«Спецоперация».

Одна из распространенных схем, при которой жители республики несут самые большие финансовые потери – звонок от псевдо-сотрудника банка или правоохранительного органа о том, что деньги гражданина находятся под угрозой хищения для предотвращения которого необходим перевод сбережений на «безопасный счет». Либо сообщение о том, что злоумышленники взяли на имя потерпевшего кредиты. Для предотвращения потери денег (исковых требований банка-кредитора) предлагается оформить кредит (зачастую несколько, в разных кредитных учреждениях). Полученные наличные деньги предлагается перевести на «безопасные счета» через банкоматы. Аналогичным образом происходят хищения под предлогом участия в «специальной операции».

Приведем типичный пример. Гражданин С., причем сам являющийся сотрудником регионального банковского учреждения, в вечернее время вступил в телефонный разговор с «псевдо» сотрудником сотовой компании, по поводу истечения срока договора абонентского обслуживания. Поскольку офисные помещения оператора сотовой связи уже были закрыты звонивший предложил продлить договор дистанционно. С. согласился и перевел полученный СМС-код звонившему. Вместе с тем, обладая информацией о мошенниках, тут же опомнился, заподозрив, что передал код от личного кабинета Госуслуг. Однако тут же потерпевшему позвонило лицо, представившееся оператором Госуслуг и сообщило, что в его личном кабинете происходят подозрительные финансовые операции, а именно в короткий промежуток времени оформлены заявки на получение крупных сумм кредитов в различных банках и попросило подтвердить эти заявки. С. сообщил о возникшей ситуации с мошенниками, после чего оператор перевел звонок на службу безопасности Центрального банка России. В свою очередь работник Нацбанка сообщил, что организована оперативная комбинация по изобличению группы мошенников и С. необходимо принять участие в ней. При этом свои слова сотрудник Центробанка подкреплял направлением различных документов с реквизитами государственного учреждения, гербовыми печатями, цифровыми и обычными подписями. Из убедительных слов, подкрепляемых документами, следовало, что на имя С. открыт безопасный счет. Для предотвращения несанкционированного кредитования необходимо получить встречные кредиты в различных банках и перевести полученные деньги на этот счет. В дальнейшем в разговор включались сотрудники ФСБ и МВД, один из которых вел разговор с С. по видеосвязи. Итогом массированной психологической обработки стала уверенность С. в том, что он принимает участие в специальной операции, проводимой правоохранительными органами. Затем, в течении последующих трех дней С., также находясь под постоянным воздействием звонивших, оформил три крупных кредита в разных банках на сумму свыше 8 млн. рублей. Полученные наличные деньги, в рамках проводимой «специальной операции», С. тут же относил в банкомат и партиями менее 100 тыс. руб. переводил на различные банковские карты указанные ему, каждый раз получая документ о их зачислении на безопасный счет. После этого связь оборвалась и С. понял, что стал жертвой обмана.

Необходимо отметить, что аналогичные преступления регистрируются практически ежедневно. Несколько различается способ вовлечения потерпевшего в комбинацию. В последнее время фиксировались факты создания лже-аккаунтов руководителей организации, где работает потерпевший в мессенджерах (WhatsApp, Telegram) и сообщение-просьба от этого руководителя поговорить с сотрудниками Центробанка, ФСБ или МВД по поводу некой ситуации возникшей в коллективе. Затем следует звонок от представителя правоохранительного органа с сообщением о финансировании ВСУ со счета потерпевшего, либо как в приведенном выше случае – оформление несанкционированных кредитов. Далее следует стандартная схема по направлению денег на «безопасный» счет.

Также мошенники очень активно начали действовать от имени работников операторов сотовой связи, ресурсоснабжающих организаций (Энергосбыт, Водоканал) под различными предлогами, такими как необходимость продления срока сим-карты, замена счетчиков (электроприборов). В ходе общения мошенники предлагают оформить заявку по телефону, требуя сообщения им кода (якобы номера заявки, очереди), поступившего на телефон потенциальной жертвы. После сообщения данного кода следует звонок от псевдосотрудника Госуслуг о взломе личного кабинета на портале, о нахождении денег в опасности, необходимости дальнейшего разговора с сотрудником Росфинмониторинга, Центробанка, МВД и ФСБ, и далее следует стандартная схема по направлению денег на «безопасный» счет.