

## СХЕМА «ЗВОНОК ОТ ОПЕРАТОРА СОТОВОЙ СВЯЗИ»

### Легенда

В связи с новыми правилами Роскомнадзора о блокировке сим-карт нам необходимо подтвердить Ваши данные и актуализировать договор, иначе номер будет заблокирован. Чтобы подписать договор электронной подписью, продиктуйте код из СМС-сообщения.

???

Продиктовать код из СМС-сообщения



### Цель звонка

- Получить ДОСТУП К ЛИЧНОМУ КАБИНЕТУ НА ПОРТАЛЕ ГОСУСЛУГ.
- Получить ДОСТУП К ОНЛАЙН-БАНКИНГУ ИЛИ ПЛАТЕЖНЫМ СЕРВИСАМ.



### Механизм кражи денег



**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ для управления действиями человека.

## СХЕМА «ЗВОНОК ОТ ОПЕРАТОРА СОТОВОЙ СВЯЗИ»

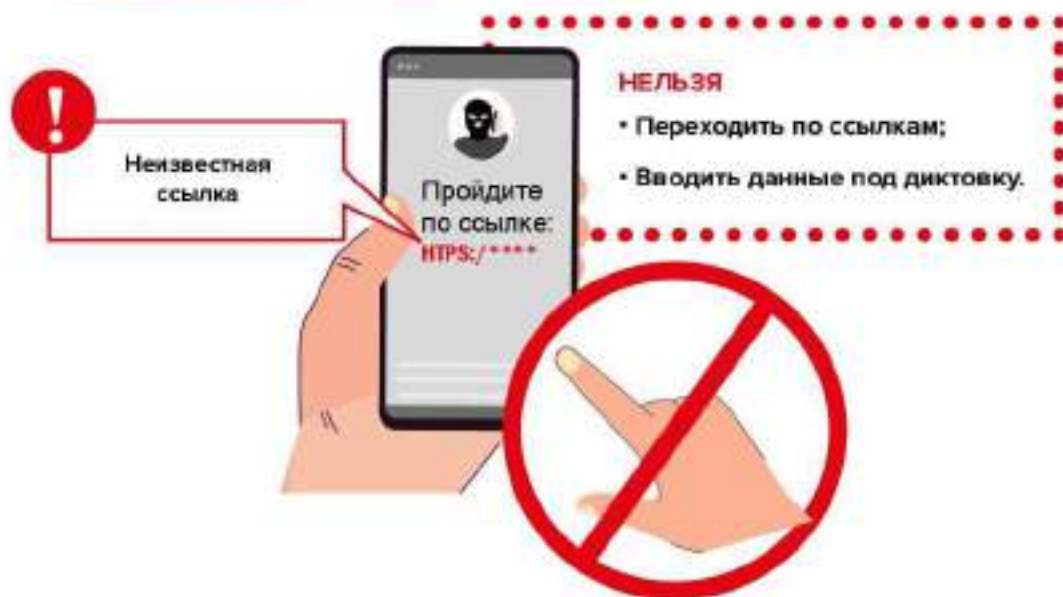
### Признаки, что звонок исходит от мошенников



## Алгоритм действий



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников



**НИКОГДА НЕ ПЕРЕДАВАЙТЕ КОДЫ** подтверждения третьим лицам, даже если они представляются сотрудниками Вашего мобильного оператора.



Двухфакторная аутентификация



Используйте **ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ** везде, где это возможно: портал «Госуслуги», банковские приложения, платежные сервисы, мессенджеры, социальные сети.

**Важно!**

**ДОГОВОР ОКАЗАНИЯ УСЛУГ С СОТОВЫМ ОПЕРАТОРОМ ЯВЛЯЕТСЯ БЕССРОЧНЫМ.**

Сотовые операторы действительно рассылают клиентам просьбы подтвердить личность, но происходит это, как правило, через офисы операторов.



FMDAM.RF

Больше информации на странице ФМЦ ФГН и на портале Моифинансы.рф



MOIFINANSY.RF

## СХЕМА «ЗВОНОК ИЗ ОТДЕЛЕНИЯ ПОЧТОВОЙ СВЯЗИ ИЛИ ПУНКТА ВЫДАЧИ ЗАКАЗОВ: ПИСЬМО/ПОСЫЛКА ВАС ЖДЕТ»

### Легенда

#### Вариант 1.

— В отделение почтовой связи поступило заказное письмо от Федеральной налоговой службы, Вам было направлено уведомление, срок хранения письма истекает завтра. Мы можем оформить услугу курьерской доставки. Письмо будет доставлено в удобное для Вас время, подготовьте паспорт для подтверждения своей личности при вручении письма. **Подтвердите оформление услуги, продиктовав код из СМС-сообщения.**

#### Вариант 2.

— В пункте выдачи заказов маркетплейса находится Ваша посылка, срок ее хранения истекает завтра. Мы можем оформить услугу курьерской доставки. Посылка будет доставлена в удобное для Вас время. **Подтвердите оформление услуги, продиктовав код из СМС-сообщения.**

???

продиктовать код из СМС-сообщения

### Цель звонка

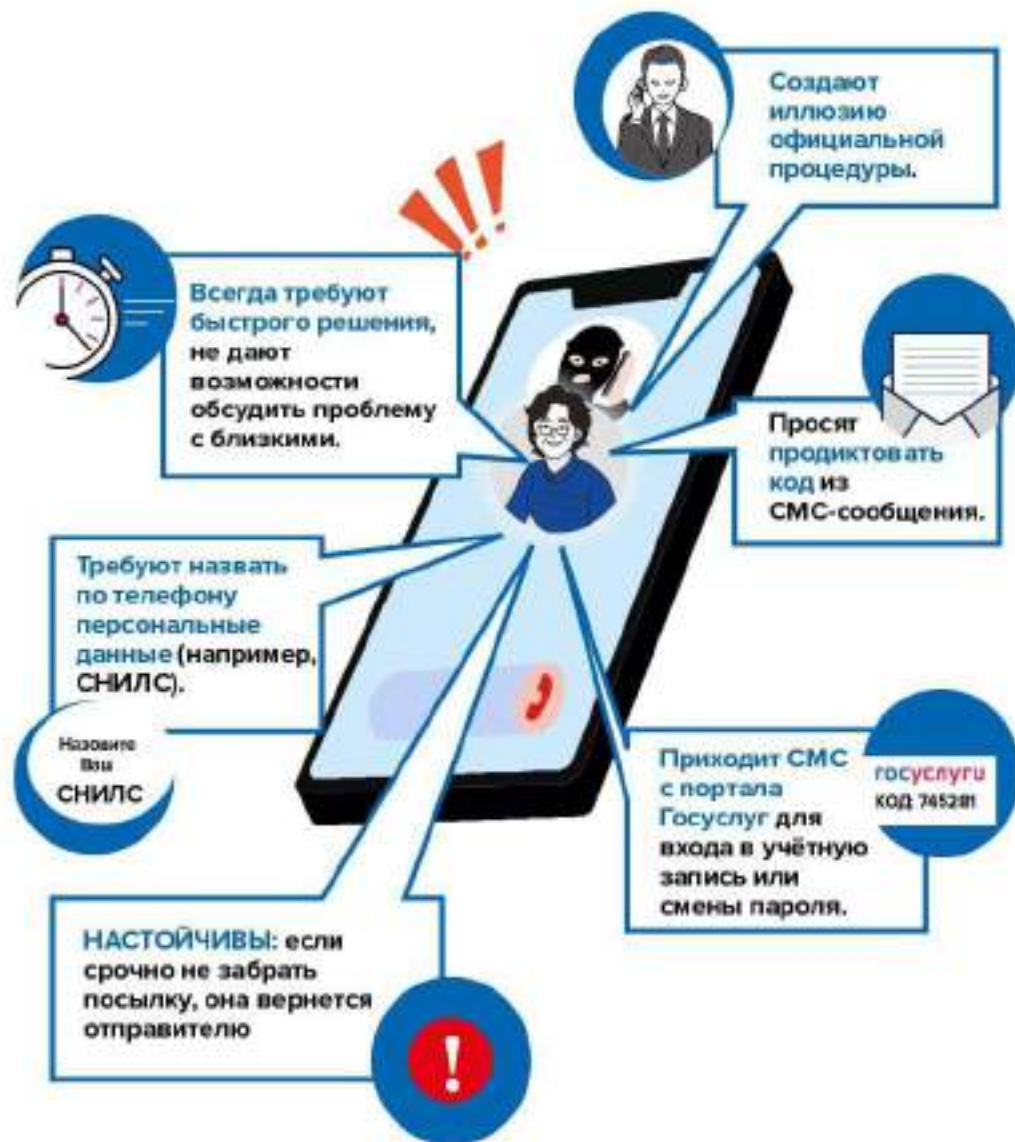
Получить доступ к личному кабинету на портале Госуслуг.

### Механизм кражи денег

**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют **ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ** для управления действиями человека.

СХЕМА «ЗВОНОК ИЗ ОТДЕЛЕНИЯ ПОЧТОВОЙ СВЯЗИ ИЛИ ПУНКТА ВЫДАЧИ ЗАКАЗОВ: ПИСЬМО/ПОСЫЛКА ВАС ЖДЕТ»

### Признаки, что звонок исходит от мошенников



Алгоритм действий



Правила, которым нужно следовать, чтобы не стать жертвой мошенников

**НИКОГДА НЕ ПЕРЕДАВАЙТЕ КОДЫ** подтверждения третьим лицам, даже если они представляются сотрудниками государственных учреждений.



**Важно!**

Сотрудники отделений почтовой связи или пунктов выдачи маркетплейсов **НЕ ОБЗВАНИВАЮТ ГРАЖДАН.**



FINGRAM.RF

Больше информации на странице ФМЦ ФГН и на портале Моифинансы.рф



MOIFINANSY.RF

## СХЕМА «МАМОНТ»

(существует несколько разновидностей сценариев, тут описан один из наиболее часто встречающихся)

## Легенда

На сайтах бесплатных объявлений размещается информация о продаже товара по сниженной цене. Потенциальная жертва пишет «продавцу» сообщение о готовности приобрести товар. «Продавец» предлагает перейти в мессенджер для дальнейшего обсуждения вопроса покупки и доставки. В мессенджере продавец запрашивает данные жертвы, якобы для оформления доставки. Далее направляется ссылка на оплату товара и доставки.

Пройдите по ссылке:  
HTTPS://\*\*\*\*



## Цель

Получение денежных средств от жертвы.



## Механизм кражи денег

**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ для управления действиями человека.



## Признаки, что общение исходит от мошенников



Всегда **ТРЕБУЮТ БЫСТРОГО РЕШЕНИЯ**, не дают времени на размышления (например, сообщают, что товар является последним).

Настойчивы. **Требуют ПЕРЕВЕСТИ ПРЕДОПЛАТУ** за товар.



Полностью **КОПИРУЮТ ОФИЦИАЛЬНЫЕ СТРАНИЦЫ** популярных курьерских служб.

**ЗАВЫШЕННЫЙ РАЗМЕР СКИДКИ** на дорогостоящие товары.

**MAKDEK**

Скидка  
**90%**

**Алгоритм действий**

Если продавец требует предоставить личные данные и провести предоплату за товар, прервите общение, **НЕ ПЕРЕВОДИТЕ ДЕНЕЖНЫЕ СРЕДСТВА НЕЗНАКОМЫМ ЛЮДЯМ.**

**Правила, которым нужно следовать, чтобы не стать жертвой мошенников**

- Пользуясь услугами сервисов по продаже новых и б/у товаров, **НЕ ПЕРЕХОДИТЕ В МЕССЕНДЖЕРЫ**, ведите всю переписку только в чате сервиса.



- Не заказывайте товар по предоплате — **СПЛАЧИВАЙТЕ ТОЛЬКО ПО ФАКТУ ПОЛУЧЕНИЯ ТОВАРА**, убедившись в его соответствии заявленным качествам и его исправности.



**ОФИЦИАЛЬНЫЙ САЙТ**  
защищенное соединение  
`https://.....`

- Проверяйте URL (уникальный адрес ресурса в сети Интернет), веб-страницы с «плохим» URL могут вести на сайт-двойник, за которым скрываются мошенники.
- Убедитесь, что используется **ЗАЩИЩЕННОЕ СОЕДИНЕНИЕ (HTTPS)** и доменное имя соответствует официальному ресурсу.

**Важно!**

- Доверяйте только официальным сайтам.
- При переходе на сайт для оплаты проверяйте адрес ресурса в интернете.
- Убедитесь, что используется защищенное соединение (значок замочка в адресной строке интернет-сайта)



FMGRAM.BE2.RU

Больше информации  
на странице ФМЦ ФГН  
и на портале  
МоиФинансы.рф



МОИФИНАНСЫ.РФ

## СХЕМА «ДРУГ В БЕДЕ»

### Легенда

Злоумышленники создают копию аккаунта знакомого или получают доступ к его аккаунту и рассылают сообщения с просьбой о помощи. Обычно речь идет о **СРОЧНОМ ДЕНЕЖНОМ ПЕРЕВОДЕ** в контексте: «попал в беду», «сломался телефон», «нужно перевести деньги, а банк не работает» и т.д. Иногда сообщение содержит просьбу перейти по ссылке и, например, проголосовать в каком-то вопросе.



### Механизм кражи денег

**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют **ПСИХОЛОГИЧЕСКИЕ ПРИЕМЫ** для управления действиями человека, в том числе посредством **ФИШИНГОВОЙ АТАКИ**.

**Фишинг** – это вид мошенничества, при котором злоумышленники маскируются под другие организации или лица и используют поддельные электронные сообщения, ссылки или сайты, чтобы завладеть денежными средствами жертвы, а также получить конфиденциальные данные (пароли, данные банковских карт, учетные записи), доступ к ее личному устройству.

## СХЕМА «ДРУГ В БЕДЕ»

### Признаки, что общение исходит от мошенников



### Алгоритм действий



Правила, которым нужно следовать, чтобы не стать жертвой мошенников



- **ПЕРЕЗВОНИТЕ** человеку и уточните ситуацию.



двухфакторная аутентификация



**ИСПОЛЬЗУЙТЕ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ**

везде, где это возможно: портал «Госуслуги», банковские приложения, платежные сервисы, мессенджеры, социальные сети.

**Важно!**

**НЕ ПОДАВАЙТЕСЬ ЭМОЦИЯМ.**  
Всегда есть риск, что аккаунт взломали.



FINPROSM.RU

Больше информации на странице ФМЦ ФГН и на портале Моифинансы.рф



MOI-FINANSY.RU

## СХЕМА «ЗНАКОМСТВО В ИНТЕРНЕТЕ»

## Легенда

Мошенник создает фальшивый профиль на сайте знакомств или в социальных сетях. Начав общение и завоевав доверие потенциальной жертвы, мошенник обращается с просьбой, которая сводится к ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ.



## Цель

Получение денежных средств от жертвы.



## Механизм кражи денег

**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ для управления действиями человека, в том числе посредством ФИШИНГОВОЙ АТАКИ.

**Фишинг** – это вид мошенничества, при котором злоумышленники маскируются под другие организации или лица и используют поддельные электронные сообщения, ссылки или сайты, чтобы завладеть денежными средствами жертвы, а также получить конфиденциальные данные (пароли, данные банковских карт, учетные записи), доступ к ее личному устройству.



## Признаки, что общение исходит от мошенников

При изучении профиля собеседника на сайте знакомств или в социальных сетях, есть несколько признаков, на которые следует обратить внимание:



## Алгоритм действий



- Если общение с собеседником на сайте знакомств или в соцсетях отвечает обозначенным выше признакам, прекратите общение.
- Обратитесь в официальную службу поддержки сайта знакомств для проверки аккаунта собеседника.

## Правила, которым нужно следовать, чтобы не стать жертвой мошенников

- Никогда **НЕ РАЗГЛАШАЙТЕ** свои персональные данные (номер паспорта, СНИЛС).
- **НЕ ОБЩАЙТЕСЬ** с людьми, чьи страницы кажутся Вам **ПОДОЗРИТЕЛЬНЫМИ**.



- Пользуйтесь поиском по изображениям для подтверждения личности собеседника и проверки, не используется ли одна и та же фотография под разными именами (современные поисковые системы позволяют загрузить фото и начать поиск данных).



## Важно!

- Уделяйте внимание защите своих персональных данных.
- Не переводите денежные средства по просьбе новых знакомых.



FINGRAM.RF.RU

Больше информации  
на странице ФМЦ ФГН  
и на портале  
Моифинансы.рф



MOIFINANSY.RF

## СХЕМА «ЗВОНОК ИЗ СОЦИАЛЬНОГО ФОНДА О НЕУЧТЕННОМ ТРУДОВОМ СТАЖЕ»

### Легенда

Во время проведения проверки был выявлен неучтенный трудовой стаж, который влияет на размер Вашей пенсии. Для перерасчета пенсии необходимо оформить заявление в отделении Социального фонда или в центрах госуслуг «Мои документы». В целях подтверждения записи на прием и идентификации гражданина необходимо назвать номер СНИЛС и продиктовать поступивший код из СМС-сообщения.

???

Продиктовать код из СМС-сообщения



### Цель звонка

Получить доступ к личному кабинету на портале Госуслуг.

### Механизм кражи денег

**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ для управления действиями человека.



### Признаки, что звонок исходит от мошенников



## Алгоритм действий



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников

**НИКОГДА НЕ ПЕРЕДАВАЙТЕ КОДЫ** подтверждения третьим лицам, даже если они представляются сотрудниками государственных учреждений.



## Важно!

- Все перерасчеты в пенсионной системе делаются автоматически из электронных баз других ведомств.
- Если из Социального фонда поступил звонок, значит гражданин ранее подавал заявление, указывал телефон, и по этому заявлению началась работа.
- Уведомления из Социального фонда могут приходить на портал Госуслуг или в бумажном формате — письмом.



fndram.sps.ru

Больше информации  
на странице ФМЦ ФГН  
и на портале  
МоиФинансы.рф



moifinansy.ru

## СХЕМА «ЗВОНОК ИЗ ПОЛИКЛИНИКИ»

### Легенда

— Вы давно не проходили обязательную ежегодную диспансеризацию. Необходимо срочно записаться в поликлинику. Если Вы не пройдёте обследование в ближайшее время, не сможете записаться к врачу в случае болезни. Для подтверждения записи продиктуйте код из СМС-сообщения.

???

Продиктовать код из СМС-сообщения



### Цель звонка

Получить доступ к личному кабинету на портале Госуслуг.

### Механизм кражи денег

**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ для управления действиями человека.



## Признаки, что звонок исходит от мошенников



## Алгоритм действий



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников

**НИКОГДА НЕ ПЕРЕДАВАЙТЕ** коды подтверждения третьим лицам, даже если они представляются сотрудниками государственных учреждений.



## Важно!

Записаться на прием к врачу можно через **ПОРТАЛ «ГОСУСЛУГИ»**, **ИНФОРМАЦИОННЫЙ КИОСК** в поликлинике или **ПО НОМЕРУ «122»** (бесплатный номер телефона Службы оперативной помощи гражданам).



fmgam.rsg.ru

Больше информации  
на странице ФМЦ ФГН  
и на портале  
Мои финансы.рф



moifinansy.rf

## СХЕМА «ОШИБОЧНЫЙ ДЕНЕЖНЫЙ ПЕРЕВОД»

## Легенда

На Ваш номер мобильного телефона **ПРИХОДИТ СМС-УВЕДОМЛЕНИЕ** о поступлении денежных средств на счет. Через несколько минут поступает звонок от неизвестного гражданина, который просит вернуть ошибочно переведенные денежные средства и сообщает номер телефона, по которому нужно осуществить перевод или номер банковской карты.



## Цель звонка

Получение денежных средств от жертвы или легализация денежных средств, полученных преступным путём.



## Механизм кражи денег



**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют **ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ** для управления действиями человека.

## Признаки, что общение исходит от мошенников



Всегда **ТРЕБУЮТ БЫСТРОГО РЕШЕНИЯ**, не дают времени на размышление (деньги нужны срочно).

## НАСТОЙЧИВО

требуют произвести перевод на указанные реквизиты.



**ЗАПУГИВАЮТ** обращением в правоохранительные органы в случае отказа от перевода.



**ОБРАЩАЮТСЯ В НЕУДОБНОЕ ВРЕМЯ** (звонят рано утром, ночью, в выходные дни и праздники).



## Алгоритм действий



Подозрительный номер



Подозрительные звонки нужно **НЕМЕДЛЕННО ПРЕРЫВАТЬ**, а полученную от собеседника информацию перепроверить, **ОБРАТИВШИСЬ** в банк **ПО ОФИЦИАЛЬНОМУ НОМЕРУ ТЕЛЕФОНА**.

**ПЕРЕПРОВЕРЬТЕ** информацию – действительно ли на Вашу банковскую карту поступили денежные средства или была только СМС с поддельного номера банка.



**ЕСЛИ ВАМ НА БАНКОВСКУЮ КАРТУ ПОСТУПИЛИ ДЕНЕЖНЫЕ СРЕДСТВА, ТО СЛЕДУЕТ ОФОРМИТЬ ВОЗВРАТ ДЕНЕЖНЫХ СРЕДСТВ ОФИЦИАЛЬНО.**

Для возврата обратитесь в чат поддержки Вашего банковского приложения или позвоните в банк по номеру, указанному на Вашей банковской карте.

Возможно Вам потребуется написать заявление в Вашем банке о возврате ошибочно зачисленных денежных средств.



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников

- Всегда перепроверяйте полученную информацию.
- Позвоните в Ваш банк и подробно расскажите о подозрительном денежном переводе, который Вы получили.
- Не торопитесь пересылать деньги обратно, лучше подождать до выяснения всех обстоятельств.

**Важно!**

**ТРАТИТЬ ПОЛУЧЕННЫЕ ОТ НЕЗНАКОМЦА ДЕНЬГИ НЕЛЬЗЯ** — это может быть расценено как незаконное обогащение. Деньги необходимо вернуть владельцу.



[FMDGRAM.ORG.RU](http://fmdgram.org.ru)

Больше информации на странице ФМЦ ФГН и на портале Моифинансы.рф



[MOIFINANSY.RU](http://MOIFINANSY.RU)

## СХЕМА «ЗВОНОК ИЗ БАНКА»

## Легенда

Сотрудник «службы безопасности банка» сообщает, что по Вашей банковской карте совершены сомнительные операции и спасти деньги от незаконного перевода поможет блокировка операции или перевод средств на «безопасный» счет. Для этого необходимо продиктовать код из СМС.

???

ПРОДИКТОВАТЬ  
КОД ИЗ СМС

## Цель звонка

Получение доступа к банковскому приложению и счетам жертвы.



## Механизм кражи денег



**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ для управления действиями человека.

## Признаки, что звонок исходит от мошенников



Всегда требуют быстрого решения, не дают возможности обсудить проблему с близкими.

Создают иллюзию официальной процедуры.



Требуют назвать по телефону персональные данные (например, данные банковской карты, включая CVV-код, или пароль от приложения банка).

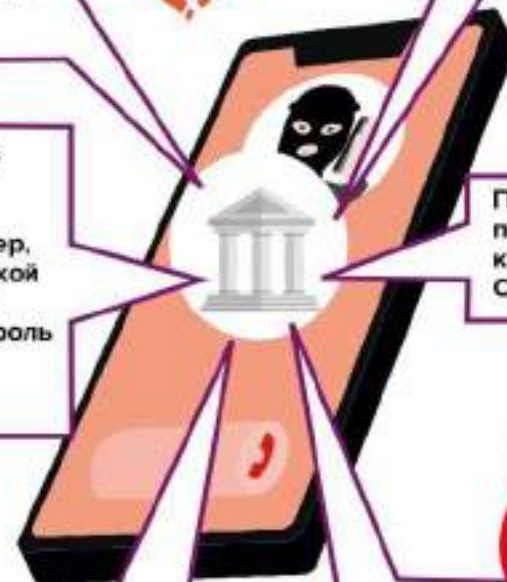
Просят продиктовать код из СМС-сообщения.



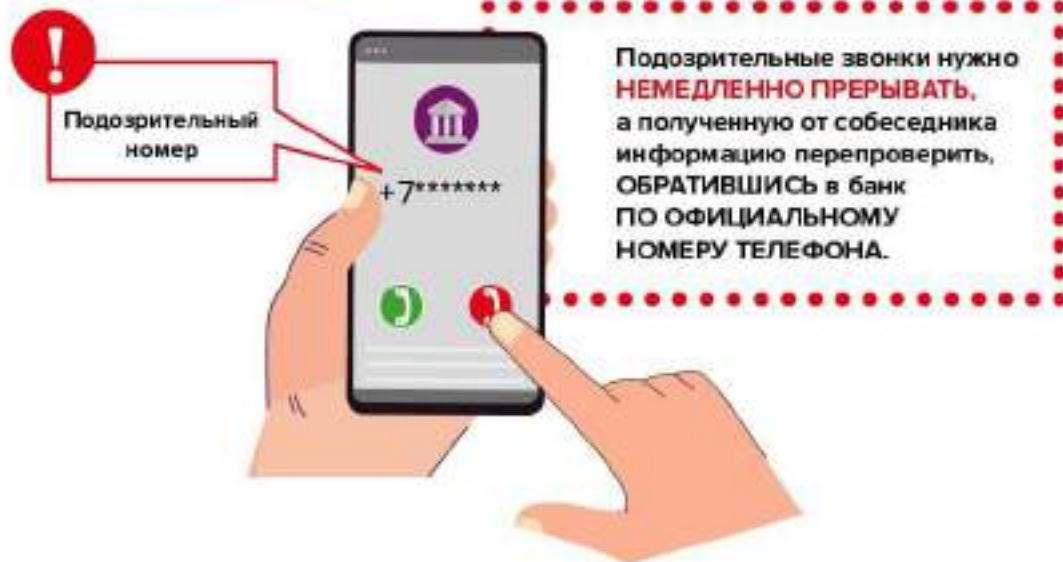
Настойчивы. Запугивают (если не перевести деньги на «безопасный» счет, ими завладеют мошенники).



Приходит СМС из банковского приложения для входа в личный кабинет или смены пароля.



## Алгоритм действий



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников



Помните, что Ваш **БАНКОВСКИЙ СЧЕТ БЕЗОПАСЕН** и **ВЫВОДИТЬ СРЕДСТВА** на другие счета **МОГУТ ПОПРОСИТЬ** только **МОШЕННИКИ**.



**НИКОГДА НЕ ПЕРЕДАВАЙТЕ** свои персональные данные и коды подтверждения третьим лицам, даже если они представляются сотрудниками банка.



## Важно!

- «Безопасных» счетов, на которые предлагают перевести деньги, не существует.
- Сотрудники банков никогда не звонят клиентам с просьбой предоставить данные карты или информацию из СМС.



[FINGRAM.RS.RU](http://FINGRAM.RS.RU)

Больше информации на странице ФМЦ ФГН и на портале МоиФинансы.рф



[MOIFINANSE.RF](http://MOIFINANSE.RF)

## СХЕМА «ЗВОНОК ИЗ СТРАХОВОЙ КОМПАНИИ»

### Легенда

— В связи с заменой полисов обязательного медицинского страхования на полисы нового образца требуется подать заявление в страховую компанию. Для подтверждений заявлений необходимо продиктовать код из СМС-сообщения. Получить готовый полис можно в офисе страховой компании, в центрах госуслуг «Мои документы» или в поликлинике.

???

Продиктовать код из СМС-сообщения



### Цель звонка

Получить доступ к личному кабинету на портале Госуслуг.



### Механизм кражи денег



**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ для управления действиями человека.

## СХЕМА «ЗВОНОК ИЗ СТРАХОВОЙ КОМПАНИИ»

### Признаки, что звонок исходит от мошенников



## Алгоритм действий



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников

## НЕ СООБЩАТЬ ПО ТЕЛЕФОНУ

- код из СМС-сообщения
- свои персональные данные.



## Важно!

Полисы ОМС являются **БЕССРОЧНЫМИ**, их замена **НЕ ТРЕБУЕТСЯ**.



FNDPAM.122.RU

Больше информации на странице ФМЦ ФГН и на портале Моифинансы.рф



MOIFINANSEY.RF

## СХЕМА «ЗВОНОК О «ПОЛУЧЕНИИ СКИДОК НА ЖИЛИЩНО-КОММУНАЛЬНЫЕ УСЛУГИ»

### Легенда

— В связи с новыми правилами начислений оплаты за жилищно-коммунальные услуги был расширен список лиц, имеющих право на льготы по оплате таких услуг. В связи с невысоким уровнем дохода и ростом тарифов на ЖКУ, Вам предоставлено право оформить скидку на оплату коммунальных услуг. Для этого необходимо подать заявление дистанционно и уже со следующего месяца скидка будет учтена в квитанции. Для подтверждения заявления продиктуйте код из СМС-сообщения.

???

Продиктовать код из СМС-сообщения

### Цель звонка

Получить доступ к личному кабинету на портале Госуслуг.

### Механизм кражи денег

**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ для управления действиями человека.

## СХЕМА «ЗВОНОК О «ПОЛУЧЕНИИ СКИДОК НА ЖИЛИЩНО-КОММУНАЛЬНЫЕ УСЛУГИ»

### Признаки, что звонок исходит от мошенников

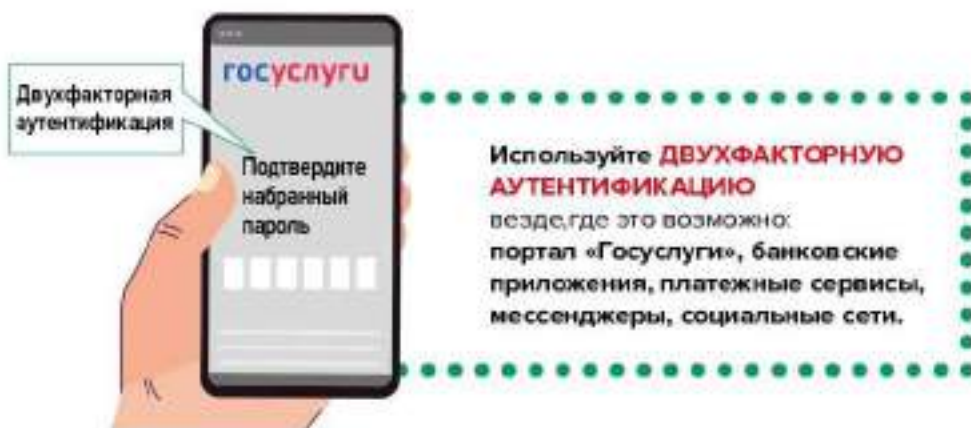


## Алгоритм действий



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников

**НИКОГДА НЕ ПЕРЕДАВАЙТЕ КОДЫ** подтверждения третьим лицам, даже если они представляются сотрудниками государственных учреждений.



## Важно!

- Представители управляющей компании, местной администрации или коммунальных предприятий, предоставляющих услуги ЖКХ, как правило **не обзывают граждан для оформления льгот и скидок на оплату услуг.**
- Получить информацию о возможных льготах на оплату жилищно-коммунальных услуг можно в центрах госуслуг «Мои документы» или на портале «Госуслуги».

**МОИ ДОКУМЕНТЫ**  
государственные  
и муниципальные услуги

**ГОСУСЛУГИ**



fmgam.ves.ru

Больше информации  
на странице ФМЦ ФГН  
и на портале  
Моифинансы.рф



МОИФИНАНСЫ.РФ

## СХЕМА «ОБНОВЛЕНИЕ БАНКОВСКОГО ПРИЛОЖЕНИЯ»

## Легенда

В связи с усилением мер информационной защиты данных клиентов, банк обновил свое мобильное приложение. Вам необходимо установить новое приложение, перейдя по ссылке в направленном СМС-сообщении или в сообщении, направленном через мессенджер.

???  
ПЕРЕЙТИ  
ПО ССЫЛКЕ  
ИЗ СМС



## Цель звонка

Получение доступа к банковскому приложению и счетам жертвы.



## Механизм кражи денег



## ПОДКЛЮЧЕНИЕ УДАЛЁННОГО ДОСТУПА.

Злоумышленники просят пользователя установить приложение, которое даёт мошенникам доступ ко всем банковским приложениям, установленным на смартфоне, и пользователь лишается средств.

## Признаки, что звонок исходит от мошенников



Всегда **ТРЕБУЮТ БЫСТРОГО РЕШЕНИЯ**, не дают возможности обсудить проблему с близкими.

**СОЗДАЮТ ИЛЛЮЗИЮ** официальной процедуры.



**ПРОСЯТ СКАЧАТЬ ПРИЛОЖЕНИЕ** из неизвестного источника.

Пройдите по ссылке: HTTPS://\*\*\*\*

**ПРОСЯТ ПРОДИКТОВАТЬ КОД** из СМС-сообщения.



Приходит СМС из банковского приложения для входа в личный кабинет или смены пароля.



код: 745281

**НАСТОЙЧИВЫ. ЗАПУГИВАЮТ** (если приложение не обновить, Вы потеряете доступ к своим счетам).



## Алгоритм действий



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников



Если банковское приложение перестало корректно работать, Вы можете обратиться в ближайший клиентский офис и попросить помочь решить проблему.

ОФИС  
БАНКА



fngbank.ru

Больше информации на странице ФМЦ ФГН и на портале МоиФинансы.рф



moifinansy.ru

## СХЕМА «ОБНОВЛЕННЫЕ БАНКНОТЫ»

### Легенда

В связи с обновлением банкнот номиналом 100 рублей, 1 000 и 5 000 рублей, участились случаи обращения поддельных банкнот. Необходимо проверить подлинность купюр через специальное приложение «Банкноты Банка России». Данное приложение необходимо установить, перейдя по ссылке в направленном sms-сообщении или в сообщении, направленном через мессенджер. Если вы выясните, что у гражданина на руках имеются поддельные купюры, их можно будет обменять в банке, в противном случае гражданин может быть привлечен к ответственности за использование поддельных купюр.

???  
ПЕРЕЙТИ  
ПО ССЫЛКЕ  
ИЗ СМС



### Цель звонка

Получение доступа к банковскому приложению и счетам жертвы.



### Механизм кражи денег

Подключение удалённого доступа и фишинг.

**Фишинг** – это вид мошенничества, при котором злоумышленники маскируются под другие организации или лица и используют поддельные электронные сообщения, ссылки или сайты, чтобы завладеть денежными средствами жертвы, а также получить конфиденциальные данные (пароли, данные банковских карт, учетные записи), доступ к ее личному устройству.



## СХЕМА «ОБНОВЛЕННЫЕ БАНКНОТЫ»

### Признаки, что звонок исходит от мошенников



Всегда требуют быстрого решения, не дают возможности обсудить проблему с близкими.

Создают иллюзию официальной процедуры.



Просят скачать приложение из неизвестного источника.

Просят продиктовать код из СМС-сообщения.



Пройдите по ссылке: HTTPS://\*\*\*\*



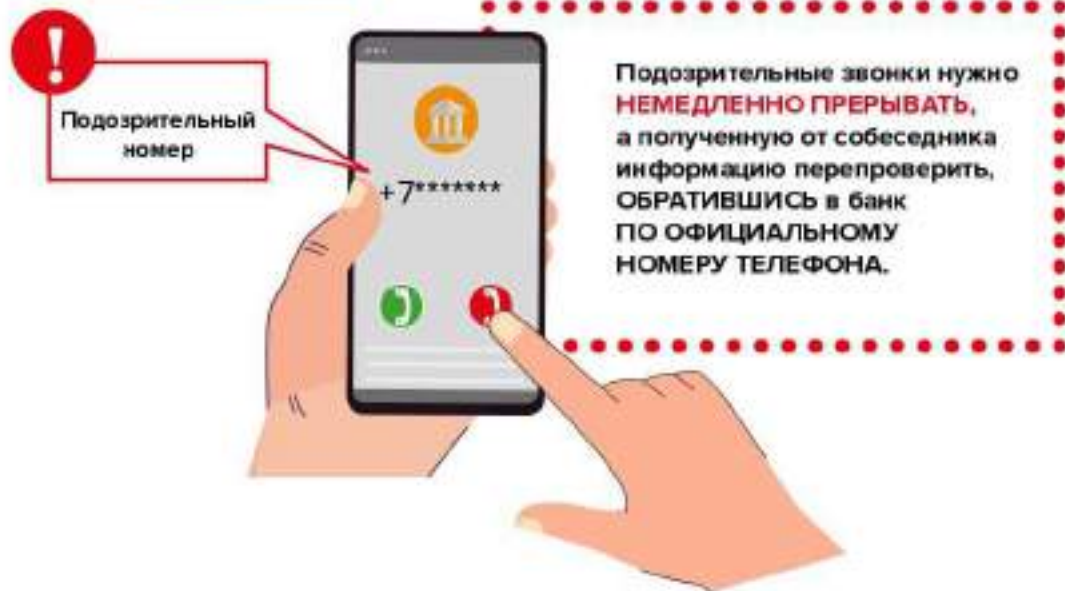
Приходит СМС из банковского приложения для входа в личный кабинет или смены пароля.



Настойчивы. Запугивают (если у гражданина будут выявлены поддельные купюры, его привлекут к ответственности).



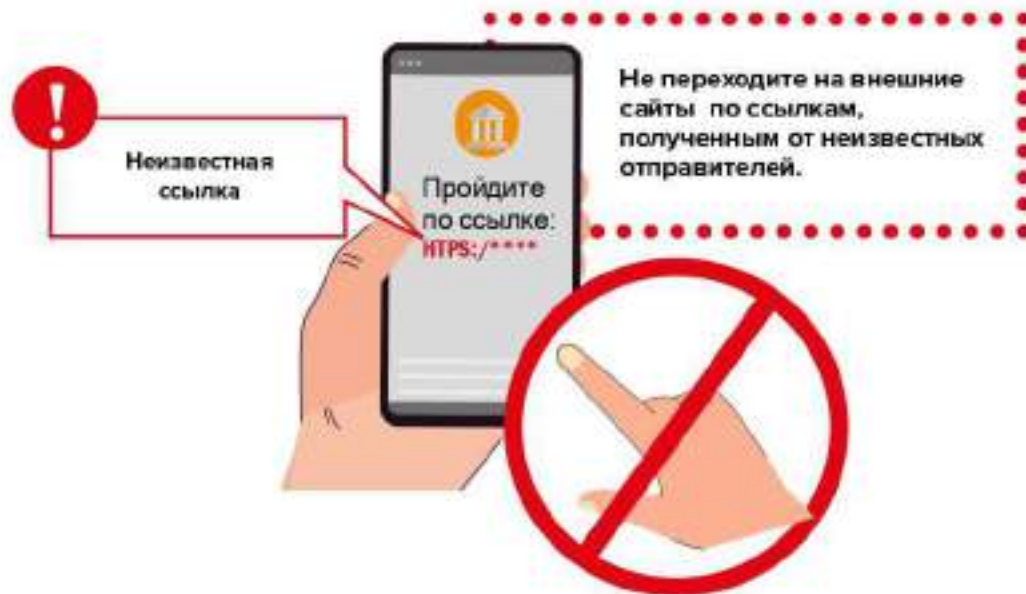
## Алгоритм действий



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников



Всегда **ПЕРЕПРОВЕРЯЙТЕ** полученную информацию. Свяжитесь по официальному каналу связи с той организацией, откуда Вам позвонили.



## Важно!

Официальное приложение «Банкноты Банка России» существует, но подлинность банкнот не определяет.

Приложение содержит информацию об основных защитных признаках банкнот — где именно они расположены и как должны выглядеть. Приложение доступно на официальном сайте Банка России.

«Банкноты  
Банка  
России»

FINGRAM.RS.RU

Больше информации  
на странице ФМЦ ФГН  
и на портале  
Моифинансы.рф



МОИФИНАНСЫ.РФ

## СХЕМА «ЦИФРОВОЙ ДВОЙНИК РУКОВОДИТЕЛЯ»

### Легенда

В мессенджер поступает сообщение от имени **руководителя организации** (для этого злоумышленники делают «двойник» аккаунта руководителя), в которой работает потенциальная жертва. В сообщении **псевдоруководитель организации** обращается с просьбой о помощи в решении проблемы или сообщает о проблемах самой жертвы.

Возможные варианты легенды:

- сбор средств с сотрудников в целях временной помощи организации с обещанием последующего возврата денег с вознаграждением;
- утечка персональных данных работников и необходимость помещения денег сотрудников на «безопасные» счета;
- допущенная сотрудником (жертвой) ошибка, из-за которой компания **потерпела убытки** или **получила штраф** от контролирующих органов, который должна взять на себя жертва.



### Цель звонка

Получение денежных средств от жертвы.



### Механизм кражи денег

**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Мошенники используют **ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ** для управления действиями человека.



### Что такое «цифровой двойник руководителя»?



ЭТО ВИРТУАЛЬНАЯ КОПИЯ РЕАЛЬНОГО РУКОВОДИТЕЛЯ, СОЗДАННАЯ НА ОСНОВЕ ЕГО ДАННЫХ, для взаимодействия в рабочих ситуациях. Но мошенники используют его как поддельный аккаунт руководителя в мессенджерах.

### Признаки, что звонок исходит от мошенников



## Алгоритм действий



## Правила, которым нужно следовать, чтобы не стать жертвой мошенников



Помните, что **РАБОТОДАТЕЛЬ НЕ МОЖЕТ ТРЕБОВАТЬ** от сотрудников **ПЕРЕВОДИТЬ СРЕДСТВА** в качестве помощи организации или **ВЫВОДИТЬ СРЕДСТВА** на «безопасные» счета.

## Правила, которым нужно следовать, чтобы не стать жертвой мошенников

**НИКОГДА НЕ ПЕРЕДАВАЙТЕ** свои персональные сведения и коды подтверждения третьим лицам, даже если они представляются сотрудниками государственных учреждений или представителями компании-работодателя.

## Важно!

Вы всегда **МОЖЕТЕ СВЯЗАТЬСЯ** с написавшим Вам руководителем иным **ПРОВЕРЕННЫМ СПОСОБОМ**. Если такой возможности нет, стоит задуматься, будет ли Вам лично писать руководитель, с которым нет прямой связи.



FMDAM.RU

Больше информации  
на странице ФМЦ ФГН  
и на портале  
МоиФинансы.рф



MOIFINANSY.RF