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

## Методическая разработка —

## Статья «Мошенничества в сфере финансовых услуг» (направлено на взрослое население, включая граждан предпенсионного и пенсионного возраста)4

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

ПО ПРЕДЛАГАЕМОМУ ПЛАНУ ВЫ МОЖЕТЕ ПОДГОТОВИТЬ СТАТЬЮ ПО ТЕМЕ ФИНАНСОВЫХ МОШЕННИЧЕСТВ. ВОЗМОЖНО И ДАЖЕ РЕКОМЕНДУЕТСЯ ИЗМЕНЯТЬ НАЗВАНИЕ СТАТЬИ, ЕЕ СТРУКТУРУ И СОСТАВ ОПИСЫВАЕМЫХ МОШЕННИЧЕСКИХ СХЕМ.

1. Описание масштабов проблем в связи с мошенничеством в сфере финансовых услуг

Описать на основе открытых данных сведения о масштабах мошенничеств: количестве выявленных случаев, динамика количества пострадавших, объемах потерь и т.д.

2. Описание примеров мошеннических действий

РЕКОМЕНДУЕТСЯ ВЫБРАТЬ АКТУАЛЬНЫЙ ДЛЯ РЕГИОНА СОСТАВ ВАРИАНТОВ МОШЕННИЧЕСТВ

2.1. Телефонные мошенничества, связанные с пользованием финансовыми услугами

*Рекомендуется по каждому из пунктов привести описание одного или двух вариантов мошенничеств, о которых известно в регионе.*

2.2. Мошенничества при пользовании банковской картой

2.3. Финансовые пирамиды

2.4. Приобретение ненужных и неоправданно дорогих товаров и услуг (в т.ч. в кредит

2.5. Мошенники под видом социальных работников

2.6. Мошенничество в сети «Интернет»

3. Признаки, по которым можно определить, что действие является мошенничеством

4. Как действовать, если стало понятно, что вас пытаются обмануть мошенники

5. Что следует делать пострадавшему от финансовых мошенничеств

**ДАЛЕЕ В ЦЕЛЯХ ДОПОЛНИТЕЛЬНОЙ ПОМОЩИ В ПОДГОТОВКЕ СТАТЬИ ПРИВЕДЕНЫ НЕКОТОРЫЕ МАТЕРИАЛЫ О МОШЕННИЧЕСТВАХ. НА ИХ ОСНОВЕ МОЖНО СФОРМУЛИРОВАТЬ ТЕКСТ ДЛЯ ПРИВЕДЕННОЙ ВЫШЕ СТРУКТУРЫ**

**ПРИ НАЛИЧИИ - ЛУЧШЕ ВЗЯТЬ РЕГИОНАЛЬНЫЕ ПРИМЕРЫ.**

**САМО ДАННОЕ ПРИЛОЖЕНИЕ В СДАВАЕМУЮ ИТОГОВУЮ РАБОТУ НЕ ВКЛЮЧАТЬ!**

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

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

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.

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.

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.

Никому не сообщайте персональные данные, а уж тем более пароли и коды. Сотрудникам банка они не нужны, а мошенникам откроют доступ к вашим деньгам.

Не храните данные карт на компьютере или в смартфоне.

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.

Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.

Установите на компьютер антивирус — и себе, и родственникам.

### Что делать, если мошенники все же украли деньги с карты?

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.