Типовые схемы телефонного мошенничества:

«Родственник попал в беду»: неизвестное лицо, по незнакомому номеру телефона сообщает заведомо ложную информацию о том, что близкий человек совершил дорожно-транспортное происшествие либо тяжкое преступление. Избежать ненужных проблем предлагается путем перевода определенной суммы денежных средств на номер неизвестного сотового телефона или неизвестный банковский счет либо путем передачи на руки курьеру, в том числе для оказания помощи пострадавшему. Злоумышленники могут представляться сотрудниками правоохранительных органов, адвокатами либо самим попавшим в беду родственником. Чужой голос они оправдывают полученной травмой, стрессом.

«Сообщение с вредоносной ссылкой»: SMS-сообщение о зачислении средств на Ваш счет от «банка» с встроенной фишинговой ссылкой «Узнать подробности», сообщение якобы из банка с призывом перейти по ссылке, чтобы уточнить задолженность. Мошенники рассылают ссылки, которые, маскируясь под адрес реального банка, ведут на сайт-«зеркало», то есть похожий на ресурсы банка (приложение или сайты), но созданный мошенниками. Дизайн может в точности копировать реальные ресурсы, но вводя на таком «зеркале» свои данные, Вы передаете их мошенникам.

«Банковская карта заблокирована»: абоненты сотовой связи получают SMS-уведомления от «службы безопасности» банка: «Ваша банковская карта заблокирована (аннулирована)» или «Заявка на списание средств принята. Информация по телефону: +7XXXXXXXXXX. ЦБ РФ» или мошенники звонят, представляясь сотрудниками банка, сообщают о проблемах с картой. В качестве отправителя может быть

Прокуратура Брянской области

«КАК НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ»

Информационно-справочный буклет

БРЯНСК
2024

указан короткий номер, используемый в услуге "Мобильный банк", или его модификация (например, использованием прописных букв "О" вместо нулей). При последующем звонке гражданину сообщают ложную информацию о технической проблеме и предлагают для «восстановления карты» или «отмены заявки» провести ряд операций в банкомате. В итоге, деньги со счета перечисляются на номер мошенников. Или же «справочный» номер телефона «оператора банка», указанный в SMS-сообщении, оказывается платным, и гражданин, дозвонившись, теряет большую сумму со счета номера мобильного телефона.

«Покупка автомобиля и другого имущества через Интернет»: на одном из сайтов сети «Интернет» размещается информация о продаже автомобиля, дачи, другого имущества («Авто ру», «Авито» и т.д.). Подробно описывается товар, выкладываются фотографии и все это по очень привлекательной цене. Низкую стоимость злоумышленники объясняют вполне житейскими ситуациями: переезд в другой регион, семейные проблемы, финансовые трудности и т.д. Желающему приобрести товар предлагается внести задаток, поскольку на него нашлось множество покупателей или продавец находится за пределами города или даже страны, но готов вылететь для оформления сделки. Деньги злоумышленники просят перечислить переводом через банк либо на абонентский номер телефона. Получив желаемое, мошенники отключают телефон и на связь с обманутой жертвой больше не выходят.

«Операторы мобильной связи»: поступает звонок от якобы сотрудника технической поддержки оператора мобильной связи с предложением подключить новую эксклюзивную услугу или