

*****18-летний студент из Новороссийска стал жертвой сложной схемы мошенничества, в результате чего со счета его матери было похищено около 2 миллионов рублей. Юноше позвонила незнакомка, представившись сотрудницей учебного отдела вуза. Она попросила принести копию паспорта и спросила, прошел ли он регистрацию на образовательном сервисе. Получив ответ «нет», она выслала ему код для «регистрации» и попросила его продиктовать.**
*****Через полчаса студенту позвонил другой человек, назвавшийся сотрудником правоохранительных органов и обвинил его в разглашении КОДа и персональных данных. Общение продолжилось в мессенджере, где по видео-звонку парень увидел мужчину в форме. Тот заявил, что студент является подозреваемым по делу о «пособничестве вражескому режиму», и потребовал полной конфиденциальности. Мошенник, узнав, что юноша дома с матерью, дал указание провести «дистанционный обыск». Студент взял телефон матери, пока она спала, перевел её деньги на свой счет, а затем по инструкции установил на свой смартфон вредоносный APK-файл**
, маскирующийся под программу для «считывания операций».
*****Под руководством злоумышленника студент снял в банкомате всю сумму (около 2 млн рублей) наличными. Далее, полагая, что таким образом деньги «задекларируют» и вернут на карту, он снова вносил наличные в купюроприемник. Вредоносная программа на телефоне эмулировала пополнение счета, но на самом деле средства уходили мошенникам.**

В Управлении МВД России по городу Новороссийску объяснили, что это технически сложная схема.

Её первая часть стандартна: получение конфиденциальных данных (кода) и запугивание.

Вторая часть использует социальную инженерию и вредоносное ПО для перенаправления денег.

Новороссийские полицейские рекомендуют:

· Никогда не скачивайте и не устанавливайте APK-файлы. Пользуйтесь только официальны
· Банк никогда не попросит вас установить специальное приложение по ссылке из SMS или
· Не выполняйте операции в банкоматах по указанию «службы поддержки» или незнакомц