторизованное вами списание денег, копию полицейского протокола, подтверждающего кражу документов и банковских карт и т.д.

Часть 3
В одном предложении еще раз укажите, каких именно действий вы ждете от банка, выпустившего карту.

С уважением,
Ваше имя_____

RUDN university

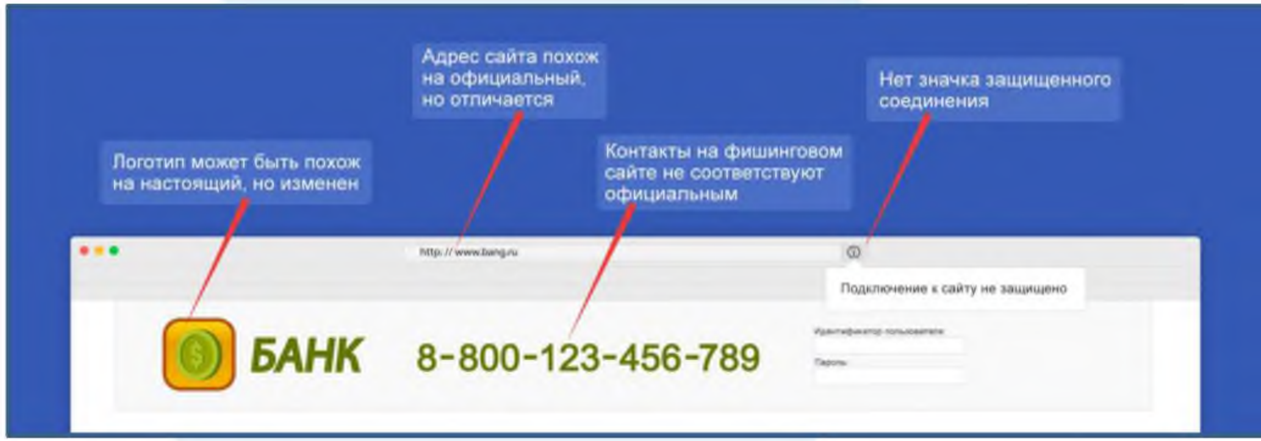
Практическое задание

Материал из рабочей тетради для ученика 9-11 классов «Личные финансы», разработанной компанией Visa совместно с Российской экономической школой в рамках программы для школьных уроков по основам финансовой грамотности.
Ссылка:https://www.visa.com.ru/visa-everywhere/about-visa/financial-literacy.html

Интернет-мошенничество: сайты-двойники

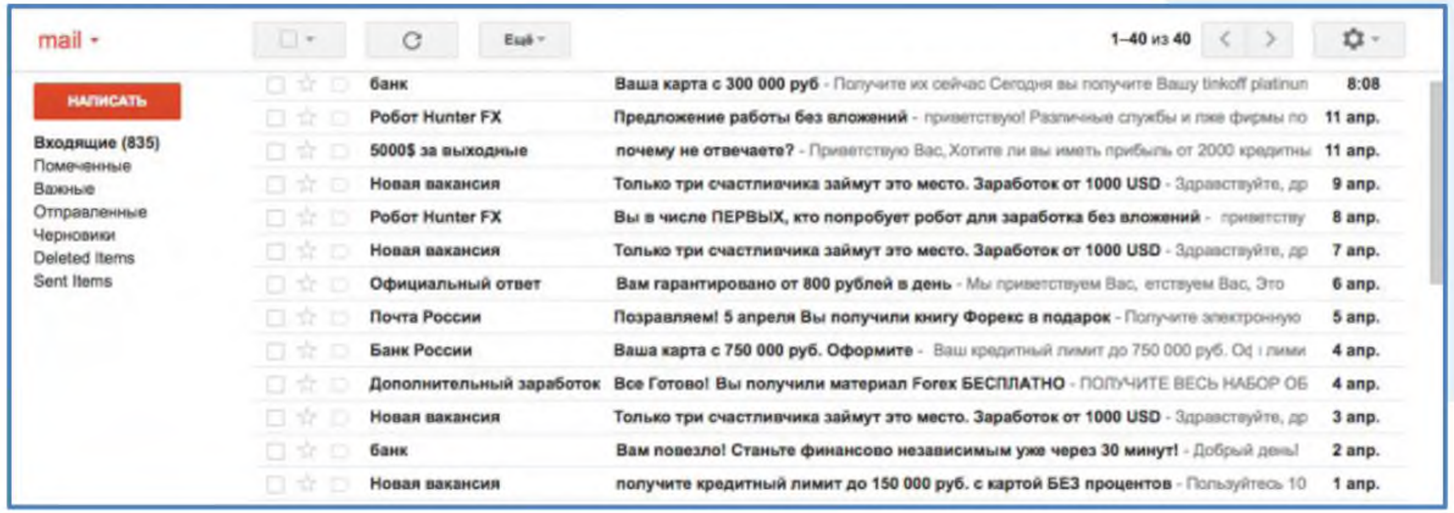
Мошенники копируют известные сайты, используя похожее название компании и оформление. Например, вы хотите узнать, есть ли у вас штрафы в ГИБДД или как оформить кредит онлайн, а попадаете на фишинговый сайт, то есть сайт-клон. Если вы введете на таких сайтах свои данные, они попадут в руки злоумышленников.

Что делать?



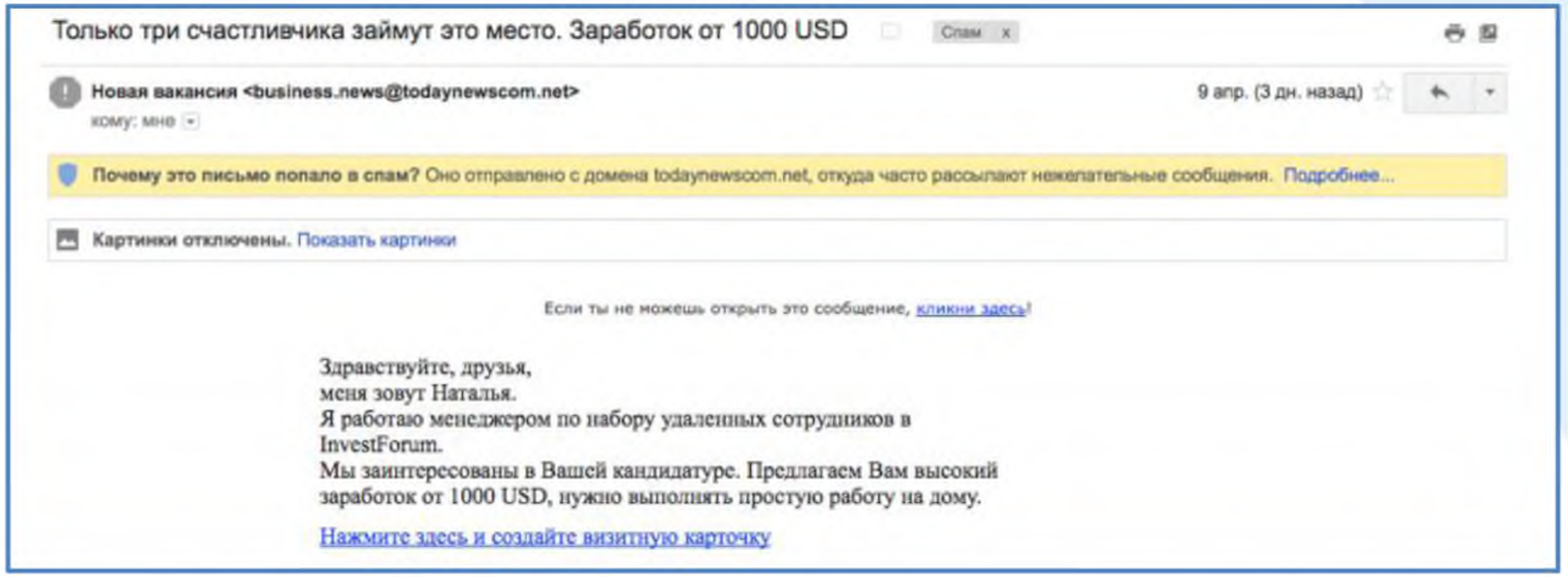
- обращайте внимание на адресную строку браузера: на сайте-клоне будет допущена ошибка
- оплачивайте покупки только через сайты с защищенным соединением и значком платежной системы
- внимательно изучите и содержание сайта — злоумышленники часто невнимательно относятся к наполнению сайта
- добавьте в закладки сайты, которыми часто пользуетесь, чтобы не набирать адрес вручную

Интернет-мошенничество



В строке отправителя может быть как неизвестный вам человек (часто иностранец), так и известный сайт, платежная система, онлайн-сервис или банк.

Вам на почту присылают письма с обещанием подарков, денег и кредитов. Мошенники пытаются заманить вас чем угодно: предлагают работу с большой зарплатой, которую вы не искали. Пишут, что вы выиграли машину. Присылают ответ на якобы ваше письмо. Просто хотят «познакомиться поближе».



Как мобильные аферисты охотятся за нашими деньгами?

Помните: любую информацию касательно денежных средств, сообщаемую вам по телефону, необходимо проверять.

Ситуация:

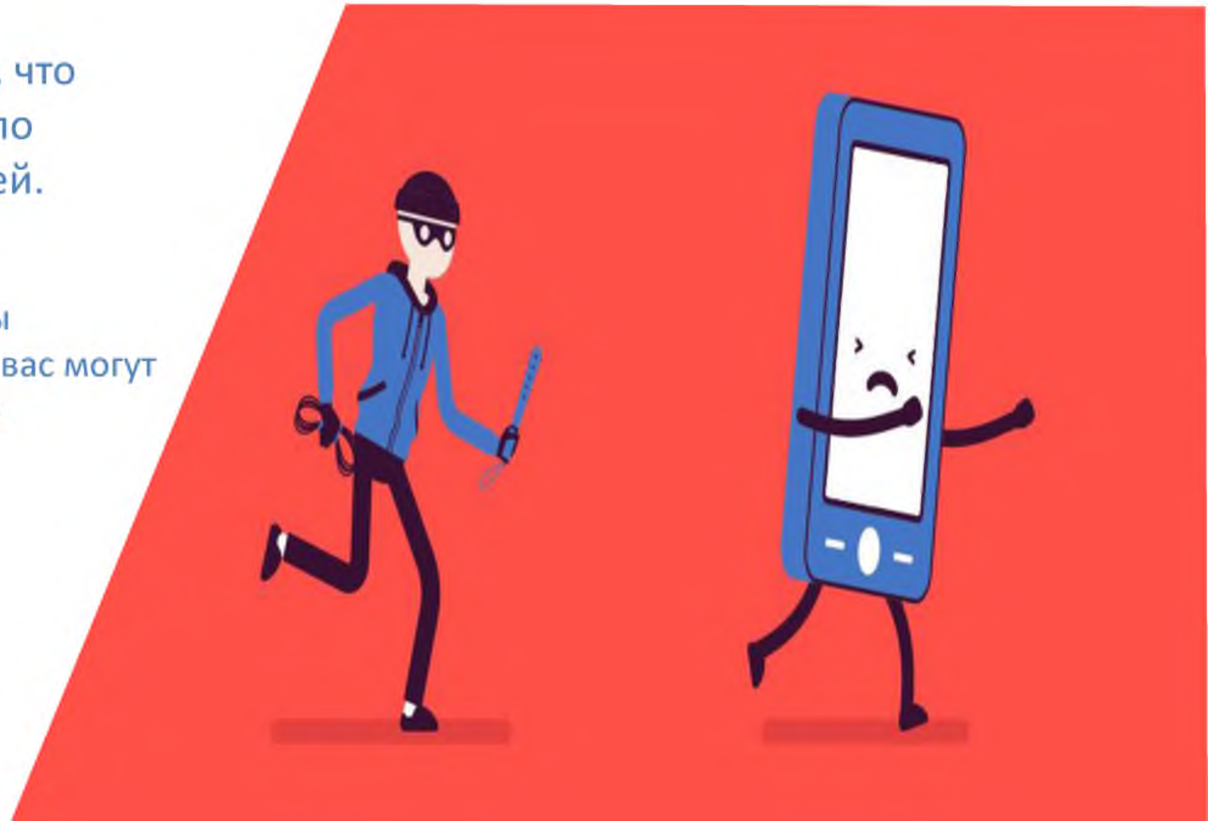
С незнакомого номера приходит смс-сообщение, что ваша карта заблокирована. В смс указан номер, по которому нужно позвонить для уточнения деталей.

Подумайте:

Что может ожидать вас на другом конце провода, если вы позвоните по указанному номеру? Какую информацию у вас могут запросить и как будут убеждать ее предоставить? На кого рассчитан этот вид мошенничества?

Порядок действий:

Как вы поступите в такой ситуации?



В случае подозрения на мобильное мошенничество:

- Если вам звонят от имени Центрального банка, наберите номер горячей линии Банка России 8-800-300-3000.
- Если вам предлагают деньги от имени какого-либо ведомства, позвоните туда и уточните информацию.
- Если вам сообщили о блокировке банковской карты, свяжитесь с банком, выпустившим вашу карту, и уточните эту информацию.

RUDN university

Подведем итоги:

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

RUDN university

МЕЖДУНАРОДНАЯ ОЛИМПИАДА ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ

Цели Олимпиады

Участники: обучающиеся 8-10 классов / 1-3 курсы бакалавриата / 1-4 курсы специалитета / 1 курс магистратуры

- повышение общей информационной, финансовой и правовой грамотности молодежи, формирование новой формы мышления и нового формата деятельности, выявление талантливых школьников и студентов в области финансовой безопасности;
- создание условий для индивидуальной образовательной траектории, содействие профессиональной ориентации школьников и студентов для формирования кадрового ресурса системы финансовой безопасности;
- стимулирование учебно-познавательной и научно-исследовательской деятельности школьников и студентов, развитие научных знаний в области финансовой безопасности.

Маршрут Олимпиады

- ✓ Всероссийский урок по финансовой безопасности
- ○ I этап Олимпиады (вузовский, отборочный)
- ○ 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

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

Отборочный этап (Северо-западный федеральный округ)

Субъекты	Университет	Направления олимпиады
Санкт-Петербург Ленинградская область Республика Карелия Республика Коми Архангельская область Ненецкий автономный округ Мурманская область Калининградская область Новгородская область Псковская область Вологодская область	Санкт-Петербургский политехнический университет Петра Великого	Обществознание и право Математика и информатика (IT, программирование и искусственный интеллект) Экономика

Отборочный этап (Приволжский федеральный округ)

Субъекты	Университет	Направления олимпиады
Республика Башкортостан Республика Марий Эл Республика Мордовия Республика Татарстан Удмуртская Республика Чувашская Республика Пермский край Кировская область Нижегородская область Оренбургская область Пензенская область Самарская область Саратовская область Ульяновская область	Нижегородский государственный университет имени Н.И. Лобачевского	Обществознание и право Математика и информатика (IT, программирование и искусственный интеллект) Экономика

Отборочный этап (Уральский федеральный округ)

Субъекты	Университет	Направления олимпиады
Курганская область Свердловская область Челябинская область Тюменская область Ханты-Мансийский автономный округ Ямало-Ненецкий автономный округ	Уральский федеральный университет имени первого Президента России Б.Н. Ельцина	Математика и информатика (IT, программирование и искусственный интеллект) Экономика
Курганская область Свердловская область Челябинская область Тюменская область Ханты-Мансийский автономный округ Ямало-Ненецкий автономный округ	Тюменский государственный университет	Обществознание и право

Отборочный этап (Сибирский федеральный округ)

Субъекты	Университет	Направления олимпиады
Республика Алтай Республика Тыва Республика Хакасия Красноярский край Иркутская область Алтайский край Кемеровская область Новосибирская область Омская область Томская область	Сибирский федеральный университет	Обществознание и право Математика и информатика (IT, программирование и искусственный интеллект)
	Новосибирский государственный университет экономики и управления «НИНХ»	Экономика

Отборочный этап (Северокавсказский федеральный округ)

Субъекты	Университет	Направления олимпиады
Республика Дагестан Республика Ингушетия Кабардино-Балкарская Республика Карачаево-Черкесская Республика Республика Северная Осетия-Алания Чеченская Республика Ставропольский край	Ростовский государственный экономический университет (РИНХ)	Обществознание и право Математика и информатика (IT, программирование и искусственный интеллект) Экономика

Отборочный этап (Южный федеральный округ)

Субъекты	Университет	Направления олимпиады
Республика Адыгея Республика Калмыкия Краснодарский край Астраханская область Волгоградская область Ростовская область Республика Крым Севастополь	Ростовский государственный экономический университет (РИНХ)	Экономика
	Крымский федеральный университет имени В.И. Вернадского	Обществознание и право
	Севастопольский государственный университет	Математика и информатика (IT, программирование и искусственный интеллект)

Отборочный этап (Дальневосточный федеральный округ)

Субъекты	Университет	Направления олимпиады
Республика Бурятия Республика Саха Забайкальский край Камчатский край Приморский край Хабаровский край Амурская область Магаданская область Сахалинская область Еврейская автономная область Чукотский автономный округ	Тихоокеанский государственный университет	Обществознание и право Математика и информатика (IT, программирование и искусственный интеллект) Экономика

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

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.

Задание 1

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, приложенного к карману или сумке жертвы, мошенники могут украсть денежные средства с карты.*
- *Трэппинг – 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 или заблокировать счет. 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 получить информацию о состоянии вашей карты и решить 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.

Как предотвратить?

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.

Как не стать жертвой скиммеров:

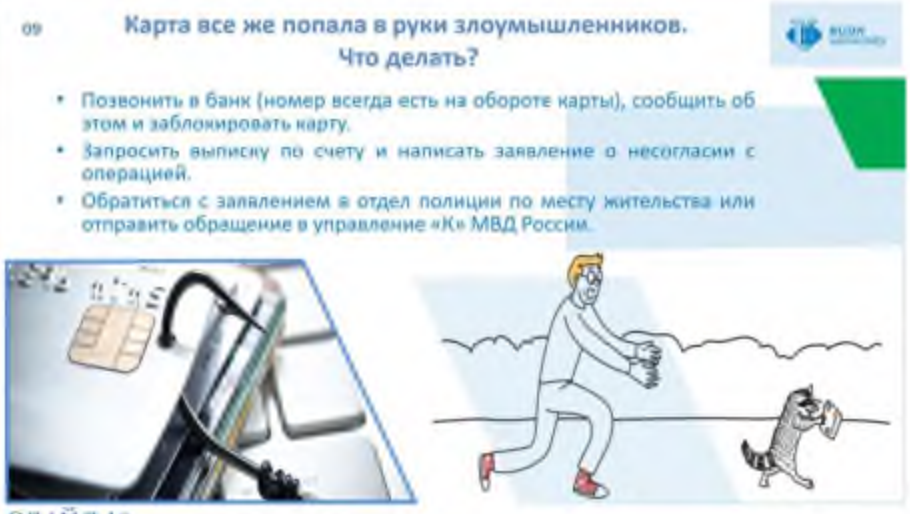
- ✓ *Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.*
- ✓ *Перед пользованием банкоматом внимательно осмотрите его на предмет наличия посторонних предметов; клавиатура не должна шататься.*
- ✓ *В случае потери карты или утраты ПИН-кода немедленно обратитесь 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?



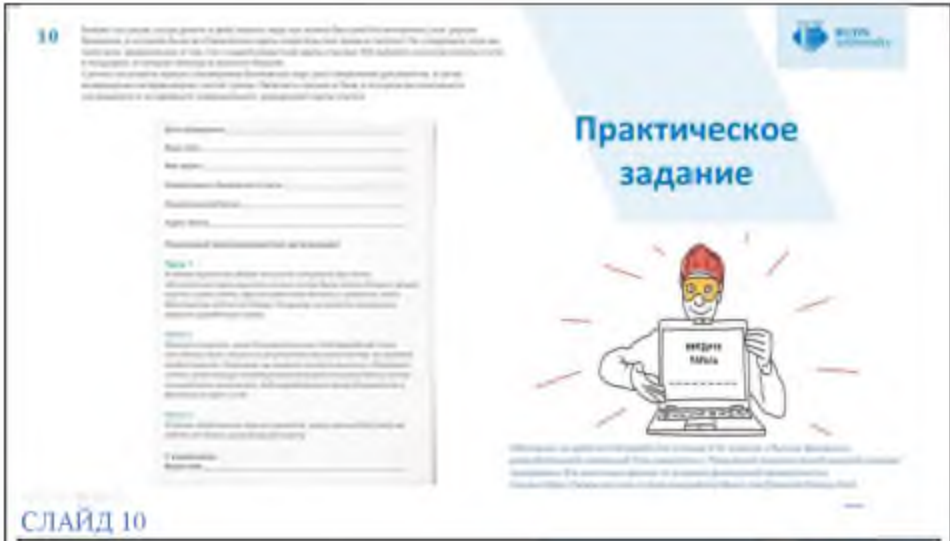
СЛАЙД 10

Задание 5. Практическое задание

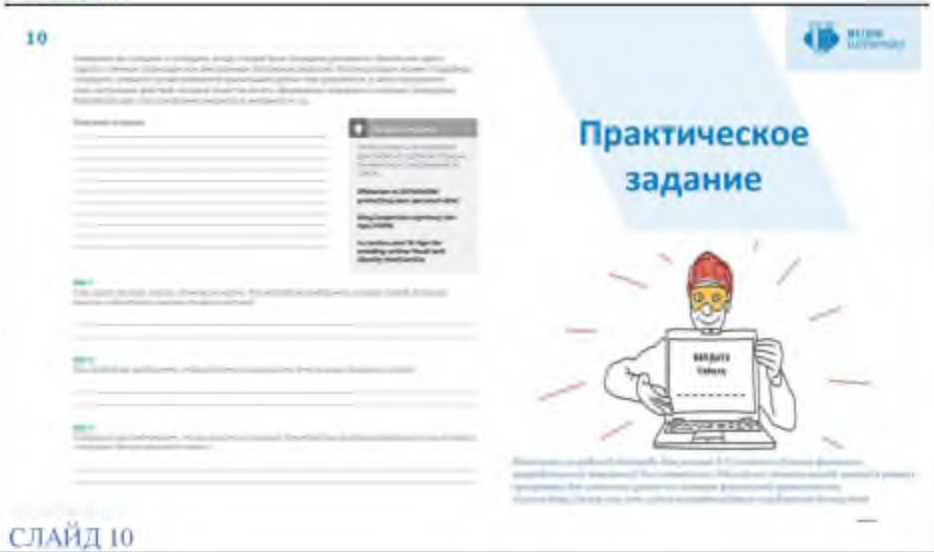
1. Случалось ли вам или вашим родным терять банковскую карту? Предложите порядок действия в такой ситуации. Сравните предложенный вами порядок с представленным на слайде №9. Все ли варианты действий были названы?
2. Изучите ситуацию, представленную на слайде №10. По образцу напишите письмо в банк, в 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).***



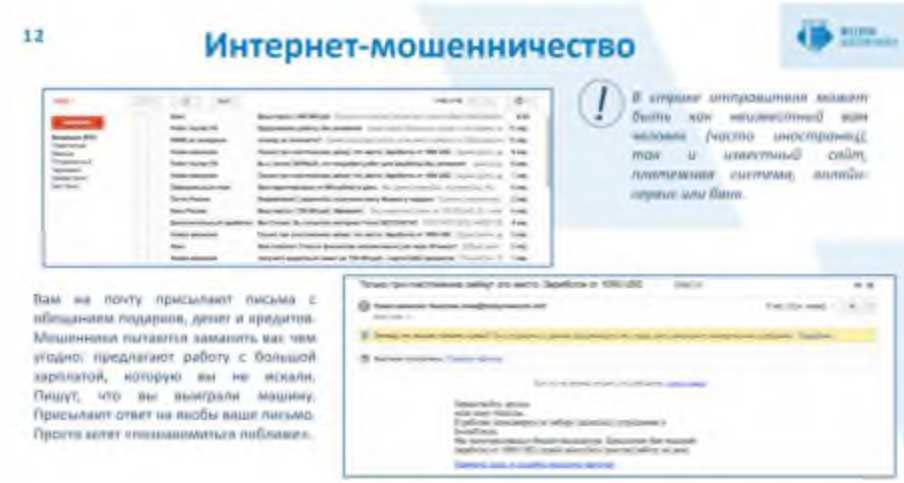
СЛАЙД 10



СЛАЙД 10

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.*



- *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.*

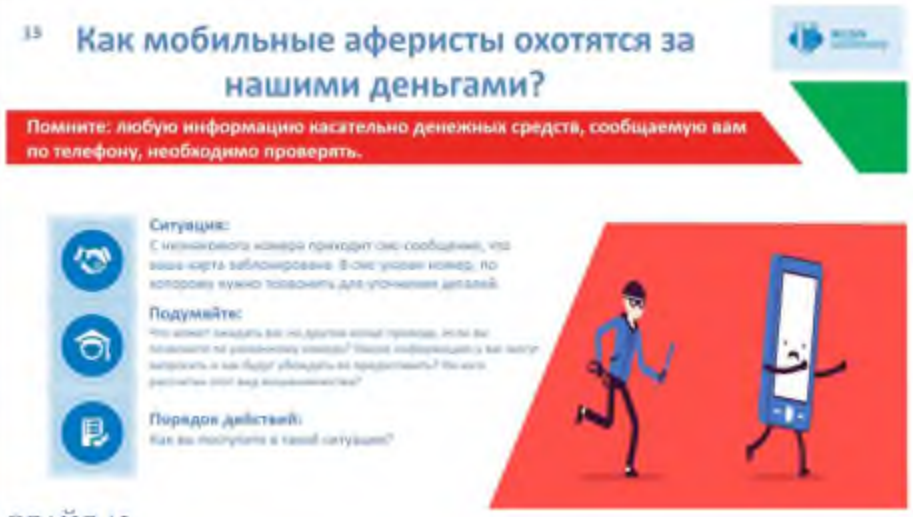
Способы защиты:

- ✓ *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.

14

В случае подозрения на мобильное мошенничество:

- Если вам звонит от имени Центрального банка, наберите номер горячей линии Банка России 8-800-300-3000.
- Если вам предлагают деньги от имени какого-либо ведомства, позвоните туда и уточните информацию.
- Если вам сообщили о блокировке банковской карты, свяжитесь с банком, выпустившим вашу карту, и уточните эту информацию.

СЛАЙД 14

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

15

Подведем итоги:

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

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

17

Цели Олимпиады

Участники: обучающиеся 8-10 классов / 1-3 курсы бакалавриата / 1-4 курсы специалитета / 1 курс магистратуры

СЛАЙД 17

18

Маршрут Олимпиады

- ✓ Всероссийский урок по финансовой безопасности
- ○ I этап Олимпиады (вузовский, отборочный)
- ○ 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 (г. 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

СЛАЙД 20