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.

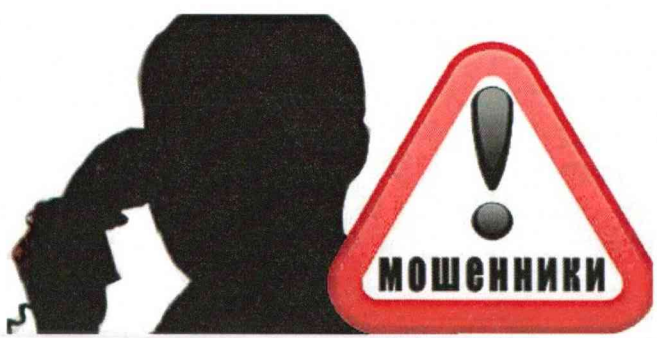
«Сообщение с вредоносной ссылкой»: SMS-сообщение о зачислении средств на Ваш счет от «банка» с встроенной фишинговой ссылкой «Узнать подробности», сообщение якобы из банка с призывом перейти по ссылке, чтобы уточнить задолженность. Мошенники рассылают ссылки, которые, маскируясь под адрес реального банка, 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

перезаключить договор во избежание отключения связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента злоумышленникам или в другом случае злоумышленники просят предоставить сведения с личного кабинета «Госуслуг» якобы с целью переоформления договора, и в случае предоставления имеют доступ ко всем персональным данным, находящихся в личном кабинете.

«Пополнение счета чужого телефона»: чаще всего речь идет о просьбе от «друга» или «ребенка» с просьбой пополнить счет того номера, откуда пришло сообщение. Другой вариант - звонок или СМС от незнакомца, который «случайно ошибся», пополняя баланс мобильного телефона, положил деньги не на свой номер, а на номер абонента, а теперь просит «вернуть» средства, пополнив счет его «мобильника». Разумеется, деньги, которыми «жертва обмана» пополняет баланс мнимого друга или «невнимательного абонента», тут же попадают на счет мошенника.

«Безопасный счет»: поступает телефонный звонок потерпевшим от «сотрудников банка или правоохранительных органов» и сообщают, что неизвестные пытаются оформить кредит на их имя. Чтобы обезопасить денежные средства мошенники предлагают перевести их на «резервные или промежуточные счета», «безопасные ячейки» и т.п. Действуя по указке злоумышленников потерпевшие снимают все свои сбережения, оформляют кредиты, а затем все суммы переводят на обозначенные аферистами банковские карты.

Как не стать обманутым:

- не давать свой телефон кому-либо постороннему с целью позвонить (якобы у незнакомца закончились деньги на телефоне);

- никогда и ни при каких обстоятельствах никому не сообщать свои персональные данные или конфиденциальную информацию: паспортные данные, PIN-код, CVV-код и другие реквизиты банковской карты, номер счета, логин и пароль от страниц в социальных сетях, на интернет-сайтах и прочее, личного кабинета на «Госуслугах»;

- задавать вопросы. Если звонящий представляется сотрудником полиции, банка, доктором поликлиники, страховым агентом, первое, что необходимо сделать, попытаться узнать как можно больше информации о собеседнике. Простые вопросы, например, фамилия и должность звонящего, из какого отделения полиции, банка или страхового агентства звонят, контактные данные руководителя организации, как найти официальный сайт, как и откуда узнал номер телефона и прочее, в том числе упоминание об уголовной ответственности за мошенничество, настоящего сотрудника не смутят, а мошенников заставят занервничать. При этом говорить необходимо негромким спокойным голосом, чтобы обманщик понял, что его разоблачили;

- прежде чем реагировать на сообщения или звонки от «родственников» или «друзей» об оказании денежной помощи, нужно попытаться дозвониться человеку, от имени которого поступило сообщение или звонок, или кому-то из его близких, с которыми он в настоящее время может находиться;

- не переходить по ссылкам, якобы присылаемым от банка;

- не спешить переводить или отдавать деньги. Требование внести денежную сумму, например, в качестве залога при розыгрыше призов или пополнить «контрольный» счет банка должно сразу насторожить;

- не откликаться на просьбу положить на счет деньги, так как по ошибке человек перевел деньги на Ваш номер;

- не перезванивать на номер, если он не знаком (если звонить оператору банка – то на номер, указанный на обороте банковской карты);

- закончить разговор в тот момент, когда только возникнет подозрение, что Вами пытаются манипулировать.

Что делать, если Вы или Ваши близкие все-таки стали жертвами мошенников:

Даже если Вас или Ваших близких обманули мошенники – обращайтесь в органы внутренних дел с заявлением. В заявлении следует максимально подробно изложить все обстоятельства произошедшего. Кроме этого, следует сообщить о факте телефонного мошенничества в абонентскую службу мобильного оператора, который обслуживает номер преступника и в Ваш банк. Принятие оператором и банком экстренных мер может позволить заблокировать перевод и вернуть деньги.

Адрес и телефоны прокуратуры Брянской области: 241023, г. Брянск, ул. А.М. Рекункова, д.1; телефон +7 (4832) 65-42-05, +7 (4832) 65-42-06.

Адрес и телефоны УМВД России по Брянской области: 241001, г. Брянск, ул. Советская, д. 102, тел. дежурной части +7 (4832) 66-70-90, телефон доверия +7 (4832) 72-22-33; телефон полиции – 02, с мобильных любых операторов – 102.