Автор: Артур Скальский © Коммерсантъ ИНТЕРНЕТ И ИТ, МИР 4095 27.10.2011, 11:29 342

В контакте с мошенниками

Вам еще не поступали сообщения от друзей в "Одноклассниках" или "Вконтакте" с просьбой отправить SMS, одолжить денег или поделиться номером мобильного общего знакомого?

Осторожно: это могут быть и не друзья — взлом и дальнейшее использование персональных страниц в социальных сетях с недавних пор стало новой золотой жилой для аферистов.

Приятный мужской голос

"Здравствуйте, это инженерная служба вашего сотового оператора. Мы перенастраиваем сеть. Чтобы оставаться на связи, вам необходимо набрать... Записывайте..." Подобные звонки за последние несколько месяцев поступили тысячам пользователям сотовых телефонов. Приятный мужской голос терпеливо диктовал набор букв и цифр. В итоге, после набора указанной комбинации со счета списывались 300 руб. (или 600 — у тех, кому "сервисный инженер" дал указание "набрать авторизацию для верности дважды"). На самом деле, вводимая комбинация являлась не чем иным, как платной отправкой SMS на короткий номер. То есть попросту SMS-платежом в пользу мошенника.

"Эта схема мошенничества, которую мы называем лжезвонком от технической службы оператора, сегодня одна из самых распространенных,— комментирует начальник отдела корпоративной социальной ответственности дирекции по связям с общественностью ОАО "Вымпелком" Анна Самохвалова.— Необходимо помнить, что у оператора связи миллионы абонентов, и настройки на сети совершаются таким образом, чтобы быть незаметными пользователям".

Это лишь один из мошеннических приемов, цель которых — заставить пользователя отправить SMS-платеж на короткий номер. А еще могут позвонить с "радиостанции" — сообщить, что на "ваш номер выпал приз", но для его получения необходимо зарегистрироваться, отправив SMS — якобы бесплатно.

Заметим, что разводку простофиль личным звонком мошенники используют сравнительно редко, куда большую долю SMS-платежей на счета аферистов дает SMS-спам, когда завлекающие сообщения рассылаются на миллионы телефонов автоматически. Содержание может быть самым разным: от "отправь SMS — получи бонус" до "прими участие в лотерее — отправь SMS стоимостью 10 руб. и выиграй Mercedes". Естественно, стоимость сообщения, отправленного на указанные мошенниками короткие номера, обычно оказывается не меньше 200 руб.

"Для рассылки SMS-спама аферисты обычно используют подключенные к компьютеру специальные GPRS-модемы на несколько SIM-карт, которые по базе данных будут рассылать до 100 сообщений в секунду. За час разошлют сотням тысяч абонентов,— рассказывает Вячеслав Варламов, гендиректор контент-провайдера "Си Эм Си Биллинг".— Самое опасное, что используемые программно-аппаратные средства позволяют подменять номер отправителя в сообщении, что запрещено операторами. То есть, можно отправить SMS от имени самого сотового оператора или кого угодно".

Заметим, в интернете есть куча сервисов, предоставляющих всем желающим за символическую плату возможность отправки SMS с подставным номером или именем отправителя.

Однако даже если пользователь телефона принципиально не участвует в лотереях и рекламных акциях, не голосует отправкой SMS, это вовсе не означает, что он в безопасности. Как говорит Вячеслав Варламов, скачивая для своего телефона какой-то софт из интернета, например игру, можно вместе с ней получить и некое java-приложение, которое будет периодически рассылать SMS-сообщения на номер мошенников без ведома владельца телефона. Более того, хитрая программка после каждой отправки заметает следы — стирает соответствующую запись в папке "Отправленные".

Именно такие жертвы дают аферистам львиную долю дохода. Забавно, что даже после того, как мошенника прижали, перевод ему денег от контент-провайдера прекратили, на короткие номера с зараженных телефонов продолжают поступать SMS и деньги за них у абонента, соответственно, списывает оператор.

Номер удался

Гигантскую часть разводок на SMS-платеж составляют реклама и предложение услуг в интернете. Отправкой SMS на короткий номер могут предлагать оплатить как доступ к порноархиву или скачивание пиратского софта, так и вполне благовидные услуги, вроде получения результата теста IQ или персонального гороскопа. Обычно стоимость SMS оказывается 300 руб., вместо декларируемых 30-50 руб. При этом за свой платеж незадачливый пользователь не получает ничего. Более того, иногда ему приходит уведомление: мол, нужно отправить еще одно "бесплатное SMS с дополнительным подтверждением" и т. д. до бесконечности.

Весьма интересный прием начал применяться примерно год назад: подцепленный в сети вирус при открытии любой интернет-страницы заполнял около четверти экрана окном с порнухой, которое не убиралось никакими действиями. Отдельной строкой порноинформер ехидно благодарил за доверие и предлагал отправить SMS с кодом на номер 3649 для своего удаления и отказа от порновидеоподписки. Те, кто решился отправить SMS, вместо кода удаления получили ответное сообщение — предложение отправить еще одно SMS для подтверждения удаления.

"Погуглив, я узнал, что номер 3649 используется везде, где только можно,— рассказывает предприниматель Сергей, бухгалтер которого год назад пострадала от такого вируса.— От спам-рассылок "Номер 3649, если на него отправить, то получишь 35 бесплатных СМС", "доступ к нереальной эротике", "получи ключ на Касперского" до предложения "скачать шпаргалки по физике". Для получения пароля нужно отправить SMS-сообщение ТТНОМ".

По сведениям Сергея, какое-то время назад номер 3649 (в пользовании у "Первого альтернативного контент-провайдера") временно закрыли. Потом, видимо, разобравшись с аферистами, его снова открыли. Во время подготовки этого материала мы провели эксперимент. Сергей снова отправил код ТТНОМ на 3649 (реклама в сети до сих пор крутится), 300 руб. исправно списались, но вместо пароля доступа к шпаргалкам по физике пришел ответ: "Уточните текст смс. Вопросы: a1help.ru".

Проведя нехитрый поиск в сети, мы выяснили, что практически на все дорогие (со стоимостью отправки SMS 200-300 руб.) короткие номера есть жалобы пользователей. Так почему же сотовые операторы их не закрывают? Об этом немного ниже.

Мы знакомы?

Наибольшую опасность для пользователя представляют персональные письма или персонифицированный спам. Например, нашей коллеге в сети "Одноклассники" пришло такое сообщение с аккаунта одного из друзей: "Привет!!! Я почти выигрываю в конкурсе лучшее фото к 9 мая , меньше процента не хватает ... Главный приз — смартфон почти мой ... Лена, можешь мне помочь? Нужно отправить смс, текст "num777 170". Номер конкурса "6008", без кавычек . Если не тяжело, проголосуй за меня, в долгу не останусь! Конечно, если полтора рубля не жалко;-) Заранее спасибо!"

Оказалось, что такие сообщения получили все, кто был в списках друзей страницы отправителя. При этом сам владелец аккаунта даже не знал, что от его имени что-то рассылалось. Подобные аферы проворачивались и в сети "Вконтакте". Судя по всему, мошенникам удается каким-то образом получить доступ к аккаунтам пользователей. Примечательно, что некоторое время назад в сеть была выложена база, содержащая данные, в том числе пароли доступа, примерно по 40 тыс. аккаунтов "Вконтакте".

Комментировать, как такое возможно, администрация ресурсов "Одноклассники" и "Вконтакте" отказалась, и мы обратились к сторонним экспертам. "По нашим оценкам, эти данные были не украдены с серверов самой компании, а набраны путем фишинга,— комментирует старший антивирусный эксперт "Лаборатории Касперского" Виталий Камлюк.— Анализ той 40-тысячной базы показал, что собирались пароли пользователей всего пару месяцев".

Фишинг — от англ. phishing, производное от password — пароль и fishing — рыбная ловля. Разновидность интернет-мошенничества, цель которого — завладеть конфиденциальными данными пользователя (паролем, номером кредитки, PIN-кодом и пр.) с помощью того или иного хитроумного способа, с применением социальной инженерии.

А у Вячеслава Варламова предположение иное: "В интернете можно найти программу-робот, которая будет ползать по "Вконтакте" и одну за другой взламывать странички пользователей. Этот же робот может сразу производить рассылку от имени владельца аккаунта. При этом раньше ему удавалось еще и сразу же стереть

следы рассылки, подчистив папку "Отправленные"; сейчас "Вконтакте" это уже не позволяет. "Одноклассники" защищены лучше — их таким роботом не проймешь".

Тем не менее обычный фишинг тоже дает бешеный эффект. Допустим, пользователю приходит на e-mail письмо: "Привет, посмотри какие отличные фотографии я выложила на своей странице в Вконтакте. Маша". "Кто такая Маша? Зайду узнаю, может, и правда знакомая",— думает получатель или даже не думает, а просто кликает автоматически прилагаемую ссылку и попадает на фишинговый сайт, дизайн которого скопирован с оригинала. Но чтобы добраться до страницы "Маши" надо авторизоваться, то есть ввести свой логин и пароль.

Как рассказал Виталий Камлюк, попасть на фишинговый сайт можно и без всяких вирусов-троянов, подставляющих фальшивую страничку, или спамерских разводов. Любой человек, забивая адрес сайта в строке браузера, может допустить опечатку. Мошенники, находя наиболее вероятные варианты опечаток, регистрируют соответствующие сайты. В итоге, набрав вместо www.vkontakte.ru (адрес настоящего "Вконтакте.ru") www.vkontaktle.ru, попадаешь на практически идентичную внешне страницу. Незначительные отличия от оригинала в дизайне именно этого фишингового сайта (а подобных может быть очень много) объясняется исключительно ленью самих аферистов — они не обновили вслед за настоящим "Вконтакте" когда-то скопированную главную страницу.

После получения логина и пароля фишинговый сайт чаще всего выдает сообщение об ошибке или переадресует вас на настоящий ресурс, так что вы можете вообще не заметить, что заходили куда-то еще. Чтобы обезопасить пользователей, владельцы популярных ресурсов стараются зарегистрировать на себя домены, на которые заходят в связи с типичными опечатками. Например, www.odnoklasniki.ru (с одной S) — ресурс не фишинговый, принадлежит "Одноклассникам" и переадресует вас в настоящую соцсеть.

Конечно, элементарную автоматическую защиту пользователю предоставляют и сами сервисы. Например, почтовые. "Заметное количество мошеннических посланий нам удается блокировать как спам,— говорит Анна Артамонова, вице-президент Mail.Ru.— Но тут важно понимать, что такого рода письма крайне редко бывают массовыми рассылками — чаще всего они отправляются вручную, с личным обращением и т. п., так что их практически невозможно отличить от легитимной корреспонденции". В большей степени обезопасить от фишинга может специальная антифишинговая защита. По словам Виталия Камлюка, последние версии персональных продуктов "Лаборатории Касперского" содержат постоянно обновляемую базу данных фишинговых сайтов, при посещении которых выдается автоматическое предупреждение.

Между тем есть способ, гарантирующий доступ к интересующему аккаунту. "Моя невеста подозревала, что я захожу на страницу своей "бывшей" в "Одноклассниках",— рассказывает Вячеслав, владелец сайта настольных игр через интернет zamutki.ru.— Чтобы проверить это, она воспользовалась дружескими отношениями с одним из модераторов "Одноклассников" — получила пароль от него".

На самом деле наибольшую опасность представляют злоумышленники, использующие данные из соцсетей не для разводок по мелочи, на 300 руб., а для более серьезных афер. Например, женщине на телефон присылают MMS с фотографией мужа в синяках, типа "твой сидит в ментовке, неси выкуп $2 тыс.". Как стало понятно, фото было взято с сайта "Одноклассники" и подправлено в Photoshop, телефон супруги каким-то образом раздобыли. Может быть, как в следующей истории?

Рассказывает Елена О.: "В "Одноклассниках" приходит сообщение от некого Коли Соловьева: "Лен! Привет! Это Коля Соловьев. Дай, пожалуйста, Пети Иванова моб. Телефон". Петю Иванова я знаю, он, кстати, у меня в друзьях в "Одноклассниках" прописан, а вот о Коле Соловьеве слышу впервые..." Такое письмо, видимо, рассчитано на невнимательного получателя, но и таких много. А вот если бы мошенники взломали аккаунт кого-то из знакомых Елены и написали подобное письмо от его имени, то нужный номер получили бы наверняка.

Позвони мне, позвони!

Помимо разводок на SMS-платеж, существует еще несколько видов афер, ориентированных на пользователей мобильников. Классика жанра — получение SMS вроде "Стою на дороге в ДТП, срочно положи рублей 200 на этот номер. Саша". Весьма распространен заход, когда пользователь получает SMS-уведомление о якобы поступившем на счет его номера платеже. Позже раздается звонок или приходит SMS с просьбой вернуть переводом некоему абоненту положенные не на тот номер деньги.

Если внимательно посмотреть на автоматическую подпись отправителя, то там, как правило, обычный (хотя

иногда "красивый") десятизначный номер. Впрочем, мошенники, располагающие системами автоматической рассылки и возможностями менять подпись, с такими аферами связываться не любят — обналичить набежавшие на SIM-карту крупные суммы не так просто. По словам представителя управления "К" МВД РФ, такими разводками часто занимаются арестанты в тюрьме — пополняют счета для собственных разговоров.

"Главное для абонента — не решать проблему самому, а отправлять звонящего к оператору связи, у которого есть процедуры корректировки ошибочно зачисленных платежей",— рекомендует Кирилл Пузырев, ведущий специалист аналитического отдела управления по безопасности ОАО "МегаФон". Реже, но случается, когда раздается звонок: "Срочно перезвони" — и сразу отбой. Или приходит SMS с подобным текстом. Зачем мошенникам нужно, чтоб им позвонили? Может, это "завлекалка" на платный телефонный сервис с повременной оплатой, вроде секса по телефону? Да, и такое бывает.

"Мы собираем претензии абонентов по таким фактам и формируем черный список платных номеров (как правило, зарубежных), которые используются в мошеннических целях,— говорит Кирилл Пузырев.— Дозвон на номера из черного списка после их проверки на предмет мошенничества блокируется для всех абонентов нашей сети с целью их защиты от финансовых потерь".

Бывают и совсем интересные ситуации. "У сотовых операторов есть тарифы, на которых за каждый входящий звонок начисляется бонус,— рассказывает Вячеслав Варламов.— У многих региональных операторов такие тарифы или акции плохо прорабатывали, и в итоге бонус за входящий звонок на мобильный оказывался больше, чем стоимость исходящего с городского номера. Многие садились и часами названивали сами себе, накапливая деньги на SIM-карте. Ко мне однажды приезжал человек, предлагавший купить с дисконтом SIM-карту, на которой он каким-то образом насобирал 600 тыс. руб."

Пишите письма

По словам Антона Веремьянина, главного редактора портала Procontent.ru, объем российского рынка SMS-платежей сами его участники оценивают в $160-200 млн в 2008 году, прогноз на 2009-й — $300 млн. "По нашим данным, доля мошеннических поступлений здесь — менее 1%,— говорит Веремьянин.— Что касается SMS-платежей за нелицензионный/запрещенный контент (например, порнография, пиратский софт), то может быть и 30%".

Как рассказал Вячеслав Варламов, в заметном количестве аферы с SMS-платежами стали проводить около четырех лет назад, когда контент-провайдеры предоставили физическим лицам возможность получать на короткие номера оплату за свои услуги. Сегодня эта схема выглядит так. Сотовый оператор сдает короткий номер в аренду контент-провайдеру (агрегатору), определяет фиксированную стоимость отправляемого на него SMS. А контент-провайдер сдает номер в субаренду партнерам — непосредственным поставщикам сервисов или контента. При этом партнеров на одном коротком номере могут сидеть сотни, и каждый из них предоставляет десятки сервисов. Соответственно, адрес получателя и конкретной услуги определяется так называемым префиксом — кодом, отправляемым на пресловутый короткий номер. Таким образом, понятно, почему операторы не могут просто так взять и закрыть номер с подмоченной репутацией.

При получении жалобы абонента (обращение в офис или в контактный центр) проводится разбирательство, и при подтверждении факта мошенничества и доказательства виновности провайдера абоненту возвращают потраченные средства. Кроме того, сотовый оператор крупно штрафует контент-провайдера (а то и разрывает отношения с ним), ну а тот, соответственно, закрывает префиксы, зарегистрированные на мошенников. Однако на этот случай аферисты регистрируют у провайдера сразу кучу префиксов: как только один закрывают как недобросовестный, они переключают поток SMS на другой.

"Как правило, мошенники, которые специализируются на таких аферах,— это школьники и студенты,— рассказывает Вячеслав Варламов.— При этом доходы у них далеко не детские: я знаю 13-летнего мальчика, который получал в месяц 200-300 тыс. руб.".

По заверениям пресс-служб "большой сотовой тройки", все они постоянно ведут разъяснительную работу и информируют абонентов о возможных аферах. Однако если об этом не знать и не искать эту информацию специально, то просто так на сайтах операторов на нее не наткнешься.

Обычно большинство обманутых абонентов ограничиваются лишь гневными звонками в call-центр оператора, где мальчики-девочки вежливо переводят стрелки на контент-провайдера: мол, вот вам его телефон, а мы тут ни при чем. Разговор же с контент-провайдером просто бессмыслен, жалоба от пострадавшего для него — всего лишь повод к размышлению и информация о партнере.

Совсем другое дело — направить своему оператору письменное заявление. "Никто не читает договор, который подписывает при покупке SIM-карты, а зря,— говорит Вячеслав Варламов.— Хотя оператор выступает как бы посредником между абонентом и производителем услуги на коротком номере, но номер-то предоставляет оператор, деньги взимает изначально он, и ответственность по закону перед абонентом несет он. Так что требовать свои деньги нужно именно с сотового оператора".

По словам Варламова, при наличии обоснованного письменного заявления оператор обязан вернуть деньги. В качестве доказательств можно приложить ссылку на рекламу в прессе, в сети, полученный текст SMS и т. д.

Судя по всему, это работает. Автор статьи знает одну жертву "лжезвонка от технической службы оператора", пенсионерку, которая не поленилась прийти в офис "Билайна" и написать заявление, 300 руб. ей вернули.

Автор: Артур Скальский © Коммерсантъ ИНТЕРНЕТ И ИТ, МИР 4095 27.10.2011, 11:29 342
URL: https://babr24.com/?ADE=99103 Bytes: 18323 / 18278 Версия для печати Скачать PDF

Автор текста: **Артур Скальский**.

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта