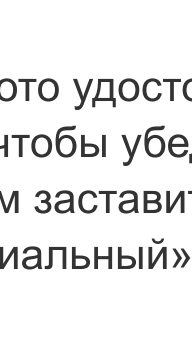




Расскажем о самых популярных мошеннических схемах и способах себя обезопасить.



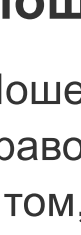
## ЗВОНКИ ИЗ ПОЛИЦИИ И ЦЕНТРАЛЬНОГО БАНКА

### Мошенническая схема

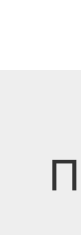
Злоумышленники представляют себя сотрудниками государственных правоохранительных органов и силовых структур или Центрального банка и сообщают о сомнительных операциях, якобы совершаемых по счету или карте.

Мошенники могут направить фото удостоверения сотрудника правоохранительных органов, чтобы убедить в правдоподобности своих действий и в дальнейшем заставить жертву оформить кредит и перевести средства на «специальный», «безопасный» счет.

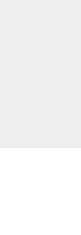
### ПОМНИТЕ



Сотрудники Центрального банка Российской Федерации **НИКОГДА** не звонят физическим лицам!

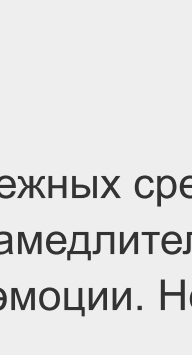


Банк России не работает с физическими лицами как с клиентами и не ведет их счета.



Сотрудники государственных правоохранительных и силовых структур (МВД, ФСБ и т. д.) **НИКОГДА** не принуждают клиента оформить кредит, чтобы проверить сотрудников банка на причастность к мошенничеству!

- При поступлении такого телефонного звонка немедленно прервите разговор.
- В случае любых сомнений относительно сохранности денег на Вашем банковском счете самостоятельно позвоните в банк.



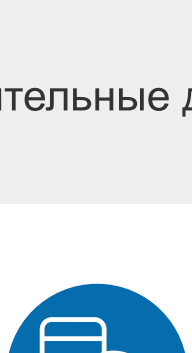
## МОШЕННИЧЕСТВО С ОБВИНЕНИЕМ В ГОСИЗМЕНЕ

### Мошенническая схема

Мошенники, представляя себя сотрудниками государственных правоохранительных и силовых структур пытаются убедить клиентов в том, что сотрудник банка украл их персональные данные и от их лица спонсировал террористические организации, за что пострадавшим грозит уголовное дело об измене Родине.

### ПОМНИТЕ!

- Такие звонки могут поступать только от злоумышленников, поэтому никогда не верьте подобным обвинениям и сразу прекращайте любые разговоры!



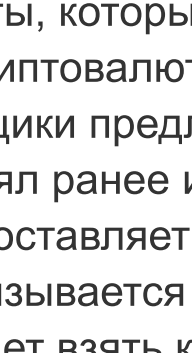
## УГРОЗА КАК МЕТОД МОШЕННИЧЕСТВА

### Мошенническая схема

Мошенники, заполучив данные потенциальной жертвы (например, номер телефона, имя, адрес проживания) совершают звонки с угрозой причинения вреда жизни и здоровью, а также могут угрожать безопасности близких потенциальной жертвы. Как правило, злоумышленники озвучивают требование немедленно перевести им на счет определенную сумму денег и дают достаточно короткие сроки для исполнения данного требования.

### ПОМНИТЕ!

- С целью получения денежных средств мошенники всегда просят действовать незамедлительно, пытаются напугать и вывести человека на эмоции. Не поддавайтесь!
- Постарайтесь записать разговор с подозрительным лицом и обратитесь в полицию.



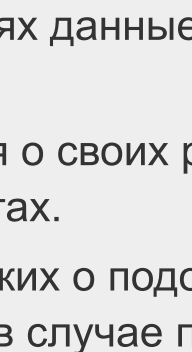
## ПРЕДЛОЖЕНИЯ О РАБОТЕ

### Мошенническая схема

Мошенники рассылают в разные каналы коммуникаций предложения о работе с заманчивыми условиями. Цель мошенников выманить у соискателя деньги за возможность начать работу или заставить вложить собственные средства. При этом они могут предложить подписать трудовой договор. Мошенники гарантируют, что вложения будут возвращены потенциальному сотруднику в большем объеме.

### ПОМНИТЕ!

- Если Вас просят за что-либо заплатить перед началом работы, это должно насторожить. Вы ни за что не должны платить. Не предоставляйте свои персональные данные и данные своей банковской карты в ответ на подобные предложения о работе.
- Не подписывайте сомнительные договоры.



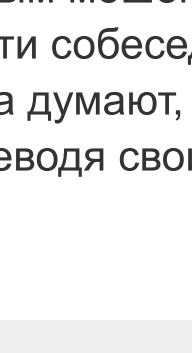
## ЗВОНКИ ОТ СОТРУДНИКОВ БАНКА ПО ВИДЕОСВЯЗИ

### Мошенническая схема

Мошенники стали звонить по видеосвязи, представляя себя сотрудниками банков и имитируя работу в офисе. Первый звонок идет по обычной телефонной связи — если собеседник не верит, то мошенник переключает уже по видео, чтобы убедить потенциальную жертву в правдоподобности своих действий и в дальнейшем перевести средства на «специальный» или «безопасный» счет.

### ПОМНИТЕ!

- Сотрудники Ситибанка **НИКОГДА** не общаются с клиентами в мессенджерах (WhatsApp, Viber, Telegram и т. п.)!
- При поступлении такого телефонного или видеозвонка немедленно прервите разговор.
- В случае любых сомнений относительно сохранности денег на Вашем банковском счете самостоятельно позвоните в банк по номеру который указан на обратной стороне вашей карты.



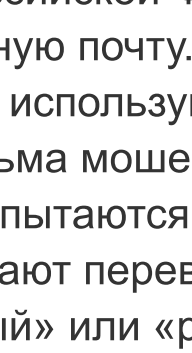
## ПРЕДЛОЖЕНИЕ ВЕРНУТЬ ПОТЕРЯННЫЕ В РЕЗУЛЬТАТЕ МОШЕННИЧЕСТВА ДЕНЬГИ

### Мошенническая схема

Злоумышленники создают сайты, которые «помогают» вернуть деньги, потерянные из-за фейковых криптовалютных брокеров и других интернет-мошенников. Обманщики предлагают за две недели вернуть деньги, которую генерирует нейросеть с использованием имени и фамилии того человека, чей аккаунт был взломан, номер карты вставляется мошеннический. Фото фейковой карты используется для того, чтобы у человека, с которым мошенник ведет диалог, не возникло никаких сомнений в подлинности собеседника. Тем самым жертвы подобного рода мошенничества думают, что помогают своему знакомому/другу, по факту перевода свои денежные средства злоумышленникам.

### ПОМНИТЕ!

- Подобные предложения — обман. Цель мошенников — узнать данные карты и заполнить денежные средства.
- Не вводите свои персональные данные и данные своей банковской карты на подозрительных сайтах.
- Не оформляйте кредитные продукты под давлением третьих лиц.



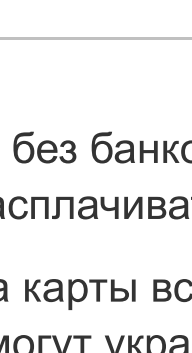
## МОШЕННИЧЕСТВО ЧЕРЕЗ ЗВОНКИ РОДСТВЕННИКАМ

### Мошенническая схема

В последнее время участились случаи, когда мошенники стали звонить родственникам потенциальной жертвы, если та не поддается убеждениям перевести деньги на «безопасный» счет. Через родственников уверяют потенциальную жертву все-таки совершить операцию. Телефоны родных злоумышленники находят в соцсетях, «слитых» базах данных. Схема более опасна, поскольку усиливает воздействие на человека.

### ПОМНИТЕ!

- Не указывайте в соцсетях данные близких Вам людей и кем они Вам приходятся.
- Не оставляйте сведения о своих родных и друзьях на подозрительных сайтах.
- Проинформируйте близких о подобном виде мошенничества, чтобы в случае получения звонка от злоумышленников, они не поддавались на их манипуляции и прекратили разговор.



## ПОДЕЛЬНОЕ УДОСТОВЕРЕНИЕ О ПОДТВЕРЖДЕНИИ ЛИЧНОСТИ КВАЛИФИЦИРОВАННОГО СОТРУДНИКА БАНКА

### Мошенническая схема

Злоумышленники представляют себя сотрудниками банка и сообщают о сомнительных операциях, якобы совершаемых по счету или карте. Мошенники через мессенджер могут направить фото удостоверения о подтверждении личности квалифицированного сотрудника банка, чтобы убедить жертву в правдоподобности своих действий и в дальнейшем заставить ее перевести средства на «специальный» или «безопасный» счет.

### ПОМНИТЕ!

- Сотрудники Ситибанка **НИКОГДА** не общаются с клиентами и не отправляют документы посредством мессенджеров (WhatsApp, Viber, Telegram и т. п.)!
- При поступлении такого звонка немедленно прервите разговор и самостоятельно перезвоните в банк.



## МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТИ

### Мошенническая схема

Мошенники взламывают аккаунты в мессенджерах и соцсетях и от лица владельца аккаунта просят его знакомых/друзей под различными предлогами перевести денежные средства якобы на карту. Для правдоподобности злоумышленники отправляют фото самой карты, которую генерирует нейросеть с использованием имени и фамилии того человека, чей аккаунт был взломан, номер карты вставляется мошеннический. Фото фейковой карты используется для того, чтобы у человека, с которым мошенник ведет диалог, не возникло никаких сомнений в подлинности собеседника. Тем самым жертвы подобного рода мошенничества думают, что помогают своему знакомому/другу, по факту перевода свои денежные средства злоумышленникам.

### ПОМНИТЕ!

- Перед тем как отправлять денежные средства друзьям/знакомым/родственникам по просьбе из соцсетей или мессенджеров, позвоните им по телефону для подтверждения информации.



## ПРОСЬБА ПРОГОЛОСОВАТЬ, ПРОИДЯ ПО ССЫЛКЕ

### Мошенническая схема

Мошенники стали присылать сообщения в соцсетях/мессенджерах якобы от Ваших знакомых с просьбой проголосовать за участника в рамках конкурса. В сообщении присутствует ссылка, содержащая вирус. Если Вы пройдете по ссылке, есть риск, что мошенники могут заполучить Ваши банковские данные, т. к. различные платежные сервисы на базе мессенджеров подвержены подобным атакам.

### ПОМНИТЕ!

- Не важно, от кого Вы получили сообщение — к **ЛЮБЫМ** ссылкам относитесь осторожно.
- Перед тем как прийти по ссылке, проверьте ее в открытых источниках на предмет безопасности.
- Свяжитесь с отправителем посредством звонка и уточните, отправлял ли он Вам сообщение.



## ПРИГЛАШЕНИЕ НА ЛИЧНЫЙ ПРИЕМ В ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

### Мошенническая схема

Злоумышленники стали приглашать потенциальных жертв на «личный прием в Центральный банк Российской Федерации», предварительно отправляя письмо на электронную почту. Такое персональное приглашение злоумышленники используют как повод начать диалог с жертвой. После отправки письма мошенники звонят получателю и под различными предлогами пытаются получить данные банковской карты и СМС-код, либо побуждают перевести денежные средства на «безопасный», «специальный» или «резервный» счет.

### ПОМНИТЕ!

- Сотрудники Центрального банка Российской Федерации **НИКОГДА** не взаимодействуют с физическими лицами.
- Не сообщайте третьим лицам одноразовые пароли, ПИН-код, ТПИН-код, CVC/CCV (трехзначный код безопасности на обратной стороне карты), коды безопасности.



## МОШЕННИЧЕСТВО С «ПРОСРОЧЕННЫМИ» SIM-КАРТАМИ

### Мошенническая схема

Злоумышленники придумали новую легенду, которая позволяет получить доступ в личные кабинеты абонентов мобильных операторов. Человеку поступает звонок якобы от оператора мобильной связи с предупреждением, что заканчивается срок SIM-карты. Для продления просят указать код из сообщения. Затем мошенники делают переадресацию звонков и SMS на другой номер или виртуальный дубликат SIM-карты. Далее они могут проникнуть в онлайн-банк жертвы, почту, мессенджеры, соцсети и даже в личный кабинет на портале Госуслуг.

### ПОМНИТЕ!

- При поступлении подобного звонка прервите разговор и перезвоните самостоятельно мобильному оператору по подтвержденному номеру телефона, который можно найти на официальном сайте оператора.
- Не предоставляйте третьим лицам коды безопасности и другую конфиденциальную информацию.

Сегодня сложно выйти из дома без банковской карты, ведь забыв ее, Вы будете вынуждены везде расплачиваться наличными.

Именно в такой ситуации, когда карты всегда под рукой, особенно велик риск их потерять. Карту могут украсть, ее можно забыть или выронить в неудачном месте. Этого можно даже не заметить, пока Вам не придет неожиданное уведомление о списании средств.



Поэтому, если Вы не можете найти свою карту, сразу заблокируйте ее через Citibank® Online\* или звоните в нашу службу поддержки:  
+7 (495) 775-75-75 — в Москве,  
+7 (812) 336-75-75 — в Санкт-Петербурге,  
8 (800) 700-38-38 — для звонков из других городов РФ.

## СЛЕДИТЕ ЗА СВОИМИ КАРТАМИ, ЧТОБЫ ВСЕГДА КОНТРОЛИРОВАТЬ СВОИ ФИНАНСЫ!

С заботой,  
Ваш Ситибанк.



\* Онлайн.  
АО КБ «Ситибанк».