ОПАСНЫЙ ЗВОНОК

КАК КРАДУТ, ПРИКИДЫВАЯСЬ БАНКОМ

С начала года все большую популярность получают атаки на граждан, при которых злоумышленники звонят с реальных телефонов банка, подменяя номер. Введенная в заблуждение жертва сама рассказывает мошенникам сведения, позволяющие похитить деньги с ее карт и счетов. Злоумышленники применяют столь искусные техники социальной инженерии, что жертвами становятся даже дипломированные психологи и сотрудники банков.

ЕВГЕНИЙ ПАВЛЕНКО

«Для подмены входящего номера используется IP-телефония, когда при помощи технических манипуляций в рамках настройки АТС мошенник звонит с любого номера, который у клиента на телефоне будет определяться как номер банка N»,— рассказывает вице-президент, директор по безопасности Почта-банка Станислав Павлунин. При этом технических решений, которые позволяют совершить подобный звонок, по его словам, множество — от весьма бюджетных приложений на мобильный телефон до весьма дорогостоящих решений. Конечная цель атаки всегда одна — получить доступ к вашим деньгам.

«Ковровые бомбардировки»

Для того чтобы при звонке от имени банка потенциальная жертва поверила в звонок от кредитной организации, мошенникам нужна информация о потенциальной жертве.

При массовой атаке, то есть когда злоумышленники действуют по принципу максимального охвата аудитории, злоумышленники берут сведения из различных баз данных, которые утекли в сеть. Из свежих актуальных утечек, отмечают в компании DeviceLock, база плательщиков штрафов ГИБДД и иных через предназначенные для выявления санкций интернет-ресурсы. В базе сотни тысяч персональных данных, включая ФИО автовладельца, номер автомобиля, номер исполнительного производства, первые и последние цифры банковских карт. Лука Сафонов из «Инфосистемы Джет» вспомнил выявленную в сети базу данных по покупке новых автомобилей по Москве и Московской области, где были данные паспортов, телефоны, марки и модели автомобилей 12 тыс. человек.

«Иногда источником данных для мошенников могут быть сведения, которые люди по неосторожности оставили в интернете, указывая в открытых источниках место работы и номера телефонов, предупреждает Станислав Павлунин.— Например, человек оставляет отзыв на сайте фитнес-клуба, и если у него в профайле есть мобильный телефон, то ему могут позвонить под видом менеджера фитнес-клуба и под предлогом оформления скидок, бонусов и подарков выведать паспортные данные, домашний адрес и другую информацию».

Небольшой объем информации из открытых баз дополняется сведениями, полученными от автоинформатора банка. Вычислить банк, в котором у человека открыт счет, достаточно просто. «В 90% случаев мошеннических звонков, о которых мне известно, злоумышленники представлялись сотрудниками службы безопасности Сбербанка,— рассказывает собеседник „Денег“ в крупном банке.— Вероятность, что у человека счет в Сбербанке, очень велика, если ж не угадывали, то сообщали о поступлении средств на человека в Сбербанк и спрашивали, в какой кредитной организации у него счет, чтоб передать информацию». Весьма странная уловка, но она обычно срабатывает, люди не видят ничего зазорного в том, чтобы сообщить службе безопасности другого банка, где у него открыт счет, отметил он.

Охота на крупного зверя

Чудеса изобретательности (и информированности) злоумышленники демонстрируют тогда, когда идет охота на крупного зверя, то есть на премиальных клиентов. Информацию по ним они собирают разными способами. «Например, по той же базе покупателей машин можно выявить свежеиспеченных владельцев Porsche и Jaguar, которые вряд ли будут из числа бедных,— рассуждает Лука Сафонов.— Кроме того, любители освещать свою жизнь в соцсетях дают злоумышленникам немало информации для планирования атак». Эксперт приводит пример любителей фотографироваться на фоне своих авто, в то время как по номеру автомобиля можно получить достаточно много информации. «Или же рассказываете вы в соцсетях, что только-только вернулись из отпуска в Таиланде,— рассуждает он.— И если вам позвонят якобы из банка и сообщат о подозрительном расчете вашей картой при оплате счета на $400 в этой стране, то велик шанс — вы поверите». По премиальным клиентам автоинформатор выдает данные далеко не во всех банках, поэтому при целевых атаках на премиальных клиентов могут быть использованы иные каналы получения той же информации об остатках. «Сейчас в Telegram существуют десятки каналов, где продаются данные по клиентам разных банков, причем продают сами же недобросовестные сотрудники кредитных организаций,— сетует собеседник „Денег“ в правоохранительных органах.— И если речь идет именно о целевой атаке, то злоумышленники могут приобрести информацию у таких посредников».

ТЕКСТ **Вероника Горячева**
ФОТО **Евгений Павленко, Александр Коряков**