**Опасный звонок. Как уберечься от телефонных мошенников**

«Здравствуйте! Вас беспокоит служба безопасности банка...» Практически каждый россиянин сталкивался с подобным звонком. Кажется, это действительно уникальный случай в истории преступлений: тактика мошенников давно известна, о ней постоянно пишут в СМИ и соцсетях, эксперты с экранов телевизоров наперебой предупреждают об опасности — но люди всё равно дают себя обмануть. Как не стать жертвой злоумышленников — в нашем материале.

**Вишинг** — телефонное мошенничество, где жертву убеждают совершить какие-то действия или передать конфиденциальную информацию. Термин произошёл от сочетания двух английских слов — voice (голос) и fishing (рыбалка, выуживание).

**Фишинг** — это другой тип мошенничества, где с жертвой общаются через электронную почту, мессенджеры, соцсети или фейковые сайты. А вот при вишинге основным инструментом злоумышленников является телефон. Выглядит парадоксально: телефонная связь появилась раньше интернета, но IT-преступления намного старше вишинга. Расцвет этого вида мошенничества начался с появления IP-телефонии. На практике всё упирается в одну уязвимость протокола связи, связанную с «идентификатором вызывающего абонента» — Caller ID. Именно он отвечает за то, какой номер будет показан у абонента на экране телефона (и отражён в детализации звонков). К сожалению, Caller ID крайне легко подменить. Этим и пользуются сотрудники криминальных колл-центров. Которые, отметим, нередко располагаются за пределами нашей страны — ведь для IP-телефонии границ не существует.

Идентификатор абонента можно менять после каждого звонка, выбирая при этом абсолютно любой номер. Вам не помогут даже популярные антиспам-приложения. А значит, единственным спасением от мошенников будет ваше благоразумие.

*Вишинг бывает простым и сложным — его ещё называют целевым.*

Простое мошенничество рассчитано на широкую аудиторию. В этом случае берут числом. Жертв банально обзванивают по очереди и пытаются перехитрить по единому для всех сценарию. В данном случае злоумышленники не будут о вас ничего знать, но попытаются выведать все нужные им сведения во время атаки. Расчёт делается именно на массовость аудитории. Если один человек из ста начал общаться — это уже успех. Если пару-тройку людей из тысячи удалось обмануть, схема приносит прибыль.

Сложный вишинг начинается, когда злоумышленники располагают реальными сведениями о вас. Например, они могут знать ваше имя, в каких банках у вас есть счета, и даже адреса и имена членов семьи. Целевые атаки опасны тем, что злоумышленники могут выбрать индивидуальную стратегию, рассчитанную именно на конкретного человека и учитывающую его особенности и слабости. Это позволяет мошенникам легче войти в доверие и обеспечить себе более высокие шансы на успех. В то же время целевой вишинг является более сложным преступлением, предполагает этап подготовки и предъявляет более жёсткие требования к квалификации атакующих.

С технической точки зрения вишинг в последние годы практически не меняется. Но при этом злоумышленники постоянно адаптируют социотехнические формы его реализации — иными словами, придумывают всё новые и новые «разводки». И такая голосовая коммуникация может быть куда опаснее фейкового сайта, ведь жертву можно банально заболтать.

**«Мама, я попал в беду»**. Одна из первых в России вишинговых схем. Жертве поступает звонок якобы от члена семьи, или сразу от «сотрудника правоохранительных органов». Они сообщают, что родственник попал в неприятную ситуацию: устроил ДТП, задержан с наркотиками и т.д. По итогам разговора жертву просят перечислить или передать курьеру крупную сумму денег для «решения вопроса».

**«Звонок из банка»**. Это не только самая популярная, но и динамично меняющаяся разновидность вишинга, что позволяет ей до сих пор оставаться в тренде. Звонки от имени банка могут носить нецелевой характер (злоумышленники просто перебирают номера наудачу), а могут быть «тёплыми» (мошенники располагают некоторыми сведениями о жертве). Сценарии атаки могут сильно разниться в зависимости от того, какие данные имеются в распоряжении преступников. Они, как правило, представляются работниками банков или сотрудниками правоохранительных органов; нередко используются автоматические информаторы, сообщающие о проблемах со счётом или транзакцией. В процессе общения жертву могут переключать с одного «специалиста» на другого.

**«Заберите выигрыш»**. Данный сценарий подразумевает не запугивание жертвы, а напротив — рассказ о некой радостной новости: выигрыш, выплата или бонус, эксклюзивное предложение или хорошая скидка. Чтобы не упустить такую выгоду, от жертвы требуется прямо сейчас совершить нужные мошенникам действия, например, продиктовать номер карты и код из СМС.

**«Оплатите услугу или товар»**. Жертве сообщают, что ей нужно срочно оплатить поверку счётчиков или приобрести дорогостоящий чудодейственный прибор. Введённые в заблуждение люди расстаются с деньгами или персональными данными, а потом на них оформляют кредиты или вынуждают заключать договоры на кабальных условиях.

Но даже если мошенники придумают совсем новую схему, вы сможете сохранить свои деньги, если последуете нашим советам.

**—Совет 1—**

***Не доверяйте никому***

По крайней мере, если речь идёт о телефонных звонках. Телефон по определению не должен быть для вас надёжным каналом связи. Вы никогда не можете быть уверены, что разговариваете с тем человеком, которым представился ваш собеседник. И уж тем более нельзя верить номеру, который отразился на экране смартфона. Даже если антиспам-приложение подсказывает, что это «менеджер банка», а звонящий говорит на фоне офисного шума. Не сообщайте по телефону никакую конфиденциальную информацию и не совершайте никаких действий, пока не убедитесь, что разговариваете с тем, с кем нужно.

Помните: вы всегда можете остановить разговор и самостоятельно перезвонить в ту организацию, с представителем которой, как вы думаете, вы общались. Там вы можете попросить соединить вас с нужным человеком. Настоящий сотрудник банка с пониманием отнесётся к такой предосторожности.

Важно: перезванивать следует не на тот номер, с которого вам поступил звонок, а на телефон, указанный в вашей записной книжке, сайте организации или в документах.

**—Совет 2—**

***Не торопитесь***

Несмотря на всю техническую начинку, в основе вишинга лежат всё те же банальные принципы обмана, которыми наверняка пользовались ещё в Древнем Египте. Во время разговора злоумышленники попытаются ввести вас в заблуждение, чтобы нащупать ваши слабые стороны и вынудить совершить нужные им действия. Большая часть социотехнических схем работает так, чтобы не дать жертве опомниться. На вас постоянно будут давить, вас станут торопить, не давая трезво оценить происходящее.

Помните: в денежных вопросах спешка недопустима. Даже если «служба безопасности банка» утверждает, что нужно вот прямо сейчас им что-то передать. Не поддавайтесь панике и постарайтесь трезво оценить ситуацию. Вы находитесь не за штурвалом падающего самолёта. А значит, у вас есть время отдышаться и спокойно обдумать слова собеседника. Возьмите ситуацию в свои руки. Прервите разговор, спокойно всё обдумайте, после чего принимайте взвешенное решение.

Важно: не верьте утверждениям, что вам нельзя вешать трубку или сообщать кому-то о факте звонка. Это стандартные уловки, цель которых — не дать вам прийти в себя.

**—Совет 3—**

***Повышайте уровень своей финансовой и цифровой грамотности***

Пожалуй, это самый главный совет — ведь мошенники всегда используют пробелы в знаниях жертвы. Если у вас есть счёт в банке — внимательно перечитайте договор и правила безопасности при пользовании услугами. Изучите, как осуществляется управление счётом, что требуется для входа в личный кабинет и проведения транзакций. Злоумышленники часто оперируют малопонятными, а то и вовсе вымышленными терминами, пользуясь тем, что люди слабо представляют работу банковской сферы или работу правоохранительных органов.

Помните: ни в коем случае нельзя совершать никаких действий, если вы не знаете точно, для чего это нужно. Это касается и передачи кодов из СМС, и переводов денег на некие «безопасные» счета, и многих других операций. Возьмите паузу и разберитесь в том, что вы планируете сделать.

*Важно: обязательно перепроверяйте информацию и не стесняйтесь обращаться за консультацией к специалистам. Всё знать невозможно, и в этом нет ничего зазорного. Только помните, что консультацию должны оказывать не те «специалисты», которые вам позвонили.*

Александр Вураско, начальник отдела анализа цифровых угроз

Infosecurity a Softline Company