POSITIVE TECHNOLOGIES

Опасность мобильной связи

Кирилл Пузанков
Positive Technologies

План

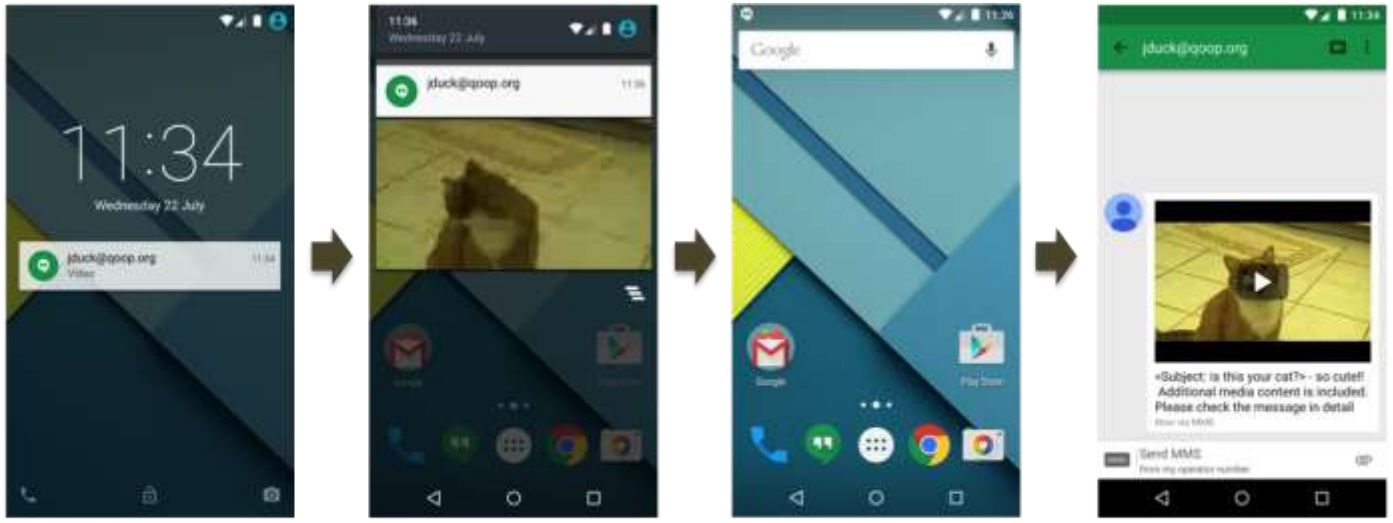
- Вирусы и трояны, уязвимости мобильных операционных систем
- Опасность публичного Wi-Fi
- Нежелательные подписки на платный контент
- Опасности мобильного банкинга и ДБО
- SMS-шлюзы и SIP-сервисы

Цели вирусов и троянов

- Денежные средства абонента
  - Отправка SMS на платные сервисы
  - Получение доступа к банковскому счету
- Кража конфиденциальных данных
- Привлечение мощностей телефона в ботнеты
- Выведение телефона из строя

Пример заражения смартфона

Уязвимости Android в библиотеке Stagefright



An MMS was received by Hangouts. At this point, an attacker may have already executed arbitrary code.

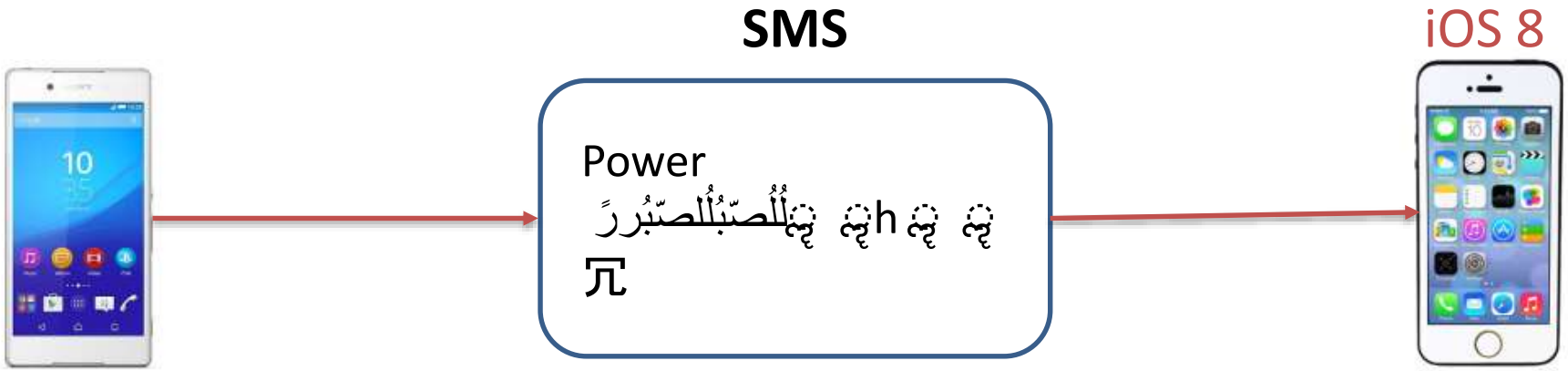
MMS notifications show a preview, which triggers the vulnerable code.

After unlocking the screen, no effects are apparent.

Viewing the MMS message triggers the vulnerable code again. Touching the video or rotating the screen triggers the vulnerable code again and again.

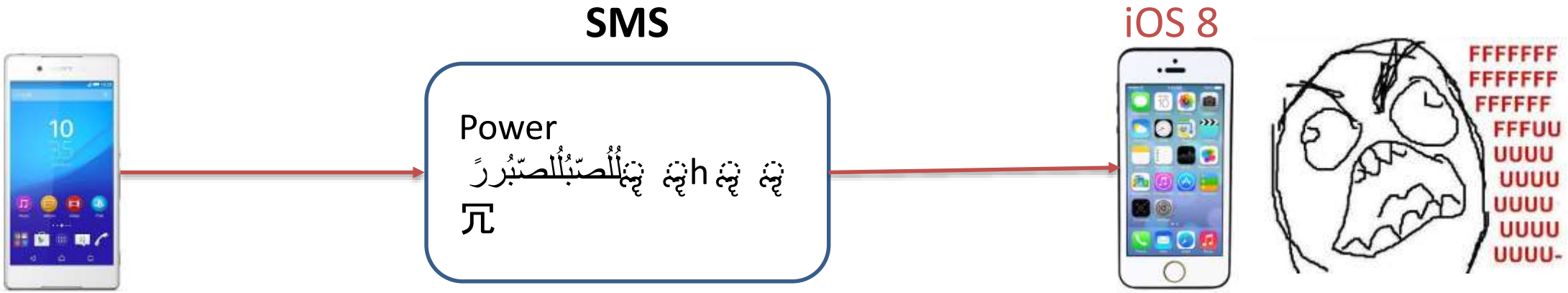
Пример эксплуатации уязвимостей

“Арабская SMS”



Пример эксплуатации уязвимостей

“Арабская SMS”



- Перезагрузка графической оболочки
- Запрет доступа к сообщениям, даже после перезагрузки смартфона

Меры защиты от вирусов, троянов и уязвимостей

- Следить за выходом прошивок, патчей, новых версий ОС
- Использование антивируса
- Осторожный серфинг в интернете
- Внимательное чтение манифестов при установке программ

Меры защиты от вирусов, троянов и уязвимостей

- Следить за выходом прошивок, патчей, новых версий ОС
- Использование антивируса
- Осторожный серфинг в интернете
- Внимательное чтение манифестов при установке программ
- Использование неуязвимого для вирусов телефона

Вопросы

Опасные особенности Wi-Fi

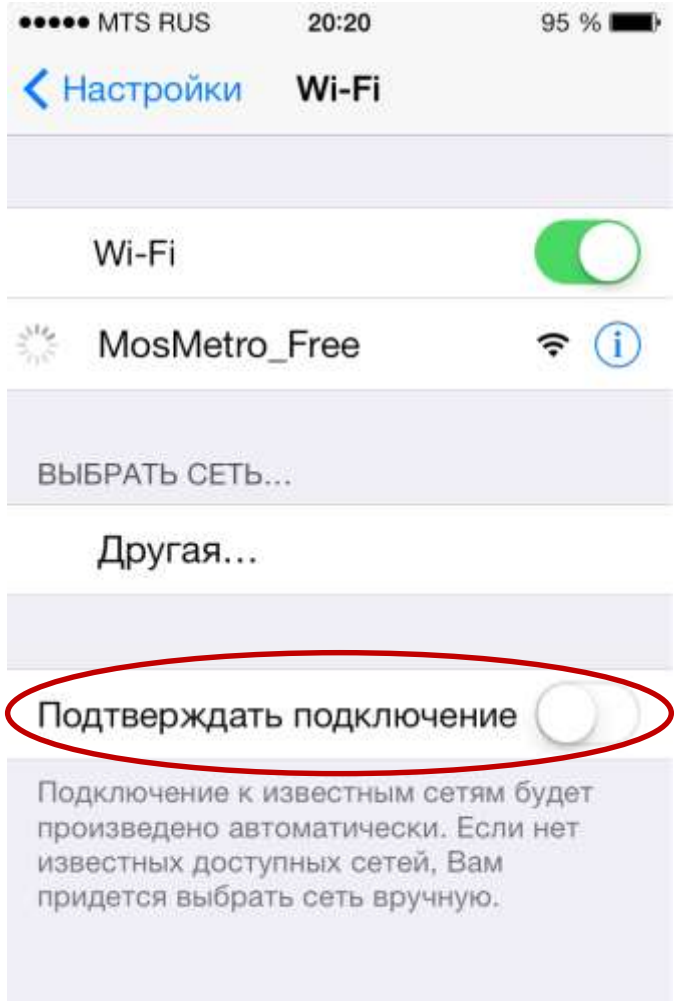
- Публичный Wi-Fi – раздолье для хакера
- Открытые сети могут быть созданы злоумышленником
- Хакеры используют SSID, похожий на легальный, либо в точности такой же

Как защититься от атак через Wi-Fi

- Использовать VPN
- Использовать защищенные протоколы (HTTPS) при работе с конфиденциальными данными
- Пользоваться только доверенными сертификатами
- Внимательно выбирать точку доступа
- Отдавать предпочтение 3G/4G сети вместо общественного Wi-Fi

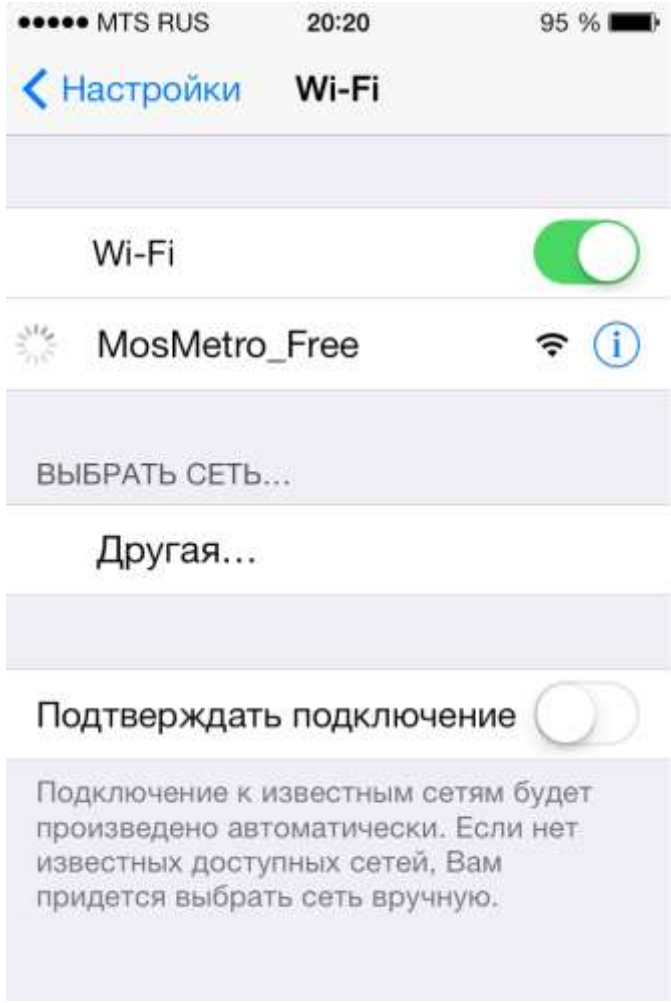
Как защититься от атак через Wi-Fi

- Не использовать функцию автоподключения к известным, а особенно открытым Wi-Fi сетям



Случаи подмены сетей

- На форуме PHDays была развернута сеть Wi-Fi MosMetro_Free
- Через WhatsApp и подобные приложения были получены телефонные номера подключившихся людей

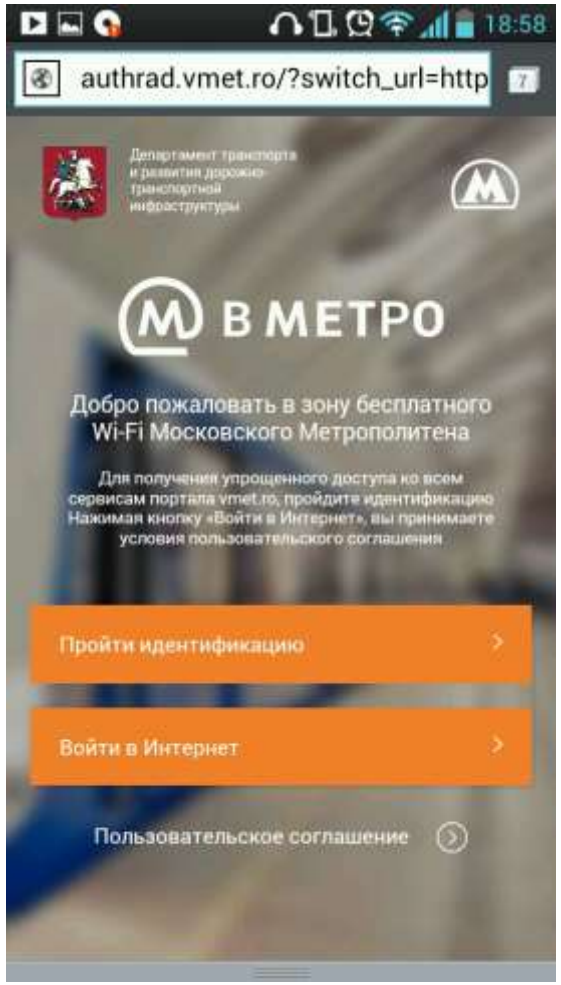


Случаи подмены сетей

- На форуме PHDays была развернута сеть Wi-Fi MosMetro_Free
- Через WhatsApp и подобные приложения были получены телефонные номера подключившихся людей
- Через SMS-шлюз были разосланы сообщения

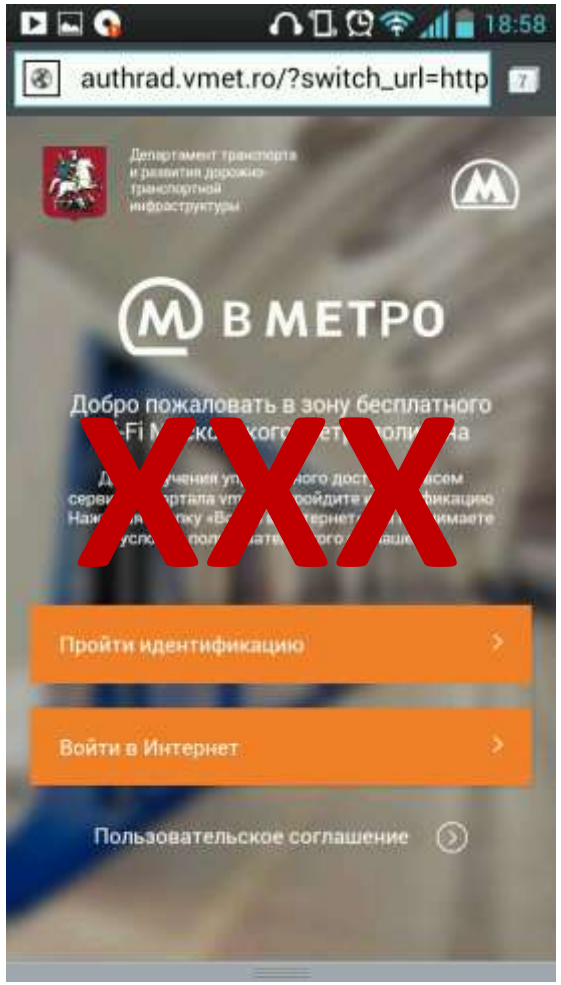
Случаи подмены сетей

- Люди увидели ролик порнографического содержания вместо привычной стартовой страницы входа в Wi-Fi метро



Случаи подмены сетей

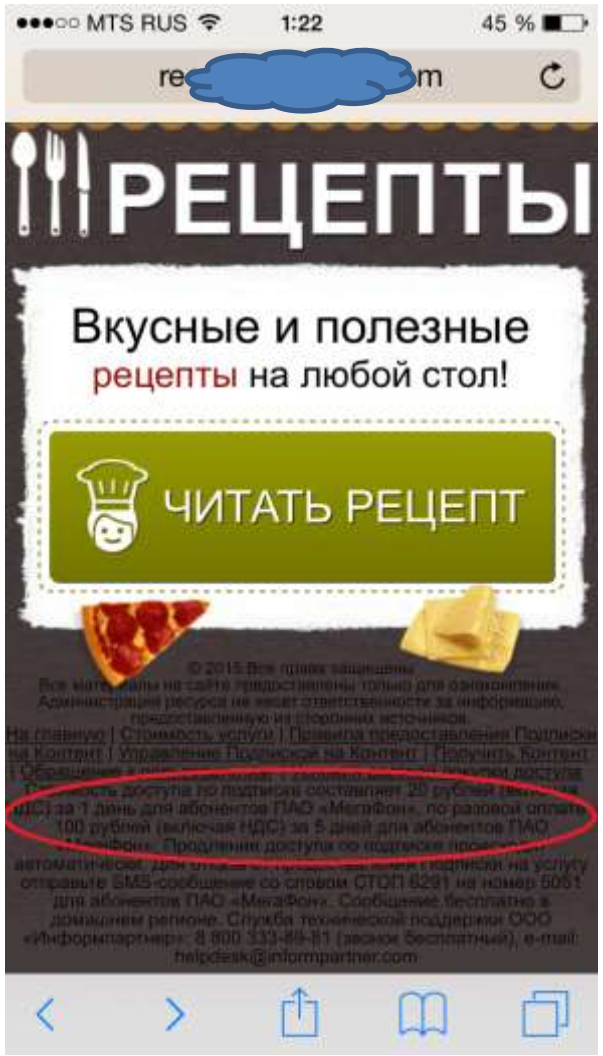
- Люди увидели ролик порнографического содержания вместо привычной стартовой страницы входа в Wi-Fi метро



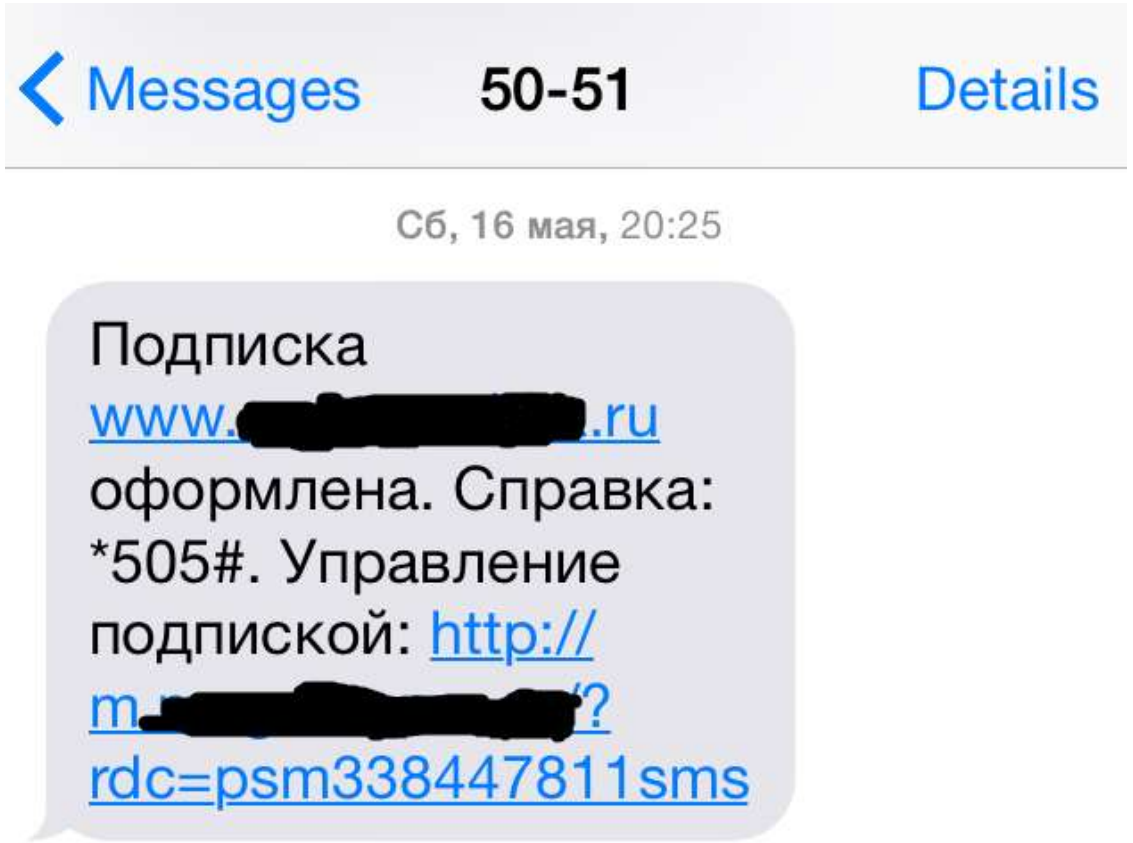
Вопросы

Нежелательные подписки

Нежелательные подписки



Нежелательные подписки



Как защититься от подписок

- Обращать внимание на мелкий шрифт перед нажатием заманчивых кнопок
- Использовать услугу запрета платных подписок
- Разделить счет на балансовый и счет для оплаты услуг мобильной коммерции

Вопросы

Опасности мобильного банкинга и ДБО

- Многие банки в последнее время перешли с КПК на SMS-коды
- Участились случаи незаконных замен сим-карт по поддельным документам и доверенностям
- Владельцы заново выданных SIM-карт получают уведомления МБ предыдущего владельца, если номер не был отключен от услуги

Меры защиты, вводимые банками и операторами

- Крупные банки фиксируют смену IMSI (уникального идентификатора SIM-карты) и перестают проводить операции до подтверждения клиентом смены SIM
- Антифродовые службы делают звонки при подозрительных операциях
- Некоторые операторы отключают возможность переводов на сутки-двое после замены SIM
- Некоторые операторы делают звонок на номер телефона, SIM-карту с которым планируется заменить по доверенности

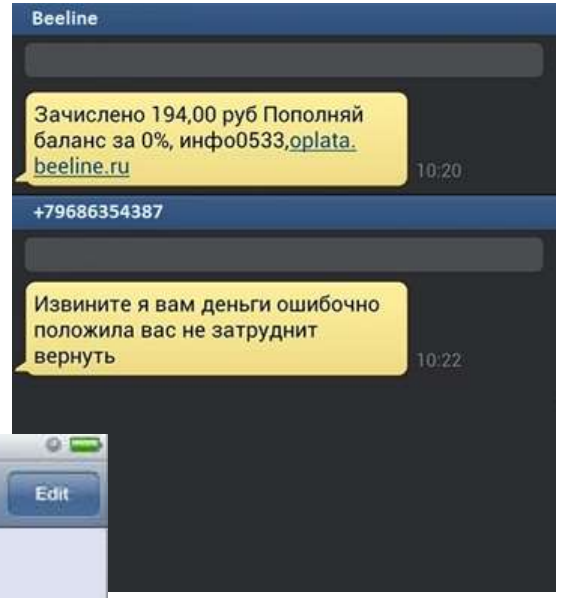
Вопросы

SMS-шлюзы

- Позволяют отправлять SMS, подставляя любой номер отправителя
- Вместо номера можно подставлять буквенные имена

SMS-шлюзы

- Позволяют отправлять SMS, подставляя любой номер отправителя
- Вместо номера можно подставлять буквенные имена



Меры предосторожности при получении странных SMS

- Проверять изменение баланса перед возвратом средств
- Связаться по телефону с родственником, просящим деньги в SMS
- Обращать внимание на номер банка, указанный в сообщении
- Не сообщать свои пин-коды, CVV-коды и пароли (банк никогда не запрашивает такие данные)

SIP-сервисы (голосовые вызовы)

- Позволяют делать подмену вызывающего номера
- Используются подобные схемы, как и при мошенничестве через SMS-шлюзы.

Меры предосторожности:

- При сомнении делать обратный звонок
- Не сообщать конфиденциальных данных

Вопросы

Спасибо за внимание

Кирилл Пузанков
kpuzankov@ptsecurity.com

POSITIVE TECHNOLOGIES