ЗАЩИТА КЛИЕНТОВ БАНКОВ ОТ МОШЕННИЧЕСТВА ПУТЁМ ПОДМЕНЫ НОМЕРА

Найдёнова Д. Р.
Научный руководитель – д.т.н., проф. Антипов И.Е.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, кафедра КРиСТЗИ
(057) 702 14 30)

In the abstract, the situation with the growth of fraud in the banking sector due to a telephone number change is described. The technical side and the proper use of the Caller ID Customization function are reviewed. The negative implications of the Caller ID Customization function using by scammers are shown. Recommendations for banks and bank costumers for the fraud changing numbers protection are proposed.

Методы социальной инженерии становятся основными при хищения денежных средств мошенниками у клиентов банков. Как отмечает «Лаборатория Касперского», за 2019 год примерно треть клиентов признались, что они или их близкие теряли деньги в результате телефонного мошенничества, причем почти каждый десятый потерял довольно крупную сумму. В большинстве подобных случаев звонки идут якобы от имени «службы безопасности банка». Нередко – с подменой номера банковской организации.

«Подмена номера» или Caller ID Customization это функция, которая может быть реализована на коммутационном оборудовании со стороны вызывающего абонента. Технически это происходит так.

В процессе установления соединения оператор вызывающего абонента по каналам ОКС-7 передаёт оператору вызываемого абонента т. н. IAM (Initial Address Message – первичное адресное сообщение), в котором содержится номер вызываемого абонента и ANI (Automated Number Identification – номер, который используется для идентификации вызывающего абонента и выставления счёта). Оборудование вызываемого оператора формирует и отправляет вызывающему сообщение INR (Information Request), в ответ на которое оператор вызывающего абонента формирует второе сообщение – INF. Именно в нём содержится Caller ID – номер, который отображается на экране телефона при входящем вызове.

Таким образом, в ОКС-7 могут существовать два разных номера – по одному выставляется счёт, второй отображается при входящем вызове.

Изначально использование этой функции предполагалось исключительно «в мирных целях». Во-первых, она позволяет добавлять/исключать префикс при наборе и отображении номера. Например, находясь в Харькове, с мобильного телефона можно набрать +380-57-XX…XX, или 057-XX…XX, или просто семизначный городской номер – вызов пойдёт одному и тому же абоненту. Во-вторых, функция

Caller ID Customization даёт возможность отображать на экране вызываемого абонента не номер, а имя звонящего, которым он сам себя назвал. Например, sms от оператора подписывается Kyivstar, без указания номера.

Однако, благодаря широкому распространению корпоративного телекоммуникационного оборудования для IP-телефонии, подключаемого к сетям операторов по стандартным протоколам, предусматривающим описанный выше обмен данными, опции Caller ID Customization стали доступны мошенникам. Они могут рассылать сообщения и совершать звонки, при этом у абонентов на экране будет отображаться «Мой_Банк». Нельзя сказать, что они могут это делать долго и безнаказанно – оператор без труда может установить истинный номер звонящего и заблокировать его. Но на это потребуются определённое время и усилия. А мошенники стараются действовать быстро, к тому же, они могут находиться в другой стране. К сожалению, «заблокировать» или запретить использовать данную функцию невозможно. Поэтому банкам и клиентам необходимо взаимодействовать с учётом того, что подмена номера возможна.

Нами предлагаются следующие рекомендации для банков и клиентов.

Клиентам рекомендуется:

1. Запомнить номер центра коротких сообщений для заведомо подлинных sms от банка. Проверять этот номер у подозрительных sms.

2. Присвоить подлинному номеру банка такое имя, которое заведомо отличалось бы от того, которое придумают мошенники.

3. Обращать внимание на искажения речи, характерные для IP-телефонии, во время подозрительных звонков «от банка».

4. По возможности игнорировать звонки в ночное время.

5. Знать психологические приёмы, к которым прибегают мошенники: изобилие технических/банковских терминов в речи, требование поспешности действий, угроза потери средств, обещание призов, бонусов и т. д.

6. Минимизировать информацию о себе в Интернете.

Рекомендации для банков.

1. Не допускать звонки, рассылки и другие обращения к клиентам, которые носят рекламный (пусть даже «информационный») характер.

2. Оговаривать порядок общения с сотрудником банка, предусматривающий «обратный звонок» на указанный в договоре номер.

3. Настаивать на доработке протоколов ОКС-7, дополнив их функцией, которая позволила бы информировать вызываемого абонента о том, что номера ANI и Caller ID у вызывающего абонента различаются.

В докладе вышеперечисленные и ряд других рекомендаций будут рассмотрены и обоснованы более подробно. Следование им позволит снизить риск мошенничества, вызванного функцией подмены номера.