МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

Технологичное телефонное мошенничество

Как мошенники могут использовать современные технологии для обмана по телефону и что с этим делать?

Авторы: Серов Даниил и Чернышёв Григорий

Группа №114.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Не так давно американская Федеральная комиссия по связи (FCC) предупредила об очень необычном методе телефонного мошенничества. Злоумышленники звонят по телефону и задают невинный вопрос: «Слышите меня?». Ответ «да» – это все, что им нужно. Имея запись утвердительного ответа, они подписывают жертву на платные услуги, которые будут включены в счет за связь.

Тип мошенничества, при котором в счет абонента без его согласия вносятся дополнительные услуги (например, рассылка гороскопов или новостей), носит название крэмминг (от англ. «cram» — «впихивать»).
В этой новости настораживают несколько моментов. Как вообще возможен крэмминг? Почему правоохранители ничего не могут с этим сделать? Неужели действительно можно использовать запись голоса, чтобы подписать абонента на дополнительные услуги?
Технически крэмминг возможен, поскольку телефонные компании позволяют включать в основной счет абонента услуги третьих лиц.
Сама эта уловка не нова — еще в 2008 году о ней сообщал сайт 800Notes.com, ведущий реестр сомнительных телефонных номеров. В то время прием использовался в первую очередь для навязывания услуг организациям. По свидетельству попавшихся на удочку, злоумышленники монтируют аудиозапись, на которой жертва собственным голосом соглашается на получение платных услуг.
Власти пытаются бороться с крэммингом: так, в 2015 году FCC обязала телекоммуникационных гигантов Verizon и Sprint выплатить 158 миллионов долларов для урегулирования претензий потребителей, которым таким образом впарили ненужные услуги. Но подобные крэммингу способы мошенничества с развитием современных технологий могут стать очень масштабными.

ГОЛОС В БАНКЕ

В ближайшем будущем что-то вроде крэмминга угрожает банковской сфере, в которой все большее распространение получает голосовая идентификация. К примеру, в 2016 году один из крупнейших банков Великобритании, Barclays, ввел возможность голосовой аутентификации для всех своих частных клиентов.

К тому же телефонным мошенникам придется как-то заставить клиента банка произнести сокровенную фразу целиком. Вряд ли у них это получится, однако они могут попытаться разговорить его и выудить слова по отдельности, если потребуется, за несколько звонков.

Если кто-то пытается придумать способ обмануть людей, наверняка найдется кто-то другой, кто будет придумывать, как этого можно избежать.

Например, технология компании Pindrop для оценки «подлинности» удаленного клиента учитывает множество факторов. Среди прочего — географические координаты звонящего. Если звонок от клиента вдруг поступил с другого конца Земли относительно его обычного местоположения, система насторожится. Собственно, такие технологии нередко включены в уже существующие антифрод-системы, используемые во многих банках.

Другой косвенный признак — выбранный канал связи. По статистике компании, мошенники используют VoIP-телефонию в 53% случаев, в то время как настоящие клиенты — лишь в 7 % всех звонков. Поэтому поступивший по интернет-телефонии звонок система Pindrop сразу берет на карандаш.

В свою очередь, злоумышленники применяют контрмеры, например имитацию плохой связи, которая теоретически может усложнить системе идентификацию звонящего. Скоро же арсенал телефонных преступников, судя по всему, пополнится новыми мощными орудиями.

ЗАЩИТА ОТ МОШЕННИКОВ

И что со всем этим делать?

Специфика атаки, в которой у жертвы выманивают слово «да», предполагает радикальный метод решения. FCC рекомендует вовсе не отвечать на звонки с неизвестных номеров. Если с вами действительно хотят связаться, оставят сообщение в голосовой почте.

1 Не сообщайте никаких личных данных о себе — они могут быть использованы злоумышленниками против вас как сразу, так и в будущем.
2 Проверяйте выставляемые счета на предмет неожиданных позиций.
3 Отдельный способ защиты от телефонного спама — внести свои контактные данные в государственный реестр номеров, которые телемаркетологи обязаны исключать из своих списков. Если он, конечно, есть в вашей стране. Такой реестр действует в США, в Европе единой базы нет, но есть отдельные национальные, а в России законодательная инициатива о создании реестра была выдвинута в 2013 году, но так и не была реализована.
4 Бороться с телефонными спамерами и мошенниками может помочь приложение Kaspersky Who Calls, которое уже можно найти в Google Play и Apple AppStore. Оно содержит постоянно пополняемую базу номеров телефонов, в том числе и принадлежащих спамерам. Who Calls поможет распознать, кто вам звонит, и на основании этого вы сможете понять – стоит ли брать трубку.

СПАСИБО ЗА ВНИМАНИЕ!

Берегите себя и свои деньги!