Защита от мобильных мошенников: не верь, не суетись, не жадничай

С расширением функциональности абонентских мобильных устройств и появлением все новых высокотехнологичных сервисов в сотовых сетях активизируются не только их пользователи, но и любители незаконной наживы. Возможность оплатить те или иные покупки и сервисы деньгами со счета сотового абонента и возможность управлять своими деньгами на банковском счете делают жизнь комфортнее, но они же осложняют жизнь риском, что в ваши "электронные кошельки" может запустить руку злоумышленник. Таким образом, информатизация жизни влечет за собой и информатизацию преступности: раньше воры крали деньги из сумок и карманов, теперь они научились изымать их из виртуального пространства.   
Нельзя сказать, что с киберпреступностью не борются: этим занимаются и правоохранительные органы, и банки, и операторы связи. По данным сотовых операторов, на противодействие мошенникам и ликвидацию последствий их вредоносной деятельности они совокупно потратили в прошедшем году сотни миллионов рублей. Проблема, однако, в том, что масштаб отдельно взятого мошенничества с использованием мобильной сети, как правило, не велик, а самих мошенников достаточно много, и переловить всю эту мелочь полностью раз и навсегда вряд ли удастся.   
Поэтому здесь как раз тот случай, когда болезнь легче предупредить, чем бороться с ней, когда она уже возникла. Причем немало в этой профилактике зависит от самих потенциальных "больных", то есть от пользователей услуг связи, любой из которых может стать объектом посягательств мошенников.   
Как это ни странно звучит, чтобы защитить себя от этих посягательств, вовсе не обязательно обладать какими-то особыми техническими навыками или глубокими знаниями об особенностях работы сотовой сети или сети доступа в интернет. Достаточно уметь правильно себя вести с точки зрения самозащиты от попыток выманить у вас деньги через сеть связи – такое правильное поведение практически полностью гарантирует вас от того, что вы попадетесь в расставленные мошенником сети. Причем успешная защита будет обеспечена от большинства видов и способов незаконного изъятия ваших денег, за исключением случаев применения преступниками наиболее сложных технических средств, когда необходимо применять технические же средства защиты.   
Подавляющее же большинство мошеннических приемов основано на использовании распространенных человеческих свойств: любопытства, невнимательности, тревоги за себя и близких, легкомыслия и доверчивости и, что уж греха таить, — желания за три копейки получить необъятное счастье.   
На основе обобщения рекомендаций специалистов по информационной безопасности можно выделить три основных принципа правильного поведения для эффективной мобильной самозащиты. Они таковы: не верь, не суетись, не жадничай.

Не верь

Первый из принципов, пожалуй, самый главный. Практически все способы мошенничества с использованием сети сотовой связи, кроме взлома электронных хранилищ абонентских денег с помощью технических средств, начинаются с того, чтобы заставить абонента поверить в какую-то ложную информацию. Например, ровно с этого начинается атака на ваш счет, когда вы получаете SMS-сообщение с просьбой якобы от близкого вам человека о перечислении денег на номер, ему не принадлежащий. Ровно так же построена схема с предложением отправить сообщение на указанный номер, чтобы получить шанс выиграть роскошный внедорожник. Даже получение вами MMS-сообщения с вирусом, замаскированным под открытку, тоже преследует цель заставить вас поверить в то, что кто-то пожелал вас порадовать.   
Поэтому умение не верить чему попало – важный компонент вашей защиты. При этом не обязательно становиться мизантропом, не верящим всему человечеству, достаточно уметь правильно опознать не заслуживающие доверия события. Например, понятно, что просьба вашего близкого перевести деньги на чужой номер необычна. Почему же вы должны безоговорочно верить в то, что сообщение с просьбой отправлено именно этим человеком? Почему вы должны верить в необычайный шанс выиграть что-то ценное, отправив SMS неизвестно куда? Почему вы должны верить, что кто-то, чьего телефонного номера вы не знаете, вдруг прислал вам открытку? Во всё это верить как раз не стоит, как и в другие подобные необычные варианты. Нетрудно понять, что если вы не поверите в то, во что верить не стоит, уже одно это не даст шанса мошеннику.

Не суетись

Но если даже вы поверили – еще не все потеряно, если вы не станете суетиться. На ту же SMS-просьбу о переводе денег не обязательно реагировать мгновенным совершением действий по переводу. Позвоните человеку, который, как вы полагаете, отправил просьбу. В 90% случаев он вам ответит, станет понятно, что ничего он не просил, – и на этом опасность для вашего кошелька будет ликвидирована. Не дозвонитесь с первого раза – позвоните еще, в итоге вы добьетесь того же – защитите себя от мошенника.   
То же касается предложения выиграть джип: даже если вы поверили, что вам предлагают именно это, а не пытаются заставить вас отправить SMS на платный номер, — не спешите, а подумайте сначала, насколько велик шанс такого выигрыша и стоит ли ради такого шанса рисковать? Подумав, вы, скорее всего, примете правильное решение. Посмотрев внимательно на номер, с которого отправлена открытка, и поняв, что вы его не знаете, вы вспомните, вероятно, чему вас учили в детстве: не брать ничего от незнакомых. И вы опять примете правильное решение – даже если это открытка, вы без нее переживете, зато не запустите в свой смартфон стаю жадных вирусов.   
Кстати, правило не пользоваться ничем, присланным на ваш телефон с незнакомых номеров: ни предложениями, ни фотографиями, ни видео- аудиофрагментами, — надежно защитит вас от большинства мошеннических попыток. В сочетании с правилом не суетиться — тем более. Не спешите, позвоните сначала тому оператору связи, который якобы прислал вам указание что-то куда-то отправить для каких-то настроек. Позвоните в банк, который прислал вам просьбы о предоставлении ваших данных или отсылки SMS для регистрации в бонусной программе. Позвоните тому, кто предлагает вам головокружительный выигрыш – хотя это вам сделать вряд ли удастся, потому что жулики, в отличие от легальных лотерей, своих телефонов не сообщают.

Не жадничай

И, наконец, не нужно жадничать и пытаться получить даром внедорожник, яхту, виллу или даже поздравительную открытку, явно не вам предназначенную. Все это вряд ли возможно, а неприятности получить вполне вероятно. Принцип "на жадину не нужен нож, ему покажешь медный грош — и делай с ним, что хош" действует безотказно.   
Если ваше поведение как пользователя сотовой сети будет включать в себя три простых элемента, о которых сказано выше, мошенников вам можно бояться не сильно. А чтобы вас и других добропорядочных людей боялись они, не поленитесь в случае подозрения на мошенническое посягательство позвонить своему сотовому оператору и рассказать, что, где, когда. Оператору тоже не очень приятно, что с использованием его сети пытаются совершать всякие безобразия, и нужные действия он предпримет.   
Есть еще и специфические способы мошенничества в интернете, требующие от пользователя специфических правил поведения для защиты своей безопасности, но это уже совсем другая история.   
Игорь Агапов.Источник: <http://ria.ru/science/20130322/928565411.html>