Мобильная безопасность

Разумеется, преступники не могли оставить всеобщую «мобилизацию» населения без своего внимания. В результате общество сейчас сталкивается с двумя блоками «мобильных» проблем:
- проблемы, характерные для использования любого мобильного телефона;
- проблемы, связанные с мобильным Интернетом.

Где могут обмануть?

СМС-рассылки

Простейшие схемы «мобильной разводки» работают «наудачу». Преступники **массово рассылают СМС** типа «Маша, это я, Вася. Я попал в беду. Помоги мне, надо срочно 1000 рублей!». Разумеется, текст не строго такой, его исполнение зависит лишь от фантазии жуликов. Это может быть необходимость взятки инспектору ГИБДД, отсутствие денег на поезд в другом городе, «украденный кошелек» или... все, что угодно. Обычно жулики просят перевести им **деньги с Вашего мобильного счета,** хотя особо наглые могут попросить и **данные Вашей банковской карты.**

Смысл «разводки» в том, что жертва - если, конечно, ее зовут Маша - начинает гадать, что это за Вася такой. Скорее всего, почти у каждой Маши найдется относительно хороший знакомый по имени Вася. Маша мгновенно отождествляет Васю из СМС со своим знакомым из реала и тут же переводит ему запрошенную сумму. Не особо «заморачиваясь» тем, что СМС пришла совершенно не с Васиного номера-хотя на этот случай жулик подготовит «правдоподобное» объяснение: новый номер, старый не работает, номер друга... При этом Маша, видя свое имя в СМС, ни секунды не сомневается, что сообщение адресовано именно ей - а как же иначе, если написано «Маша» и пришло именно на ее номер? Значит, ей... Впрочем, имени получателя в просьбе может и не быть вообще - такое тоже бывает сплошь и рядом.

На самом деле такие рассылки жулики обычно делают «на кого Бог пошлет». **Из тысячи разосланных СМС примерно 50-60 по законам статистики попадут к людям с тем именем, которое мошенники используют в своей рассылке.** Из этих 50-60 некоторое число все-таки «купится» на столь настойчивую просьбу - все зависит от уровня цифровой грамотности получателей. Дополнительный расчет жулики делают и на небольшие суммы, которые обычно просят мошенники (1000 рублей - для такого способа многовато, обычно просят рублей по 200-300) - дескать, даже при наличии некоторых подозрений жертва не будет особенно бояться расстаться с такой суммой. В итоге же - поскольку обманутая жертва далеко не одна - у мошенников образуется весьма немаленький капитал...

Вам может позвонить «взволнованный голос»

Он сообщит примерно то же - «голос» якобы попал в сложную жизненную ситуацию и потому вынужден просить помощи у других людей. Помощи, разумеется, денежной. Как вариант - позвонить на ту же тему от имени Вашего знакомого или родственника.

Разновидность «взволнованных голосов» - **вымогатели с программно-техническим инструментарием.** Вам точно так же может позвонить или написать случайный человек, и под неким предлогом попросить Вас ввести, допустим, логин и пароль от некоего Google-аккаунта. Вы введете - и злоумышленник, получив таким образом доступ к Вашему смартфону, тут же заблокирует Ваш телефон и потребует денег «за разблокировку». Причем во многих случаях, даже получив от Вас деньги, никто разблокировать телефон не будет. Отсюда рекомендация: посылайте с подобными просьбами «куда следует» (в службу поддержки или в полицию), если это не стопроцентно идентифицированный Вами близкий родственник. Подробнее об этом виде угрозы уже упоминалось в разделе «Электронное вымогательство».

СМС или звонок с информацией, что Вы получаете некий сногсшибательный бонус

Пожизненную подписку на некий сервис, новую онлайн-игру - опять же все зависит от фантазии жуликов, а с этим у них обычно полный порядок. Если жулик именно звонит, то он представится менеджером Вашего сотового оператора или какой-нибудь компании-партнера (банка, дистрибьютора игр и так далее). Далее Вам предложат совершить некие действия - которые на самом деле и интересуют злоумышленников. К примеру, Вам могут попросить отправить некий код на «короткий номер» - а СМС окажется стоимостью рублей в триста или больше. Короткий номер приобрести довольно легко, так что четырехзначный номер для отправки СМС - отнюдь не гарантия надежности «контрагента». Впрочем, жулики могут и прямо попросить Вас оплатить некую сумму за обещанный «бонус», а то и попросить Ваши персональные данные или данные банковской карты.

Вам может позвонить уже отнюдь не «взволнованный», а «очень строгий» голос

Он тоже представится работником сотовой компании или некоего сервиса, к которому Вы якобы подключились, и строго поведает Вам, что у Вас есть некий долг за услуги - который Вам надо срочно погасить. Для этого Вы будете должны опять же перевести куда-то некую сумму, иначе будут те или иные санкции вплоть до суда или запрета на выезд за границу. Бывают, конечно, случаи, когда мошенники представляются сотрудниками банков или коллекторами, но эта схема работает редко - человек обычно в курсе своих финансовых отношений с банками.

«Ошибочный перевод»

Схема довольно проста - Вам «прилетает» сообщение о пополнении Вашего баланса на некую сумму. Вскоре Вам напишет или позвонит некий человек, который скажет, что он ошибся при переводе денежных средств - набрал не ту цифру, и платеж якобы улетел на Ваш номер. А потому он просит вернуть ошибочно переведенную сумму, но не на тот номер, на который он якобы хотел перевести деньги, а на его собственный - причем не на тот, с которого Вам якобы поступил перевод.

Чаще всего сообщение о пополнении Вашего баланса является «липой», и никто на самом деле Вам никаких денег не переводил. А само сообщение пришло с постороннего номера - либо вообще с обычного, либо с короткого (который может быть «замаскирован» под название Вашего сотового оператора). Поэтому Вы, пойдя на поводу у мошенника, просто переводите ему свои деньги. Однако под влиянием роста цифровой грамотности абонентов мошенники тоже адаптируют свои схемы. Теперь они знают, что грамотный пользователь обязательно проверит свой настоящий баланс и историю переводов - к примеру, через свой «Личный кабинет» на сайте сотового оператора, благо смартфоны сейчас далеко не редкость. И придумали, как усыпить бдительность грамотных абонентов...

По новой схеме Вам придет уже не поддельное, а самое настоящее сообщение о переводе денег на Ваш мобильный. Вы проверите баланс, «Личный кабинет» и действительно увидите совершенный перевод. По логике мошенника, Вы успокаиваетесь и возвращаете «ошибочно» переведенные деньги на указанный мошенником номер. Однако все не так просто - получив от Вас перевод, мошенник тут же мчится в ближайший офис сотового оператора и подает заявление на возврат своего платежа. Сотовый оператор удовлетворяет просьбу, снимая эти деньги с Вашего аккаунта. Ведь он не знает, что Вы уже вернули эти деньги «в добровольном порядке»! В итоге, Вы «возвращаете» деньги дважды. Доказать же что-то в офисе сотового оператора при разборе дела вряд ли получится, так как Вы наверняка «вернете» деньги не на тот номер, с которого Вам был перевод. Поэтому лучший способ защиты - порекомендовать «ошибившемуся» самому обратиться в офис сотовой компании с заявлением на возврат ошибочного платежа. Для честного человека это никакой проблемы не составит, да и мошенник - если это все же он - останется «при своих».

Что можно сделать?

Если Вам «прилетело» подобное сообщение - не торопитесь делать все, что от Вас просят.

Для начала переберите в уме всех потенциальных знакомых с похожим именем. Затем ОБЯЗАТЕЛЬНО перезвоните им - но по тому номеру, который у Вас давно записан в телефонной книжке! И поинтересуйтесь, что у друга (подруги) за проблема и что происходит. Если друг не отвечает - не беда, можно поискать его в соцсетях, позвонить его близким или просто подождать. Но до прояснения ситуации **НИ В КОЕМ СЛУЧАЕ не переводить деньги!** 300 рублей, как известно, «не спасут гигантов мысли», а вот Ваш кошелек - вполне.

В случае звонка неизвестного попробуйте завязать разговор.

Если Вас мучает совесть, что рассказ неизвестного может быть и правдой - Выясните, какая именно проблема случилась, и поймите, как можно ее решить без перевода денег. Скажем, звонком родственникам. Предложите такой выход «взволнованному голосу». Если же он будет настаивать на деньгах, спросите просто: «Вам нужны деньги или помощь?»

Позвоните Вашему сотовому оператору по координатам, указанным на его официальном сайте, и поинтересуйтесь, что происходит.

Если у Вас действительно есть какой-то долг, то Вам о нем, разумеется, сообщат достоверную информацию - и решать возникшую проблему Вам следует именно

по достоверным координатам. Однако, скорее всего, никакого долга на самом деле нет, и Вас просто пытался атаковать очередной мошенник.

Сейчас существуют Интернет-справочники коротких номеров, которые Вам точно скажут, сколько в реальности будет стоит отправляемая на конкретный короткий номер СМС.

Если же Вам «позвонил менеджер сотовой компании», то лучше всего взять и позвонить в Вашу сотовую компанию по ее общеизвестному номеру.

И поинтересоваться у настоящего менеджера, есть ли в реальности обещанная Вам акция, спецпредложение или бонус. Если обещанное Вам - правда, то настоящий менеджер без проблем подключит Вам интересующую Вас опцию.