ICQ

Номера ICQ не растут в огороде

Недавно я зашел в гости к своему другу, который работает директором одного из местных банков. Зашел, судя по всему, не совсем вовремя, потому что даже любимые темы про мобильники-машины-откаты не вызывали у него желания вступить в разговор. И тут я случайно упомянул Интернет. Это вызвало неожиданную реакцию — под толстыми стеклами директорских очков что-то мигнуло, и в наступившей тишине я явственно услышал хруст хорошего «винта»...

«Слушай, Влад, — от меланхолии не осталось и следа, — мне наш сисадмин вчера подарил шестизначную аську!» Дальше последовало перечисление всех возможных вариантов запоминания шести цифр, длинный рассказ о том, как он на каком-то форуме ненароком обмолвился про новый номерок (все сказали «ах!»), а также сравнение номера с купленным в свое время «золотым» номером сотового телефона.

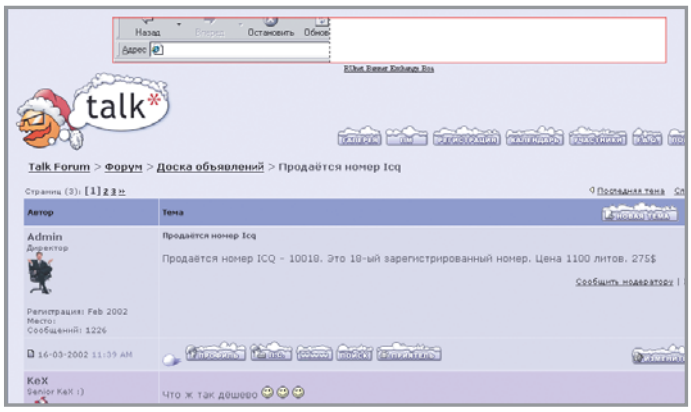
Я сидел, вытянув замерзшие ноги к камину, и вспоминал, как буквально за день до этого один человек написал мне в завершение переписки: «Я уважительно отношусь к людям с такой аськой». Господи, да почему? Неужели все то, что мы с ним обсуждали (а тема была вполне серьезная), менее важно, чем красиво расположенные циферки в моем номере ICQ?

И вообще — о чем речь? Давайте попробуем разобраться. Но во избежание путаницы и непонимания необходимо определиться с терминологией, а также рассказать несколько общеизвестных и не слишком фактов.

Итак, ICQ, она же «аська» — это самый популярный интернет-пейджер, созданный шесть лет назад в израильской фирме Mirabilis, ныне являющейся частью американского концерна America Online. Программа бесплатная, удобная и оттого завоевавшая популярность практически во всех странах мира, в отличие от большинства последовавших за ней аналогов и клонов.

При регистрации каждому новому пользователю ICQ присваивается номер в порядке возрастания — проще говоря, чем позже зарегистрируешься, тем больше цифр в твоем номере. Номера для обычных пользователей выдавались начиная со 100000 и в нынешний момент уже перешагнули за 200000000. »

▲ Счастливый обладатель UIN 10000 совершенно безлик. Кстати, и в онлайне с ним столкнуться почти невозможно. Так вот и рождаются мифы



▲ Если номер 10000 еще не выставлен на продажу, то уже восемнадцатый зарегистрированный готов сменить хозяина. Интересно, первого ли?

Самые короткие, пятизначные и четырехзначные номера были изначально зарезервированы для внутреннего пользования — то есть для сотрудников Mirabilis, а также их друзей, жен, любовниц и прочих приближенных лиц. Впрочем, позже они были аннулированы, так что на данный момент самым маленьким номером остается номер 10000, которым владеет неизвестная личность с подозрительным ником 80zGrl.

Попробуйте зарегистрироваться. Вы получите длинный девятизначный номер, на запоминание которого уйдет не один день... Не нравится? Хотите такой же маленький и симпатичный номерок, как у вашего собеседника в чате или соседа по дому? Что ж, есть два варианта действий — самому вскрыть красивый номер (что весьма маловероятно и может быть чревато последствиями, а уж о моральной стороне дела я и не говорю) либо просто его купить.

Почем номера для народа?

Расценки на номера ICQ в российской части Интернета определить относительно сложно, так как сформировавшегося рынка нет — сайты, специализирующиеся на продаже этого своеобразного товара, можно пересчитать по пальцам одной увечной руки. Да и стоимость того или иного номера зависит от субъективной оценки его «красоты».

Тем не менее приблизительные цены назвать можно. Так, обычный шестизначный номер без признаков закономерности в подборе цифр обойдется вам в сумму от одного доллара до трех. Что-то поприличнее, с двумя ноликами на конце или с тремя одинаковыми цифрами подряд, будет стоить вам примерно долларов десять. А в обмен на сумму от двадцати до пятидесяти условных единиц вы сможете получить нечто совсем уж радующее взор и не требующее запоминания.

Цены на «пятизначки» начинаются примерно с сотни. Но если надумаете покупать, учтите, что это товар скоропортящийся — не исключено, что буквально на следующий день после окончания «гарантийного срока» какой-нибудь ленивый админ фирмы Mirabilis наконец-то решит почистить базы от «fucking russian hackers»... И превратится ваша кровно заработанная сотня баксов в надпись «Password error».

Кроме того, учтите, что есть одна закавыка, связанная с системой возврата паролей, принятой в компании. С некоторых пор, а именно с первого сентября 1999 года, действует следующий принцип — «забытый» пароль высылается на любую почту, которую когда-либо вводили при использовании этого номера. Но! При этом все адреса, введенные позднее того, на который вы получили пароль первоначально, аннулируются и перестают иметь отношение к данному аккаунту. Система замысловатая, но весьма и весьма эффективная.

Именно поэтому при продаже номера вместе с ним обычно отдают так называемый primary mail — то есть почтовый адрес, который был введен в продаваемой аське на первое сентября 1999 года. Иначе нет гарантии того, что хитрый продавец, получив с вас деньги, не заберет номер обратно, получив пароль через принадлежащий ему primary mail.

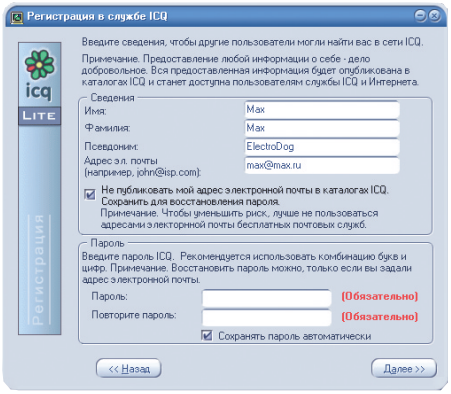
Технология добычи

Надеюсь, с покупкой все более-менее понятно. А вот откуда продавцы циферок берут эти маленькие номера, явно выданные много лет назад, да к тому же наверняка не им?

Вообще-то, ответить на этот вопрос можно одним словом: «Вскрывают». То есть отбирают у не слишком заботящихся о сетевой безопасности людей. Способов для этого существует довольно много — к основным относятся интеллектуальный или механический подбор пароля и захват primary mail. Гораздо реже используется проникновение в компьютер жертвы с помощью, скажем, трояна — все-таки наивных граждан, которым можно его подсунуть, становится все меньше и меньше.

Интеллектуальный подбор пароля — это попытка угадать его по тем или иным сведениям, известным о владельце номера. Это могут быть имя и фамилия, дата рождения, название компании — словом, подбор пароля по данным, указанным владельцем номера при регистрации.

▲ Некоторые пользователи отводят для продажи номеров отдельные странички. Номера здесь обновляются довольно регулярно



▲ Не забудьте при регистрации активировать пункт «Не публиковать мой адрес...»

» Но сейчас более популярен механизированный подбор паролей специальными программами, так называемыми брутфорсерами. Задается список желанных номеров или просто диапазон, в котором требуется производить проверку, подставляется пароль или опять же их список, нажимается кнопка Start. Затем оператор этого «цеха машинного доения» уходит пить пиво или спать до вечера, пока компьютер прогоняет пару десятков тысяч номеров на предмет соответствия паролю «12345».

Правда, в ответ на подобные действия Mirabilis ввела ограничения на попытки подключения с одного IP, запретив делать это больше трех раз в течение десяти минут. Но это привело только к созданию следующего поколения брутфорсеров, в которых кроме списка номеров и паролей можно задавать еще и список прокси-серверов. Насколько мне известно, ответа на эту новую угрозу пока не последовало.

Кроме того, «ловцы асек» подбирают пароли к почтовым адресам, захватывают освобожденные публичными почтовыми службами адреса, ищут ошибки и уязвимости в протоколах Mirabilis. С каждым годом таких уязвимостей становится все меньше и меньше, но они, разумеется, есть — так, использование последней из них принесло знающим людям множество пятизначных номеров, которые сейчас активно продаются в Интернете.

Еще один тонкий вопрос: а насколько все это законно? И насколько честно? От людей, вскрывающих аськи, я слышал следующее мнение: «Реально можно увести только те номера, которые уже давно брошены своими владельцами. Они им не нужны, так что никто не страдает. Да и если это не так, то кто ж мешал поставить нормальный пароль?»

Похоже, что и люди в Mirabilis думают примерно так же — по крайней мере, на письма с просьбой вернуть уведенный номер всегда приходит один и тот же ответ: «Воспользуйтесь нашей системой возврата паролей». Мол, мы предоставили вам методы защиты вашей виртуальной собственности, а уж если вы ими не воспользовались — что ж, господа, это уже ваши проблемы.

Как не стать дичью

Наши так наши. А чтобы их, этих проблем, вообще не было, я предлагаю вам несколько простых советов, написанных по моей просьбе одним профессиональным «ловцом асек».

Совет первый. Придумывайте сложные пароли. Ни в коем случае не используйте в них информацию, указанную в своих «User details». Также забудьте про имена или обычные слова, которые можно найти в словаре — не суть важно, в словаре Даля или Webster Dictionary. Зато старайтесь использовать буквы в разных регистрах и раскладках клавиатуры, а также цифры после или вместо букв. Так, пароль «MiSha#69» во много раз безопаснее, нежели просто «Misha». По крайней мере, такой пароль практически невозможно угадать или вскрыть простым перебором словарных слов.

Совет второй. Предохраняйтесь! Обязательно используйте firewall и регулярно проверяйте систему каким-нибудь антивирусом. А лучше двумя. Так, антивирус имени товарища Касперского лучше знаком с вирусами отечественного происхождения, а его западный друг имени господина Нортона — с иностранной заразой.

Совет третий. Не указывайте в открытом виде свои почтовые адреса при заполнении «User details». Там есть такой пункт «Don't publish my e-mail adress», так вот — обязательно активируйте его.

Во-первых, это избавит вас от лишнего спама, а во-вторых, не даст кому-то лишнего повода попытаться вскрыть вашу почту ради получения понравившегося ему номерка.

Совет четвертый. Не прописывайте в ICQ адреса сомнительных почтовых служб. Идеальный вариант — почта вашего провайдера, так как в этом случае вы всегда можете обратиться в службу технической поддержки. О публичных почтовых службах что-либо определенное сказать сложно, но из популярных отечественных самой надежной считается mail.ru.

Вот я и дошел до того места, где в плане статьи у меня написано «вывод». Но какие тут могут быть выводы? Нужен ли «золотой номер» сотового, три семерки на номерных знаках машины, красивый номер ICQ — решать вам. Точнее, вашему тщеславию.

■ ■ ■ **Влад Егоров**

Личный опыт

Как Chevrolet загубил ICQ

Эту историю рассказал мне знакомый, периодически подрабатывающий взломом ICQ и последующей продажей номеров: «Один красивый номер не давал мне покоя несколько дней. США, возраст 35-45, имя-фамилия-почта указаны (очень благоприятные признаки), да и фотография владельца, имеющаяся на прописанной в «User details» домашней страничке, явственно указывала на то, что пароль лежит где-то на поверхности. Проверял все классические сочетания типа qwerty, уменьшительные от имени владельца, от имени членов его семьи и его собаки, проверял все, что только приходило мне в голову. Бесполезно.

Времени было затрачено много, пора было сдаваться, но интуиция кричала: «Горячо!» Еще раз прохожусь по страничке и вдруг замечаю — уж очень красивая машина фигурирует на заднем плане многих фотографий. Красненькая, чистенькая, явно любимая... Mustang? Нет... Corvette? Не похож... Ага, старенький Chevrolet Camaro. Ввожу в окошечко для пароля «chevy». Password Error. А «camaro»? Чуть более длинная пауза, тихий хруст винта, и красный цветочек в трее стал ярко-зеленым.

Вот для этого я и вскрывал аськи — ради тех двух-трех секунд, которые наступали после этого мгновения...»