## ФИО, должность автора (допустимо до 4-х авторов)

## Методическая разработка —

## серия семинаров «Мошенничества в сфере финансовых услуг» (направлено на взрослое население, включая граждан предпенсионного и пенсионного возраста)

По желанию можно ввести титульный лист, перенеся в него заголовок и ФИО авторов)

1. **Общее описание**

**Цель:** предупреждение неблагоприятных финансовых последствий от попадания граждан в ситуации, сопряженные с мошенническими действиями третьих лиц, связанными с финансовыми услугами.

**Предлагаемые темы семинаров:**

«Телефонные мошенничества, связанные с пользованием финансовыми услугами»

«Мошенничества при пользовании банковской картой»

«Финансовые пирамиды»

«Приобретение ненужных и неоправданно дорогих товаров и услуг (в т.ч. в кредит)»

«Мошенники под видом социальных работников»

«Мошенничество в сети «Интернет» (можно использовать в рамках обучения компьютерной грамотности)

ЖЕЛАТЕЛЬНО УКАЗЫВАТЬ ТЕМЫ, АКТУАЛЬНЫЕ В РЕГИОНЕ

**Форма проведения семинаров**

Очная беседа (семинар) с возможностью задать вопросы или интерактивный онлайн-семинар. (здесь и далее сохраняйте слова об онлайн-формате, если он применим в вашем регионе)

**Продолжительность одного семинара**

Каждый семинар рассчитан на 60 мин, из них последние 10 мин - сессия вопросов и ответов в случае очной формы.

В случае удаленного мероприятия можно предусмотреть возможность отвечать на вопросы слушателей по мере их поступления. (ОСТАВЛЯЙТЕ, ЕСЛИ АКТУАЛЬНО ДЛЯ РЕГИОНА)

При необходимости семинар можно продлить до 80-90 мин за счет увеличения количества рассматриваемых примеров мошенничеств.

**Методы и приемы, используемые при проведении мероприятия**

При проведении мероприятия используются такие приемы, как беседа, лекционное изложение материала, презентация, элементы интерактивного взаимодействия.

1. **Подготовка к проведению семинара**

**Подготовительные действия при очной форме семинара:**

Перед началом семинара ведущему необходимо выполнить следующие действия:

* провести инструктаж ассистентов, которые помогают проводить мероприятие;
* обеспечить наличие и настроить оборудование (проектор, экран, микрофон) для демонстрации слайдов;
* подготовить помещение к заключительной части мероприятия — неформальному общению;
* подготовить раздаточные материалы (при наличии);
* при необходимости – раздать слушателям бейджи (таблички) с именами.

**Подготовительные действия при дистанционной форме семинара: ЭТОТ БЛОК СОХРАНЯЕТСЯ, ЕСЛИ АКТУАЛЬНО ДЛЯ РЕГИОНА**

Перед началом семинара ведущему необходимо выполнить следующие действия:

* подготовить оборудование для проведения семинара, проверить исправность микрофона, камеры и иных технических устройств;
* убедиться в наличии бесперебойной и надежной Интернет-связи;
* подготовить помещение: проверить, чтобы лицо ведущего было достаточно освещено, в кадре не было лишних предметов, а фон был нейтральным;
* при необходимости подготовить интерактивную доску;
* проверить презентацию;
* провести инструктаж с ассистентами или службой технической поддержки, в том числе продумать порядок действий в случае ухудшение Интернет-связи, отключения электричества (укажите актуальные для региона проблемы, которые могут помешать).

1. **Общий план семинара**

### Часть 1. Организационная (продолжительность - 5 минут)

**Цель мероприятия и основные организационные вопросы**

 Можно произнести примерно следующий текст:

«Добрый день, уважаемые слушатели. Мы рады приветствовать на нашем семинаре (онлайн-семинаре). Тема мероприятия … (любая тема из представленных выше).

Далее необходимо рассказать о планируемых результатах самого мероприятия, например: «Уважаемые слушатели в ходе семинара вы познакомитесь с алгоритмом действий, которые помогут вам не стать жертвой мошенников…».

Небольшие организационные детали:

* в случае очного мероприятия сказать, что личные вопросы можно задавать в течение мероприятия, и ответы на них будут даны в последние 5 мин. Общее время мероприятия 60 мин. без перерыва. Далее наш план работы…
* в случае заочного мероприятия сказать, что вопросы можно задавать в чате, и ответы на них будут даваться по мере поступления. Время мероприятия 60 мин. без перерыва. Далее наш план работы… «

В случае, если количество участников в группе небольшое, рекомендуется, чтобы участники назвали свои имена (или даже раздать им бейджи с именами / именами и отчествами) – чтобы ведущий и другие участники могли обращаться друг к другу по имени.

**План мероприятия**

На данном этапе занятия необходимо огласить порядок освещения основных вопросов темы занятия.

Например, можно сказать следующее:

«Сначала мы рассмотрим примеры наиболее распространенных мошеннических действий … Будем рады, если вы поделитесь собственным

Затем выделим признаки, по которым можно определить, что это мошенничество.

После – обсудим, как действовать, если вы поняли, что это мошенники, и они пытаются вас обмануть.

Затем мы с вами отработаем на практике, как именно стоит реагировать на слова мошенников.

И в заключение вам будет предоставлена информация, в какие органы и организации обращаться, если человек пострадал от финансовых мошенников.»

### Часть 2. Теоретическая (продолжительность — 20 минут)

Ведущий проводит семинар в соответствии с планом, используя подготовленную презентацию на соответствующую тему с учетом региональной специфики.(РЕКОМЕНДУЕМ УКАЗАТЬ НАИМЕНОВАНИЕ СУБЪЕКТА РФ) и актуальных на текущий момент способов мошенничества.

Вступление. Общее описание проблемы (желательно со статистическими данными, подтверждающими, что от финансовых мошенников страдает много граждан, какой объем средств они теряют – например, по текущим данным Банка России, бОльшая часть потерь находится в диапазоне 40-80 тысяч рублей; при этом сейчас очень сильно расширилась реклама в сети Интернет ненужных, вредных услуг и сайтов РЕКОМЕНДУЕТСЯ ДОПОЛНИТЬ РЕГИОНАЛЬНЫМИ ПРОБЛЕМАМИ, ЕСЛИ О НИХ ИЗВЕСТНО).

* 1. Основная часть
* Примеры мошенничеств (один пример мошеннической схемы на одном слайде, рекомендуемое количество – 5 различных примеров мошенничеств). После описания ведущим каждого из примеров рекомендуется задавать слушателям вопрос, встречали ли они такое и что они подозрительного замечают в ситуации.
* Общие признаки мошенничеств (помимо прочего, необходимо упомянуть, что мошенники воздействуют на эмоции, торопят, призывают к каким-то лучшим сторонам человека, используют привязанности к близким людям, стремление к материальной обеспеченности, боязнь показаться слабым/глупы/нерешительным/некомпетентным/невежливым и т.п.; преступники часто маскируются под сотрудников банков, государственных органов (особенно социальных), полицейских и др. – тех, кому трудно не доверять и кого хочется послушаться).
* Порядок действий, если вы заподозрили, что с вами общаются мошенники (как вежливо, но при этом надежно и безопасно избавиться от них, не обидев при этом людей, которые, возможно, в действительности мошенниками не являются).

### Часть 3. Практическая (продолжительность — 20 минут)

1. Отработка с аудиторией практически навыков.

Возможны следующие варианты в зависимости от количества слушателей в группе: (МОЖНО СКОРРЕКТИРОВАТЬ РАЗДЕЛ В ЗАВИСИМОСТИ ОТ ТОГО, КАКИЕ ГРУППЫ СОБИРАЮТСЯ У ВАС И КАК ВАМ УДОБНЕЕ С НИМИ РАБОТАТЬ)

* при численности группы до 6 человек включительно ведущий проигрывает совместно с желающими представителями слушателей (либо группой целиком, если никто не пожелает проявить активность) сценарии работы мошенника, для чего берет на себя роль мошенника и описывает ситуацию, вносит слушателям предложения или задает вопросы – в ответ выбранный слушатель или все слушатели вместе предлагают варианты ответов и дальнейшего развития событий;
* при численности группы более 6 человек и равномерной активности слушателей их можно разбить на группы по несколько человек и предложить им для отработки карточки с 3-5 диалогами мошенников и обычных людей – данные диалоги целесообразно проговорить в группах.

2. Подведение итогов отработки практически навыков.

По результатам практической отработки совместно со слушателями целесообразно подвести итоги (в каких ситуациях мошенников было распознать проще, в каких сложнее).

### Часть 4. Заключительная (продолжительность — 10 минут)

1. Рекомендации ведущего, в какие органы и организации следует обращаться, если вы поняли, что пострадали от финансовых мошенников (начиная с банка, карту которого в случае необходимости может потребоваться заблокировать, и написать заявление о мошеннических действия).

2. Подведение итогов – как принципиально стоит поменять свое поведение, чтобы не стать жертвой мошенников; кого стоит бояться, стоит ли бояться вообще всех людей вокруг.

### Часть 5. Неформальное общение (продолжительность 5 минут)

1. **Дополнительные предложения, пояснения и материалы**

1. При возможности к проведению мероприятия можно привлечь:

- представителей полиции (либо воспользоваться актуальными материалами о мошенничествах или памятками, распространяемыми органами полициями);

- представителей регионального управления Банка России, осведомленных относительно актуальных способах финансовых мошенничеств и оказывающих потребителям помощь в защите из прав;

- представителей регионального управления Роспотребнадзора, занимающихся защитой прав потребителей финансовых услуг.

СОСТАВ ПРИВЛЕКАЕМЫХ К ПРОВЕДЕНИЮ СЕМИНАРА ОРГАНОВ МОЖЕТ БЫТЬ ИЗМЕНЕН (СОКРАЩЕН / РАСШИРЕН) С УЧЕТОМ ВАШЕГО ОПЫТА И РЕГИОНАЛЬНОЙ СПЕЦИФИКИ

2. Дополнительно, по теме финансовых мошенничеств (в т.ч. для расширения состава мошеннических схем) можно воспользоваться информацией, размещаемой на сайтах:

- Банка России (например, актуальное интервью о мошенничествах <http://www.cbr.ru/press/event/?id=6913>);

- «Финансовая культура» (Раздел «Осторожно, мошенники!» -https://fincult.info/articles/ostorozhno-moshenniki/ );

- региональных отделений Пенсионного фонда России можно посмотреть, привести свои ссылки);

- региональных управлений МВД России (можно посмотреть, привести свои ссылки).

МОЖНО РАСШИРИТЬ ИСТОЧНИКИ ПОЛЕЗНОЙ ИНФОРМАЦИИ – ИСХОДЯ ИЗ ТОГО, ЧЕМ ПРИВЫКЛИ ПОЛЬЗОВАТЬСЯ ВЫ САМИ

Приложение

**Примеры действий мошенников и предложения, как избежать проблем и что делать, если они все же произошли**

(ЗДЕСЬ РЕКОМЕНДУЕМ ПРИВЕСТИ ПЕРЕЧЕНЬ ПРОБЛЕМ, КОТОРЫЙ АКТУАЛЕН ДЛЯ ВАС, РАСШИРИВ/ИЗМЕНИВ/СОКРАТИВ ПРЕДЛОЖЕННЫЙ ПЕРЕЧЕНЬ)

1. Вы получаете информацию (телефонный звонок, СМС или электронное письмо):

1.1. СМС / электронное письмо содержит ссылку на неизвестный сайт, на который обязательно следует пройти и выполнить какие-то операции (вероятнее всего, это фишинговый сайт).

1.2. СМС/электронное письмо содержит ссылку на неизвестный номер телефона, по которому следует перезвонить или направить сообщение (это номер мошенников – вероятнее всего, звонки / СМС очень дорогие, а на том конце вас введут в заблуждение).

1.3. СМС/электронное письмо содержит файл, который надо открыть, или программу, которую необходимо установить (содержащие вирус, открывающий доступ к вашему телефону/компьютеру мошенникам).

1.4. СМС содержит сообщение о зачислении средств на ваш счет, а затем какой-то гражданин звонит или шлет СМС с другого номера, что средства перечислил ошибочно и надо бы вернуть (на самом деле первое СМС о средствах было не из вашего банка – надо проверять выписку по счету, а потом действовать).

1.5. СМС / электронное письмо содержит информацию о получении вами крупного выигрыша; проходя далее по ссылкам вы узнаете, что для его получения надо немного заплатить: комиссию за операцию и т.п. (комиссию вы оплачиваете, ваши данные, возможно, украдены, никакого выигрыша нет).

1.6. Вам звонят из банка и выражают обеспокоенность по поводу операций на вашем счете / вкладе (для разрешения проблемы у Вас могут попросить данные карты, включая CVV/CVC, предложить перевести деньги на другой счет и т.д.).

1.7. Вам звонят из социальной службы / вы получаете СМС или электронное письмо о предоставлении вам социальной помощи (только что подписан приказ) в связи с чем угодно (коронавирусом, наводнением, критическим потеплением климата, слишком снежной зимой, пожарами в степях и связанным с этим задымлением, открытием новой трассы, вырубкой лесов и т.д.) – для ее получения необходимы данные вашей карты.

1.8. Вам звонят / вы получаете СМС/ вы читаете в социальных сетях, что пострадал ваш друг или близкий родственник попал в беду (сбила машина, потерял телефон, арестован полицией, сам кого-то сбил на машине) и срочно нужна помощь: деньги – их нужно перечислить на конкретный счет (на самом деле с вашим другом/близким, скорее всего, все хорошо – позвоните ему по известному вам номеру и убедитесь в этом)

1.9. Вы получаете письмо об очень простой и выгодной работе (например, переводить крупные суммы денег за рубеж, со счета на счет – а комиссия с каждого перевод ваша, только для начала надо все оформить, внести взнос, оплатить платные обучающие материалы, заплатить свою комиссию за подключение счетов, протестировать, «работает ли» процедура и т.д.).

1.10. Вы видите контекстную рекламу об «очень выгодном предложении» - нереально много заработать, узнать супер-новую технологию, купить новый курс «счастья и богатства», «идеальной работе, не вставая с дивана» и т.д. Ваши данные, может, и не украдут, но склонят вас купить за очень большую сумму бесполезную (хорошо, если не вредную) бессмыслицу.

1.11. В ходе совершения покупки онлайн Вам поступает предложение оплатить покупку, затем приходит СМС с кодом подтверждения – и в ту же минуту раздается звонок от «рассеянного», который якобы по ошибке вбил ваш номер – и теперь ему нужны данные, чтобы завершить оплату своей покупки (на самом деле он охотится за вашей картой и вашим паролем)

### Советы - как не попасться мошенникам

(ТАКЖЕ РЕКОМЕНДУЕМ ДОПОЛНИТЬ/УТОЧНИТЬ С УЧЕТОМ ВАШИХ ПРИМЕРОВ МОШЕННИЧЕСТВА И РЕГИОНАЛЬНОЙ ПРАКТИКИ)

1. Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках.
2. Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем звонит якобы растяпа, который по ошибке зачислил вам деньги и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС — не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.
3. Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок опять же от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас код, чтобы списать с вашего счета деньги или подписать вас на ненужный платный сервис.
4. Никому не сообщайте персональные данные, а уж тем более пароли и коды. Сотрудникам банка они не нужны, а мошенникам откроют доступ к вашим деньгам.
5. Не храните данные карт на компьютере или в смартфоне.
6. Проверяйте информацию. Если вам говорят, будто вы что-то выиграли или c вашей карты случайно списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты.
7. Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.
8. Установите на компьютер антивирус — и себе, и родственникам.

### Что делать, если мошенники все же украли деньги с карты? МОЖНО РАСШИРИТЬ СВОИМИ СОВЕТАМИ С УЧЕТОМ СВОИХ ПРОБЛЕМ

1. Позвоните в банк (номер всегда есть на обороте карты или на главной странице сайта банка), сообщите о мошеннической операции и заблокируйте карту.
2. Запросите выписку по счету и напишите заявление о несогласии с операцией.
3. Обратитесь с заявлением в отдел полиции по месту жительства или отправьте в управление «К» МВД России.