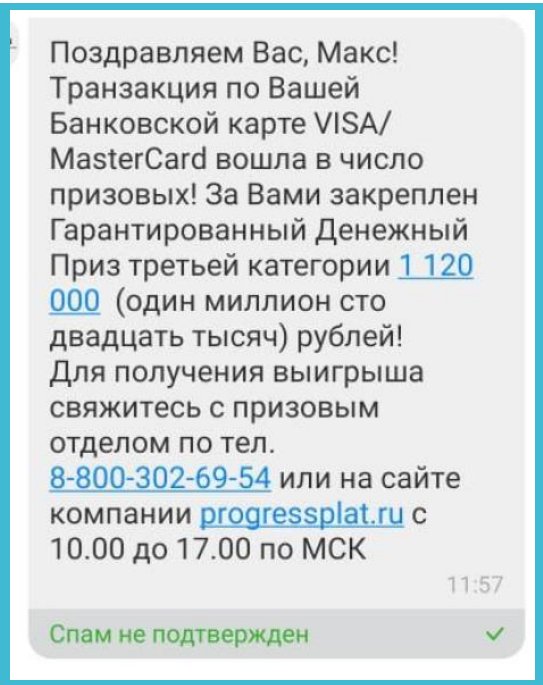
Ханты-Мансийская городская организация Общероссийской общественной организации «Всероссийское общество инвалидов»

ГРАНТ ГУБЕРНАТОРА ЮГРЫ

Выпуск №3

«Как заблокировать «мошеннический» сайт»



Мошенническое сообщение присланное нашему сотруднику.

- Некоторое время назад, в момент подготовки материалов по противодействию преступлениям в сфере компьютерной информации, нашему сотруднику пришло вот такое сообщение, явно мошеннического характера.
- Мы решили попробовать связаться с мошенниками, понять каким образом будут похищать денежные средства, и какие меры нужно предпринять для блокировки их сайта.
- ПРЕДУПРЕЖДАЕМ: в этом «эксперименте» нами использовался абсолютно новый номер, к которому не привязаны банковские карточки, мобильные банки и другие услуги. НИКОГДА не выходите на связь с мошенниками, если не уверены в том, что сможете контролировать ситуацию и не сообщите мошенникам личную информацию

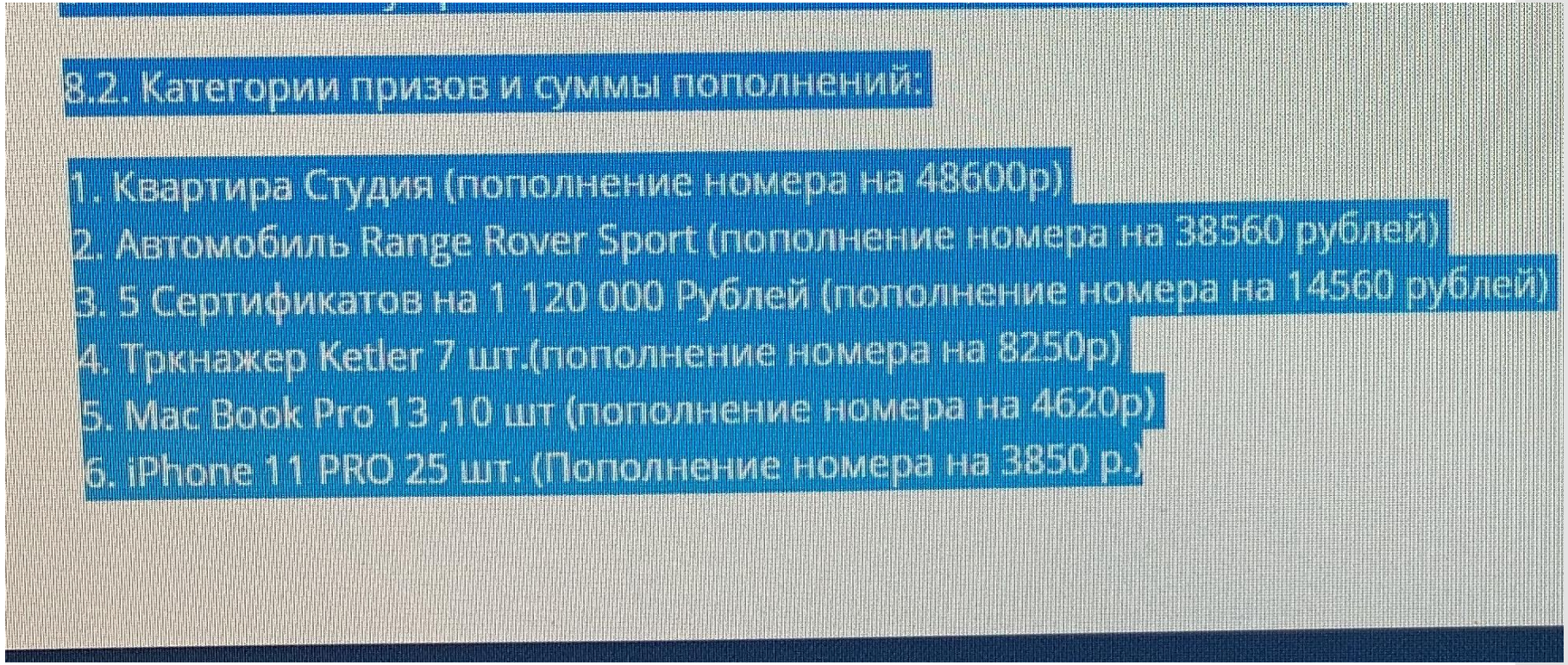
Явные ошибки в оформлении сайта.

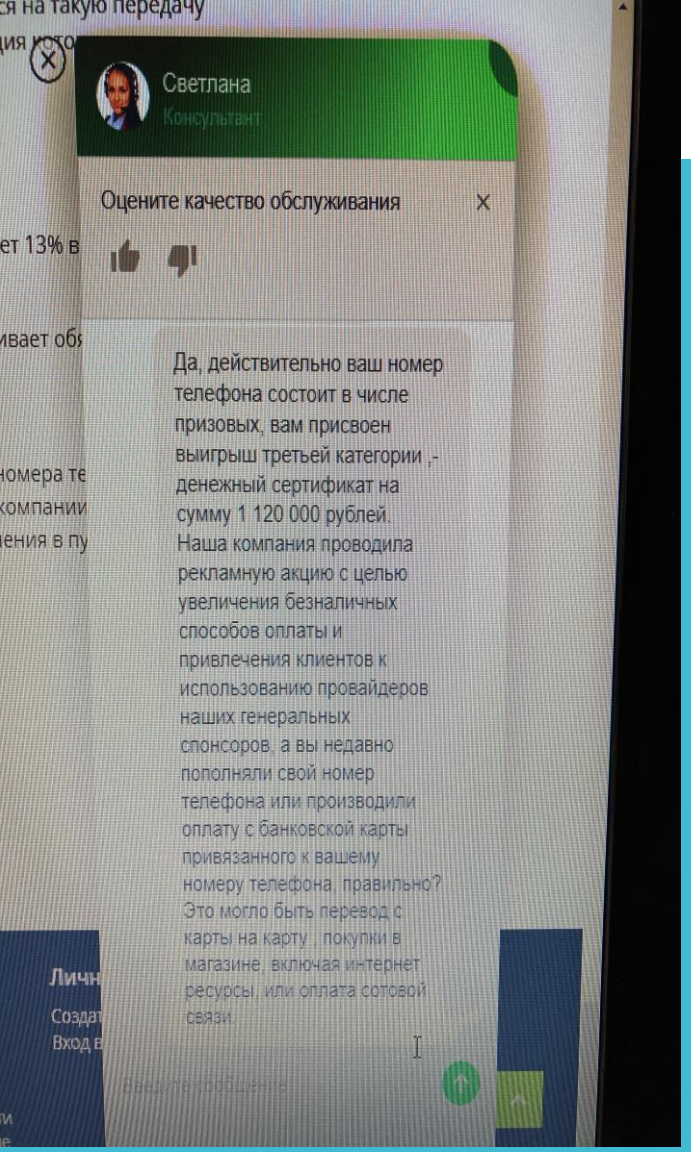
Обратите внимание на правильность оформления сайта и наличие грамматических ошибок:

-трКнажер Ketler вместо Тренажер keTtler .

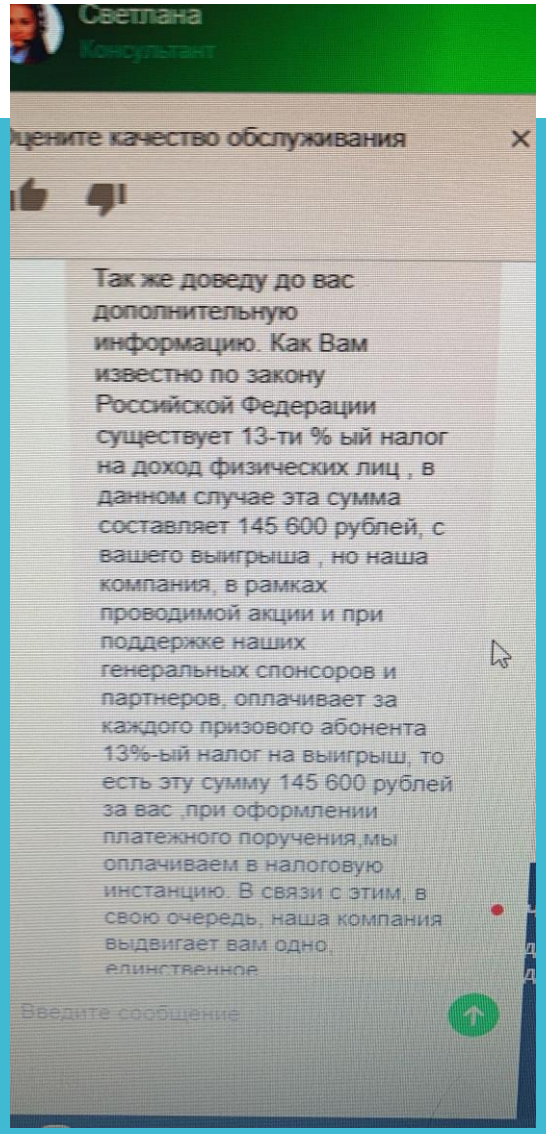
В одном случае «Пополнение» написано с большой буквы, в других – с маленькой.

Таким мелкие детали могут указывать на мошеннические действия, свидетельствуют о небрежности в его оформлении что не допускают серьезные компании.

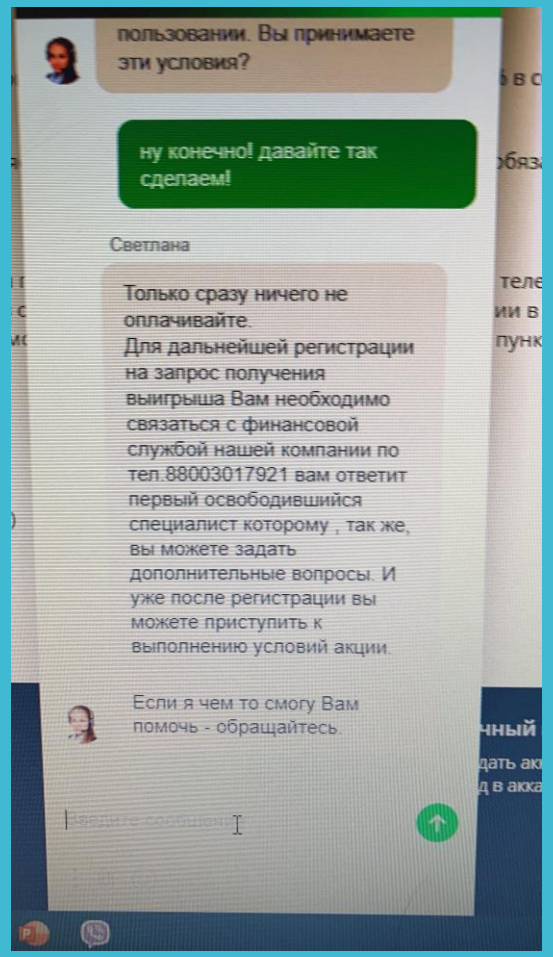




- Несмотря на то, что на наш номер не приходило сообщение о выигрыше, оператор службы помощи сайта подтвердил, что номер выигрышный, сумма выигрыша составляет 1 120 000 рублей.



- В ходе разговора Светлана- оператор сайта разъяснила, что нужно заплатить 13% налогов. Но ввиду их щедрости, они просят перечислить на свой счет мобильного телефона 10% от указанной суммы т.е чуть менее 15 000 рублей.



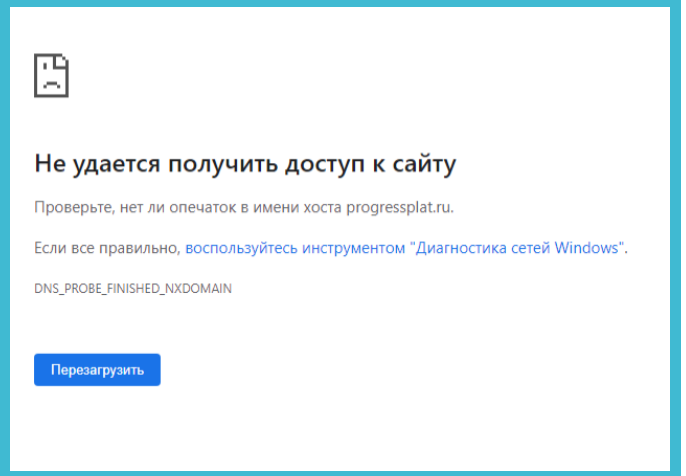
- После того, как нами показана заинтересованность в деньгах, Светлана попросила перевести разговор из интернета на телефон.
- Одновременно с этим Светлана начала готовить нас, что нужна регистрация, что является обязательным условием участия в акции.

- Сам телефонный разговор был построен на вовлечении жертвы в диалог и не дать её опомниться.
- Представитель компании постоянно говорил о сумме выигрыша, который мы можем получить. Было понятно, что он читает текст, при этом говорил быстро и много.
- Весь разговор сводился к тому, что нужно подойти к банкомату и ввести код.
- Одновременно с этим на телефон пришла смс с сообщением «никому не сообщайте код доступа в личный кабинет 8998».
- После этого продолжать диалог бессмысленно т.к. стало понятно, что отвлекая внимание жертвы, преступники просят подойти к банкомату, подключить личный кабинет и назвать им код доступа из смс. Сразу после этих действий жертва теряет контроль над своими деньгами и остается с пустым счетом. Мы прервали разговор с этими преступниками.

- После того, как выяснили способ хищения денежных средств преступниками наша команда решила заблокировать их ресурс.
- 1) нашли в интернете установочные данные сайта:

domain: PROGRESSPLAT.RU
nserver: adaline.ns.cloudflare.com.
nserver: rayden.ns.cloudflare.com.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGRU-RU
admin-contact: http://www.reg.ru/whois/admin_contact
created: 2021-05-26T08:49:52Z
paid-till: 2022-05-26T08:49:52Z
free-date: 2022-06-26
source: TCI

- Обратите внимание, сайт зарегистрирован менее недели до происходящих событий
- 2) написали письмо регистратору reg.ru с приложением скрин-шотов и переписки.
- 3) написали обращение в отдел К МВД РФ.



- По результатам наших обращений:

1) reg-ru заблокировал сайт мошенников, в настоящий момент он не работает.

2) отдел К направил наше обращение в местный территориальный отдел МВД, где по нему провели проверку в порядке ст. 144-145 УПК РФ.

На закрытие сайта, с учетом всех мероприятий у нас ушло 2 дня.

Таким образом, если вы столкнулись с явной схемой мошенничества через сайты, то стоит предпринять меры по их блокировке, для того чтобы другие граждане не пострадали от действий преступников.