

**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 portalу 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](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 использованием 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, 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. 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 / CSC-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/](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/](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 V Всероссийской 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](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/](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/analytics/](https://www.cbr.ru/information_security/analytics/)
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 \(xn--80afmshcb2bdox6g.xn--p1ai\)](https://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» (НИ «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](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 \_\_\_\_\_.