Будьте внимательны!
Все способы мошенничества в мобильных сетях!

К сожалению, мошенники всех пород и мастей облюбовали мобильные телефоны, так как с их помощью можно обмануть доверчивого человека в считанные минуты и ровно так же быстро получить его деньги. А потом ищи-свищи ветра в поле.

Знание — это ваша сила и оружие. Надеюсь, что прочитав все о мошеннических схемах, вы не попадетесь на крючок к нечистоплотным на руку людям.

Наибольшей популярностью пользуются SMS-мошенничества, их в нашем списке 11 разновидностей. Звонить мошенники также любят, но обманных схем тут намного меньше. В интернете таких схем также немного, всего шесть основных.

В 4 квартале 2010 года наибольшей популярностью у мошенников пользовались следующие схемы (по числу пострадавших либо по количеству отправленных сообщений):

1. MMS-подарок;
2. Ошибочный платеж;
3. Мама, у меня проблемы;
4. Вирус Trojan Winlock;
5. Социальные сети
6. SMS-мошенничества и сообщения

1. MMS-подарок

Текст сообщения:

Poluchen MMS podarok ot "Katya" dlya abonenta +7985XXXXXXX. Otkroite: my605.my1.ru/606.jar";.

При нажатии на ссылку на телефон скачивается и автоматически запускается java приложение, содержащее вредоносное ПО, которое отсылает SMS с переводом средств на номера мошенников. Затем злоумышленники в течение короткого времени выводят средства со своих мобильных счетов.

Что делать: Никогда не открывать ссылки или файлы, полученные с незнакомых номеров.

2. SMS с настройками

Текст сообщения:

"Ваш телефон имеет неверные настройки. Наберите на клавиатуре код XXXXXXXXXX, чтобы установить правильные настройки"

Текст сообщения может отличаться, но оператор никогда не просит вас вводить что-то на клавиатуре телефона либо загружать программы по ссылкам.

Что делать: Позвоните в абонентскую службу и сообщите номер мошенников. Если вы думаете, что вам нужны настройки, попросите их выслать абонентскую службу отдельным сообщением, эта услуга бесплатна.

3. Кредитная карта заблокирована

Вы получаете сообщение от «банка» в котором говорится:

"Ваша банковская карта заблокирована. По вопросу разблокировки обратитесь по тел. XXX-XXXX».

При звонке по этому номеру вам отвечает якобы поддержка «банка». У вас узнают данные вашей кредитной карты, после чего с ее помощью покупают в сети те или иные товары.

Что делать: Не перезванивать по телефонам в SMS-сообщениях с незнакомых номеров. Звонить в банк только по номеру, указанному на вашей кредитной карте. Позвонить в абонентскую службу и сообщить о мошенничестве.

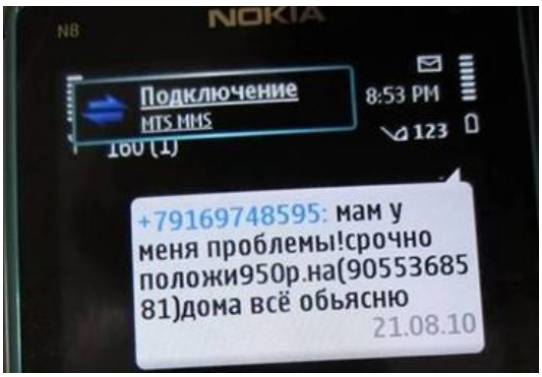
4. У меня кончились деньги

Вы получаете сообщение:

"У меня проблемы, позвони по такому-то номеру. Если номер не отвечает, положи на него деньги и перезвони".

Поверьте, что это не ваши знакомые, и класть деньги на этот номер телефона точно не стоит.

Что делать: Позвонить в абонентскую службу и сообщить о мошенничестве.



5. Отказ от получения рекламы

Вы получаете сообщение:

"Для запрета всех рекламных SMS-сообщений отправьте бесплатное SMS на номер 0000 с кодом 123456».

При отправке такого сообщения с вас спишут деньги.

Что делать: Позвонить в абонентскую службу и сообщить о мошенничестве.

6. Ошибочный платеж

Вы получаете сообщение:

"На ваш счет поступила сумма 400.00 рублей». Через некоторое время вам снова пишут с другого номера: *«Извините, по ошибке положил деньги на ваш счет. Моя сестра лежит в больнице. Верните, пожалуйста, деньги».*

Что делать: Проверить состояние счета и поступление денег. В 99 процентах случаев ваш счет не был пополнен, а SMS — всего лишь подделка. Позвонить в абонентскую службу и сообщить о мошенничестве.

7. Вам открытка

Вы получаете сообщение:

"Для вас получена открытка, открыть ее можно по адресу xxxxx, пароль 123456».

При открытии ссылки вы подпишетесь на платный сервис или загрузите вирус, который украдет деньги со счета.

Что делать: Не открывать ссылки в сообщениях с незнакомых номеров.

8. Пожертвования

Вы получаете сообщение:

"Фонд помощи жертвам террористического акта просит вас о содействии. Переведите деньги на xxxxx».

Что делать: Позвонить в абонентскую службу и узнать, проводится ли такой сбор средств. Скорее всего, мошенники используют печальный повод, чтобы получить ваши деньги.

9. Получи безлимитные звонки

Вы получаете сообщение:

"Отправь SMS на короткий номер, чтобы перейти на более выгодный тариф! Все локальные звонки — теперь безлимитные!".

При отправке сообщения с вас спишут деньги, а ваш тариф останется прежним.

Что делать: Позвонить в абонентскую службу и сообщить о мошенничестве.

10. Заявка с вашей карты принята

Вы получаете сообщение:

"(bank) Заявка с карты 5.500р. Принята. Инфо 8(xxx) xxx-xx-xx»".

Обеспокоенный абонент перезванивает на указанный якобы информационный номер, где трубку берет мужчина и представляется «службой финансового контроля». На вопрос, о чем идет речь, собеседник отвечает, что, скорее всего, это ошибка, с которой будет разбираться «служба безопасности банка». Но для того, чтобы избежать перевода денег, необходимо отправиться к банкомату, перезвонить снова и выполнить несколько действий с пластиковой картой под диктовку мнимого сотрудника банка. В данном случае, следуя указаниям мошенников, абонент совершает процедуру перевода денег на счет чужого мобильного телефона со своего личного банковского счета, привязанного к пластиковой карте. Причем при этом абонент сознательно выбирает опцию «оплатить услуги сотовой связи».

Что делать: Не выполнять никакие действия со своей картой под чужую диктовку. Не перезванивать по номерам из SMS-сообщений.

11. Сообщение по Bluetooth

Если у вас активирован Bluetooth, то некто может послать вам файл. Приняв такой файл с незнакомого телефона, вы можете сами установить вирус. Это опасно.

Что делать: Не выполнять никакие действия с полученными файлами.

Звонки от мошенников

1. Звонок от технической службы оператора

Раздается звонок, приятный голос сообщает, что оператор проводит технические работы, либо требуется предоставить дополнительную информацию, чтобы ваш телефон работал или вы получили бонус. В этой схеме всегда используется доверчивость абонента, который верит, что звонок поступил от оператора связи. Помните, что сотрудники вашего оператора никогда не запрашивают никакую информацию у своих абонентов (пароли, просьба ввести код на телефоне и так далее).

Что делать: Запомнить номер телефона и обратиться в абонентскую службу оператора, чтобы мошенников нашли. Не выполнять никакие действия, иначе вы рискуете потерять свои деньги. Например, в сети Билайн кодом можно активировать услугу «Мобильный платеж», и ваши средства будут переведены на счет мошенников. Вернуть их будет невозможно.

2. Мама, у меня проблемы

Звонок от вашего «ребенка», его плохо слышно, но вы понимаете, что у него проблемы. Есть вариант, когда звонит некто третий, так как ваш родственник попал в аварию. Надо срочно перевести деньги на телефон, чтобы была связь. В зависимости от истории и ситуации, мошенники также могут рассказать, что нужны деньги на взятку, и ее надо передать при встрече.

Что делать: Не волноваться. Позвонить человеку, о котором говорят. Если он недоступен, а мошенники вновь звонят, то попросите их описать машину, человека, любые приметы. Как правило, вы тут же поймете, что вас обманывают.

3. Приз от радиостанции

Схема может отличаться в деталях. Звонящий представляется популярным ведущим с радиостанции или представителем известной компании и говорит, что ваш номер выиграл некий приз. Для его получения вам надо позвонить на

радиостанцию, и вам дают номер. При звонке выясняется, что вы можете также получить телефон, но для этого надо «подтвердить» свой номер и продиктовать данные карты пополнения баланса либо какую-то иную информацию.

Что делать: Если вы не слушаете радио, то поверьте, даже это не дает оснований полагать, что вы счастливчик, который выиграл. Это одна из самых популярных в прошлом схем, никакой выигрыш вас не ждет, вас пытаются раскрутить на карту оплаты.

4. Акции операторов

Абонент получает сообщение об акции, проводимой его оператором. По условиям "акции", абонент до конца недели (месяца, года, жизни) получает возможность осуществлять бесплатные звонки по стране. Для этого ему необходимо всего лишь отослать в службу информационной поддержки (телефоны прилагаются) "оператора" коды нескольких карт оплаты. Естественно, выясняется, что оператор никаких акций не проводил, а карты оплаты пополнили счета мошенников.

Что делать: Не выполняйте действий под диктовку неизвестного Вам человека, как бы правдоподобно он ни описывал условия акции. Перезвоните в абонентскую службу Вашего оператора связи и проверьте информацию.

Компьютерные вирусы и интернет

1. Вирус Trojan Winlock

На вашем компьютере после посещения подозрительных сайтов или установки программ из непроверенных источников, появляется следующее сообщение (текст сообщения может отличаться):

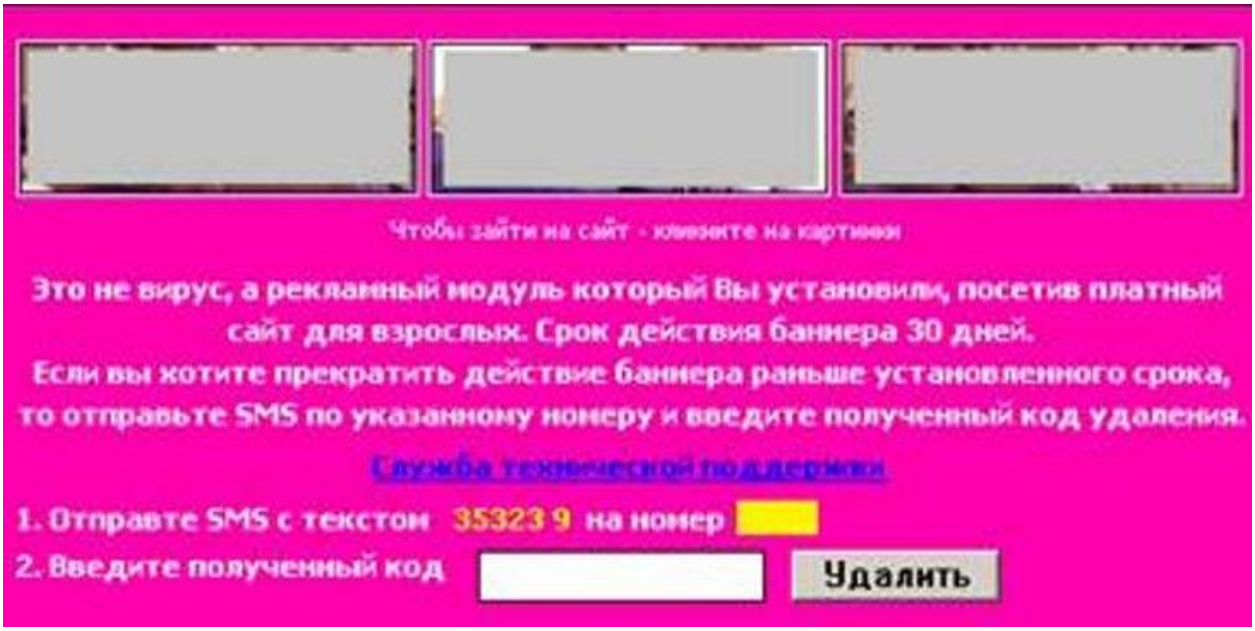
"Ваш Windows заблокирован. Microsoft установил некорректное пользование Интернетом с вашего компьютера. Вы просматривали сайты, содержащие ненадлежащую информацию/имеющие порнографический контент. Попытка перезагрузить ваш компьютер приведет к необратимым последствиям. Если не принять мер, в течение 12 часов после получения данного сообщения все данные, включая Windows и Bios, будут полностью удалены. Для устранения блокировки вы должны в течение 12 часов внести 300 рублей на телефон "Билайн" номер x-xxx-xxx-xx-xx (указан частный номер). Вы можете сделать это в ближайшем пункте приема платежей. После этого на ваш телефон придет сообщение либо на чеке об оплате будет указан код, по которому сможете разблокировать ваш Windows".

Что делать: Проверить компьютер антивирусной программой, после чего он будет разблокирован. Обратиться в абонентскую службу оператора и указать номер, на который вам предлагали перевести деньги. Быть осторожнее в сети.

2. Баннер, закрывающий экран

Вариант описанного выше поведения характерного для вируса.

Что делать: Проверить компьютер антивирусной программой, после чего он будет разблокирован. Обратиться в абонентскую службу оператора и указать номер, на который вам предлагали перевести деньги. Быть осторожнее в сети.

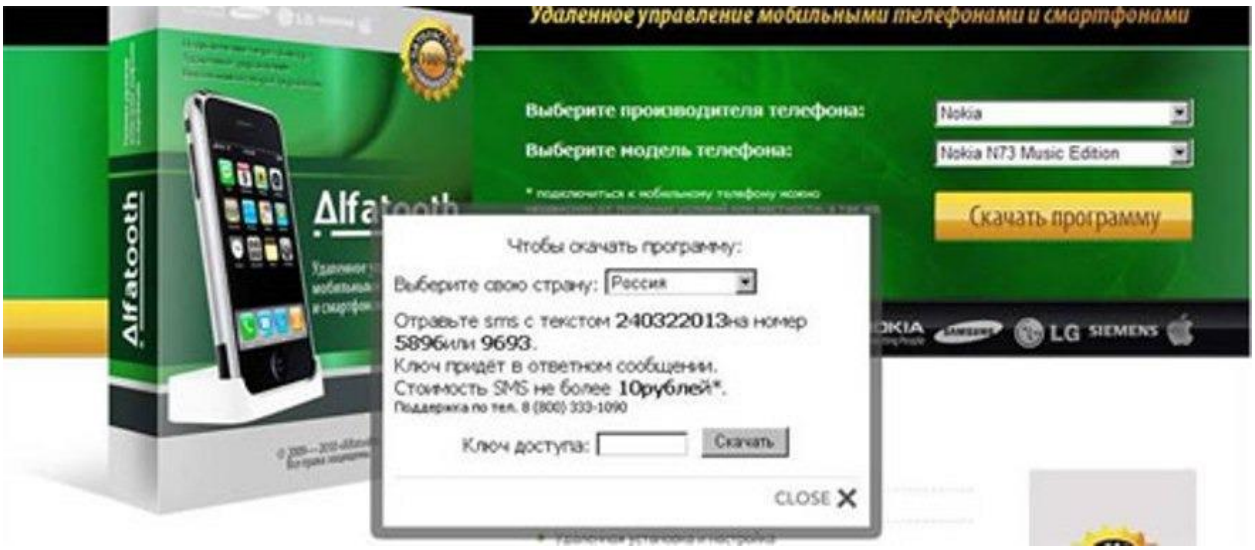


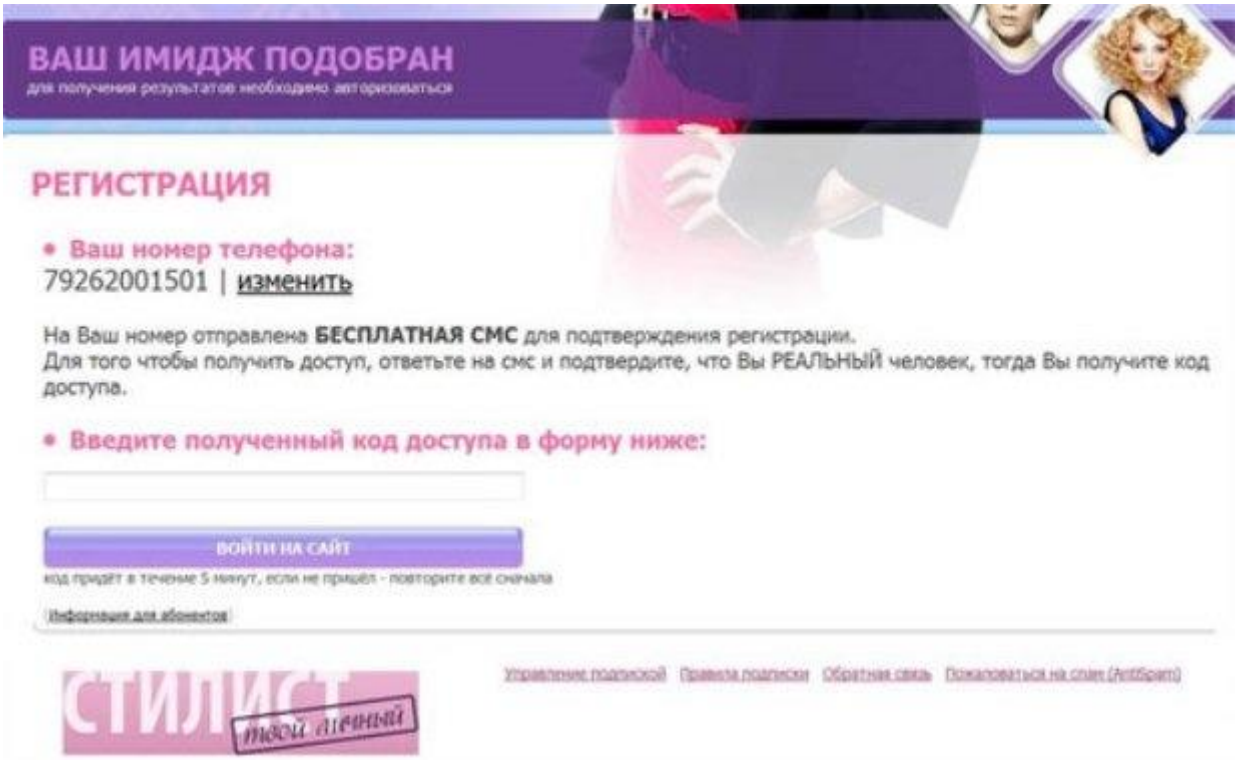
3. «Бесплатная» подписка на услуги

На информационном сайте вам предлагают оставить свой номер телефона, чтобы бесплатно получать те или иные новости, программы, информацию. При получении SMS с подтверждением вам предлагают ответить на него, чтобы подтвердить, что это ваш номер телефона.

Как правило, «бесплатные» услуги оказываются не таковыми, и вы получаете подписку на услуги.

Что делать: Не указывать свой номер телефона на незнакомых, подозрительных сайтах. Не отвечать на полученные SMS.





4. Работа за миллион рублей

На неком сайте предлагается идеальная работа с огромной зарплатой. Для получения координат работодателя вам необходимо отправить SMS (реже позвонить по телефону). В обоих случаях указанный номер является платным, вы оплачиваете стоимость SMS или каждой минуты разговора.

Что делать: Не отправлять SMS или не звонить, если вы не знаете сайт, на котором находитесь.

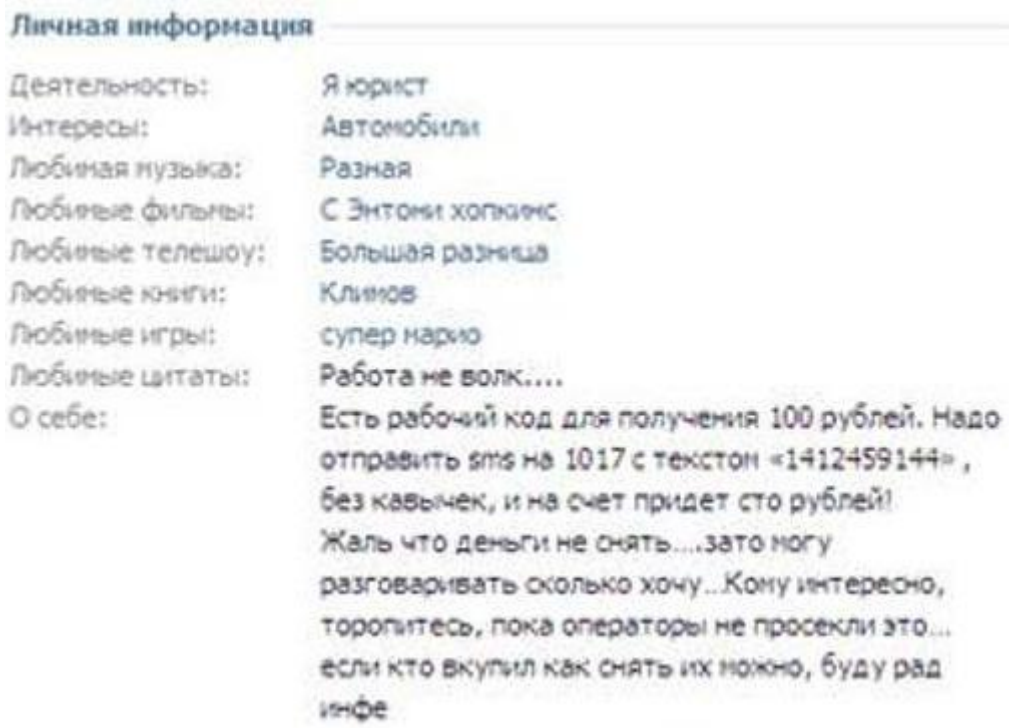
5. «Секретный» код

На неком сайте или форуме появляется подобное сообщение (текст может отличаться):

«Когда-то я работал в компании МегаФон, но они меня уволили из-за кризиса! Поэтому я хочу, чтобы как можно больше человек знали про секретный код, благодаря которому возможно пополнять свой баланс со всех мобильных сетей. Мы делали так: отправляешь SMS с текстом xxxxxx на номер XXXX, и в течение 10 минут приходило около 200р! ОБРАТИТЕ ВНИМАНИЕ, что пользоваться этой процедурой можно 2 раза в сутки! Я сообщаю это не для своей выгоды, а для того, чтобы отомстить им за то, что уволили квалифицированного работника!

100% работает на BeEline, MTS, MegaFon, SKyLinK, Tele, Tele2, а также Укр. оператор Киевстар!»

Что делать: Не отправлять SMS или не звонить, никаких секретных кодов не существует.



6. Социальные сети и другие ресурсы

Разными способами жертва перенаправляется на псевдо-сайты «Одноклассников», «ВКонтакте», где сообщается информация о проводимой «акции» и наличии для пользователя подарка. «Нам 4 года / Новый год / у Вас День рождения, всем дарим подарки, для получения отправьте SMS с текстом

xxxxxx на номер xxxx». Либо говорят о блокировке аккаунта: «Вас заблокировали за рассылку спама, подтвердите, что вы не бот, для этого отправьте SMS с текстом xxxxxx на номер xxxx».

Что делать: Не отправлять SMS или не звонить.

Информация взята с сайта www.mobile-review.com