



РОСКОМНАДЗОР

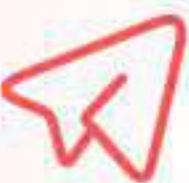
Осторожно, мошенники

Раскрываем
популярные схемы
злоумышленников



Сообщение от босса в Telegram

Злоумышленники представляются высшими руководителями организаций и их заместителями. Для этих целей используют **ложные аккаунты в Telegram**.



Мошенники сообщают об утечке персональных данных в организации и просят оказать содействие **«следователям»**.



Дальше полицейские сообщают о мошеннических кредитах, которые оформили на имя человека, обещают разобраться в вопросе и **выманивают деньги**.



Звонок от оператора сотовой связи

Схема 1

Заканчивается срок действия договора на сотовую связь.
Номер будет заблокирован.



Схема 2

От имени абонента подали заявку на **перенесение номера** к другому оператору (услуга MNP).



Чтобы избежать «неприятностей», продиктуйте **СМС-код**.



С помощью кода преступники получают доступ к номеру жертвы, а следовательно, к **личному кабинету** банков, Госуслуг и других сервисов.



Помните, что договор с оператором связи бессрочный!
При всех подозрительных звонках свяжитесь с вашей компанией по официальным каналам.



Звонок из банка

Мошенники звонят и сбрасывают звонок в ожидании того, что им перезвонят.



Если это происходит, звонящий слышит музыку из рекламного ролика банка.



Дальше стандартная схема: убеждают назвать код из СМС или сообщить логин и пароль для входа в учетную запись онлайн-банка. Мошенники получают доступ к счету клиента и выводят с него деньги.



Звонок от сотрудника силовых органов

● «Вам грозит до 20 лет тюрьмы!»
С такой фразы начинается разговор.



“Сотрудник» органов заявляет, что кто-то украл ваши данные и сделал перевод для помощи иностранному государству в деятельности против России. А это квалифицируется как **госизмена**.



••• Чтобы вычислить «предателя», нужно **перевести средства** на некий счет. Иногда и этого мало. Злоумышленники начинают шантаж и втягивают человека в противоправные действия.



Звонок от сотрудника Госуслуг

Мошенники сообщают, что на ваше имя пришло **электронное письмо**.



Чтобы оно отобразилось в личном кабинете на «Госуслугах», нужно назвать **код из СМС**.

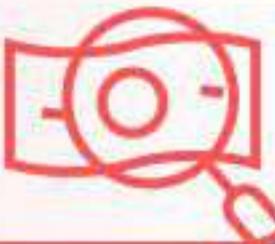


Злоумышленники получают **доступ к аккаунту**. Могут сменить пароль, запросить кредитную историю, получить справку о доходах, информацию о транспортных средствах или оформить займ.



Звонок из ЦБ

Мошенники предлагают **проверить подлинность обновленной пятитысячной купюры.**



Предлагают установить на телефон **приложение «Банкноты Банка России».**



Вместе с приложением пользователи скачивают **вредоносную программу.**



Звонок из пенсионного фонда

Легенда: подтвердите **списание** всех накопленных средств/вам **не начислили** доплаты/**выплатили** слишком много.



К пенсионерам обращаются по имени и отчеству, втираются в доверие и начинают **запугивать**.



Цель: получить доступ к личному кабинету, уговорить перевести деньги на другую банковскую карту или установить предлагаемый номер мобильного телефона в качестве доверительного, что позволит аферистам войти в мобильный банк пенсионера.

