

Семинар «Информационная безопасность»

Безопасность платежей

Лекция 2

Ущерб от карточного мошенничества

- 4,6 млрд. рублей в России в 2013 году
- Россия — 4-я в Европе страна по количеству ущерба от мошенничества

Кто виноват?

Человеческий фактор:

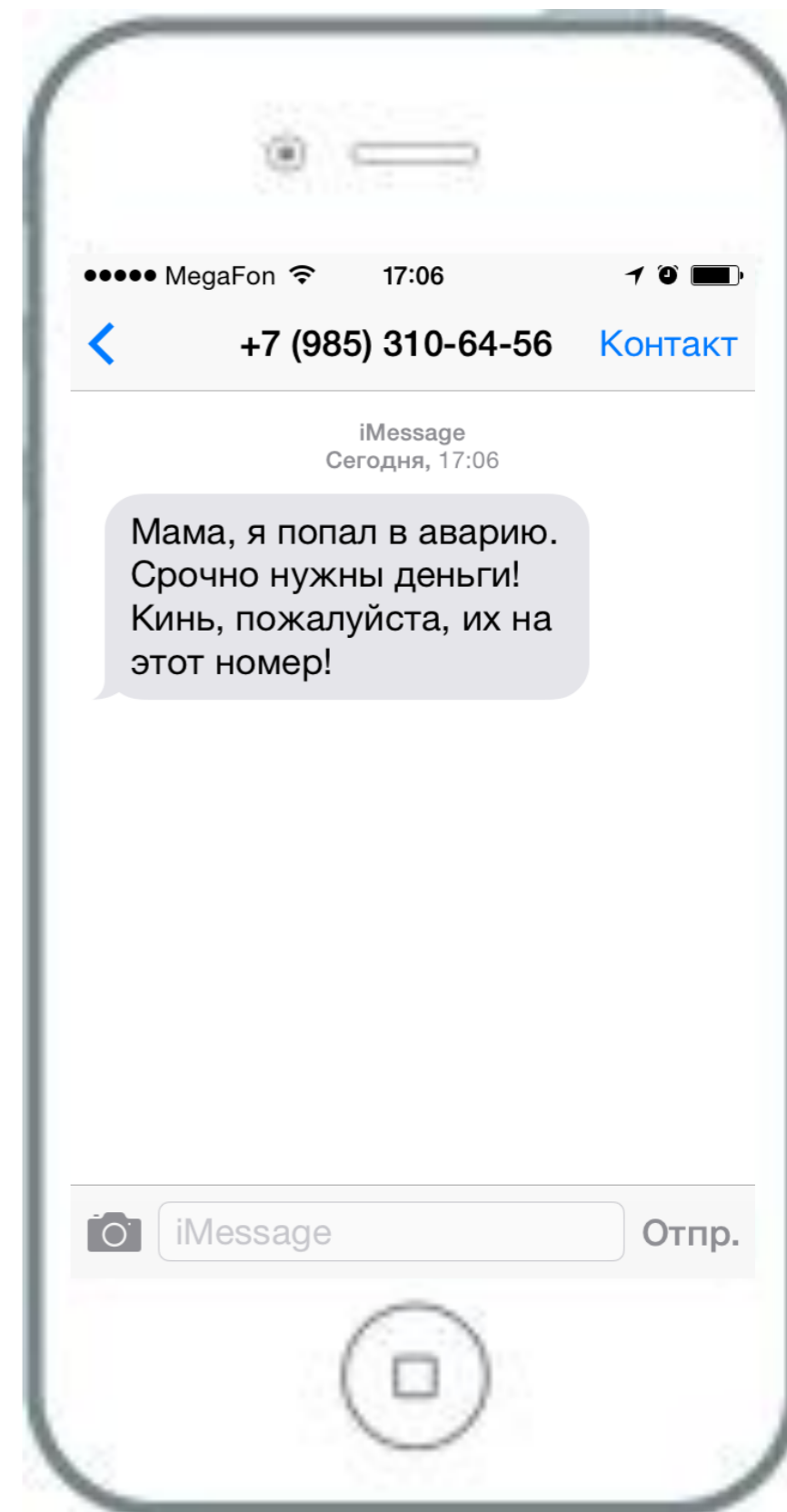
- Наивность
- Невнимательность
- Неосведомленность
- Беспечность

Фальшивые смски

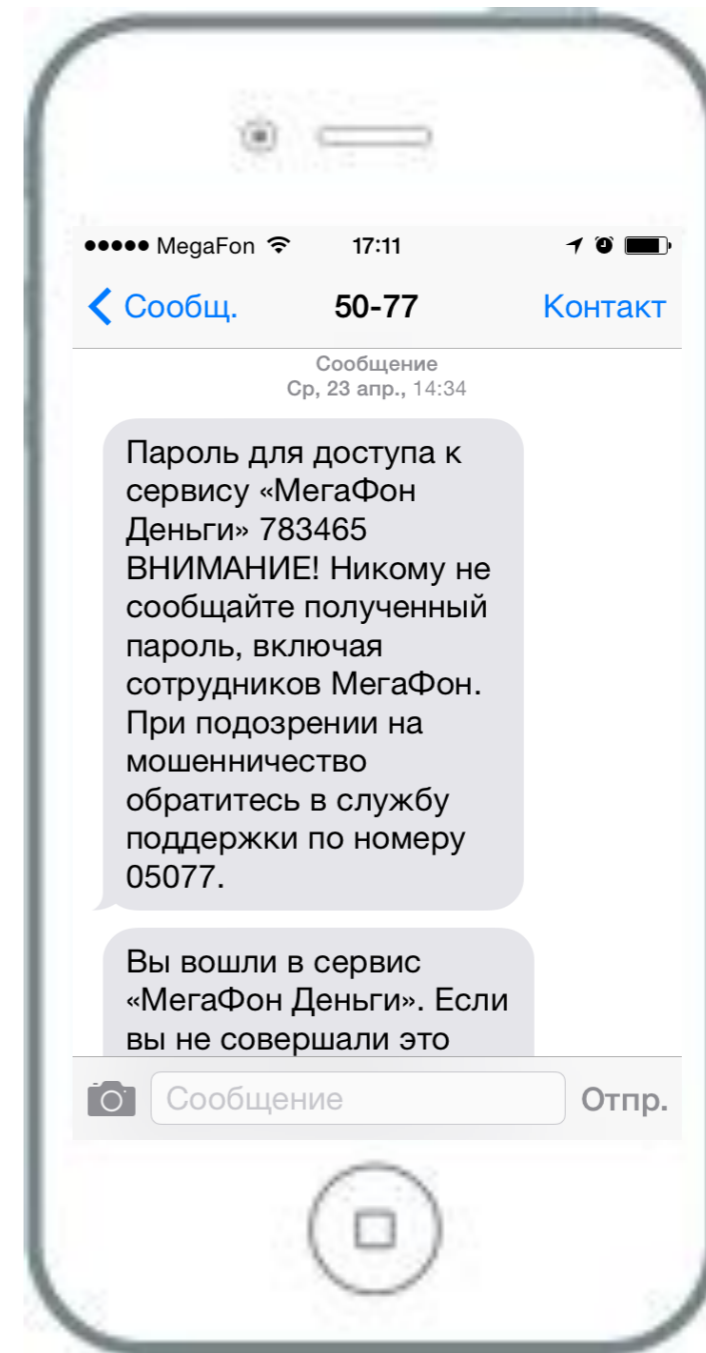
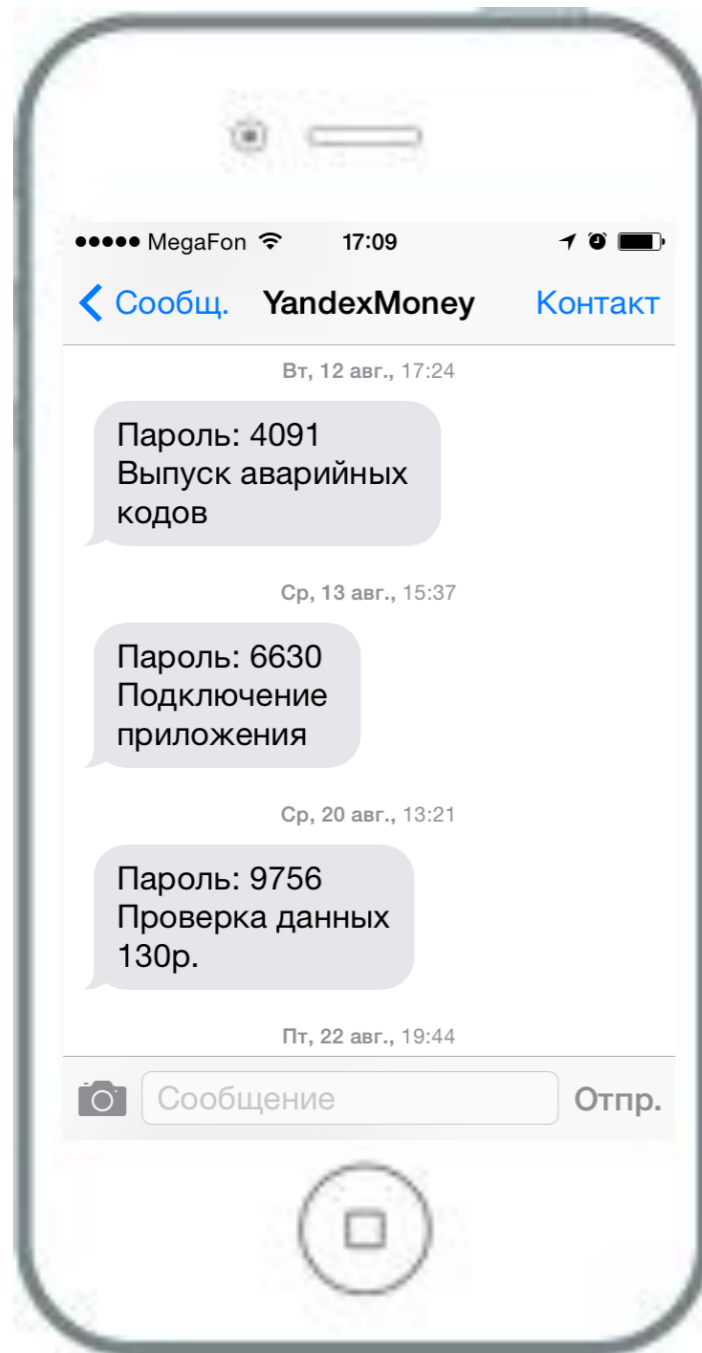
«Мама, я попал в аварию\больницу\полицию, срочно нужны деньги. Кинь их на этот номер\переводи на такой-то кошелек»

Выход:

Перезвонить тому, у кого проблемы, чтобы проверить информацию



Выманивание sms-пароля



«Официальные» письма платежных сервисов

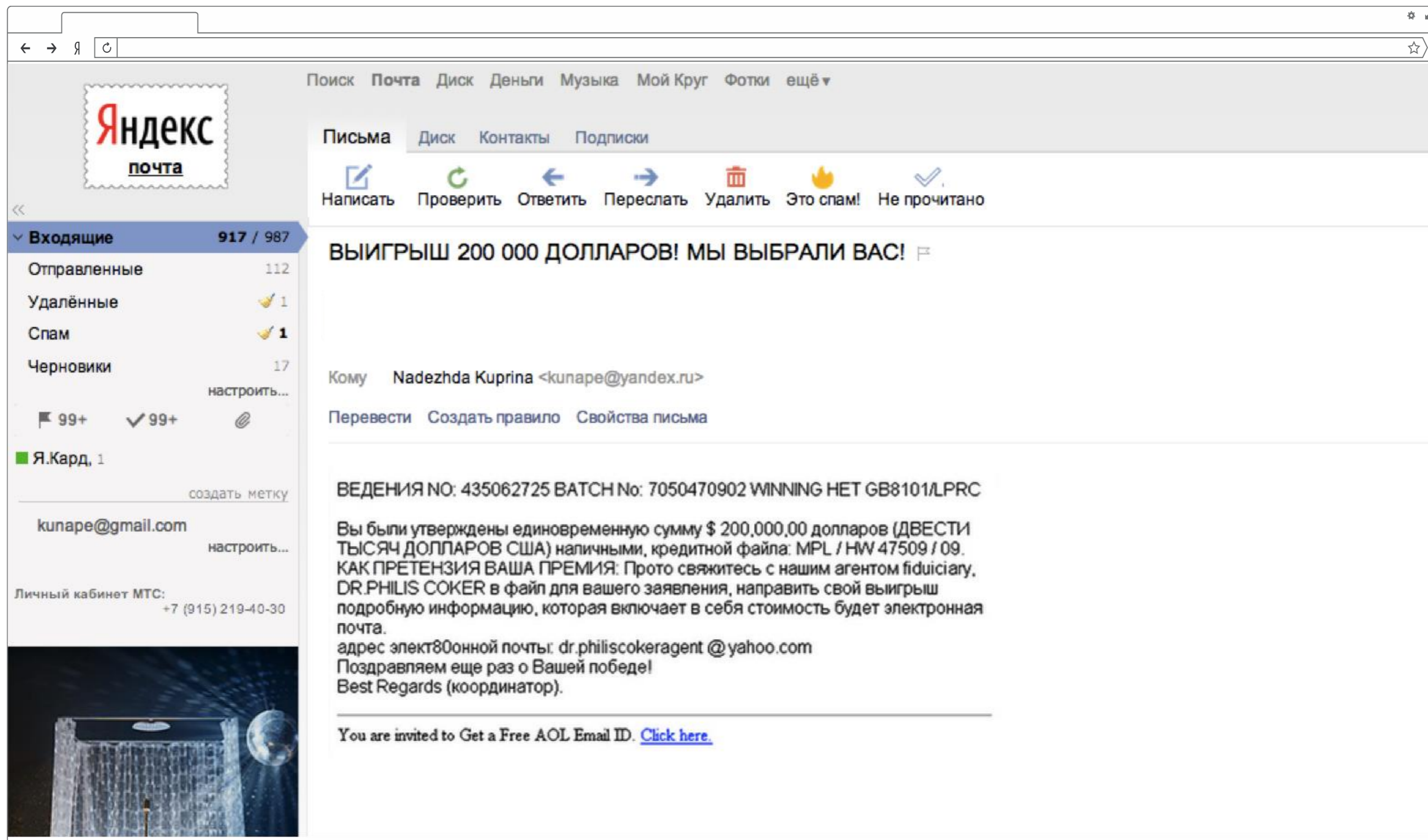
- «Ваш кошелек в Яндекс.Деньгах заблокирован. Для разблокировки перейдите по ссылке и введите пароль».
- «Вас беспокоит служба безопасности банка. Чтобы мы разрешили вам продолжать пользоваться картой, скажите проверочную информацию и пин-код».

«Официальные» письма платежных сервисов

Выход:

- Знать, что банки и платежные сервисы никогда не запрашивают у вас пин-коды, пароли и другую информацию.
- Проверять адрес сайта, на который вы переходите и где вводите свой пароль.

Фальшивые выигрыши в лотереи



The screenshot shows a Yandex Mail interface. The left sidebar contains navigation options: Входящие (917 / 987), Отправленные (112), Удалённые (1), Спам (1), Черновики (17), Я.Кард (1), and a contact for kupa@gmail.com. The main content area displays an email with the subject "ВЫИГРЫШ 200 000 ДОЛЛАРОВ! МЫ ВЫБРАЛИ ВАС!". The email body contains the following text:

ВЕДЕНИЯ NO: 435062725 BATCH No: 7050470902 WINNING NET GB8101/LPRC

Вы были утверждены единовременную сумму \$ 200,000,00 долларов (ДВЕСТИ ТЫСЯЧ ДОЛЛАРОВ США) наличными, кредитной файла: MPL / HW 47509 / 09. КАК ПРЕТЕНЗИЯ ВАША ПРЕМИЯ: Прото свяжитесь с нашим агентом fiduciary, DR.PHILIS COKER в файл для вашего заявления, направить свой выигрыш подробную информацию, которая включает в себя стоимость будет электронная почта. адрес элект80онной почты: dr.philiscokeragent @yahoo.com Поздравляем еще раз о Вашей победе! Best Regards (координатор).

At the bottom of the email, there is a link: "You are invited to Get a Free AOL Email ID. [Click here.](#)"

Фальшивые выигрыши в лотереи

Признаки:

- Вы ничего не знаете о данной лотерее и никогда в ней не принимали участие;
- Вы никогда не оставляли своих личных данных на этом ресурсе или этой организации, от лица которой приходит письмо;
- Сообщение составлено безграмотно, с орфографическими ошибками;
- Почтовый адрес отправителя – общедоступный почтовый сервис. Например, gmail.com, mail.ru, yandex.ru.

Пример “нигерийского” письма

Дорогой друг!

Я миссис Сесе-секо, вдова бывшего президента Заира (ныне Демократической республики Конго) Мобуту Сесе-секо. Я вынуждена написать Вам это письмо. Это в связи с моими нынешними обстоятельствами и ситуацией. Я спаслась вместе со своим мужем и двумя сыновьями Альфредом и Башером в Абиджан, Кот-д’Ивуар, где мы и поселились - затем мы переехали в Марокко, где мой муж умер от рака. У меня есть банковский счет на сумму 18 000 000 (восемнадцать миллионов) долларов США. Мне нужно ваше желание помочь нам - чтобы вы получили эти деньги для нас, в таком случае я представлю Вас моему сыну Альфреду, который имеет право получить эти деньги. Я хочу инвестировать эти деньги, но не хочу, чтобы было известно, что это делаю я. Мне хочется приобрести недвижимость и акции транснациональных компаний, а также вложиться в надежные и неспекулятивные дела, которые Вы посоветуете.

Искренне Ваша,

Миссис Мариам М. Сесе-секо

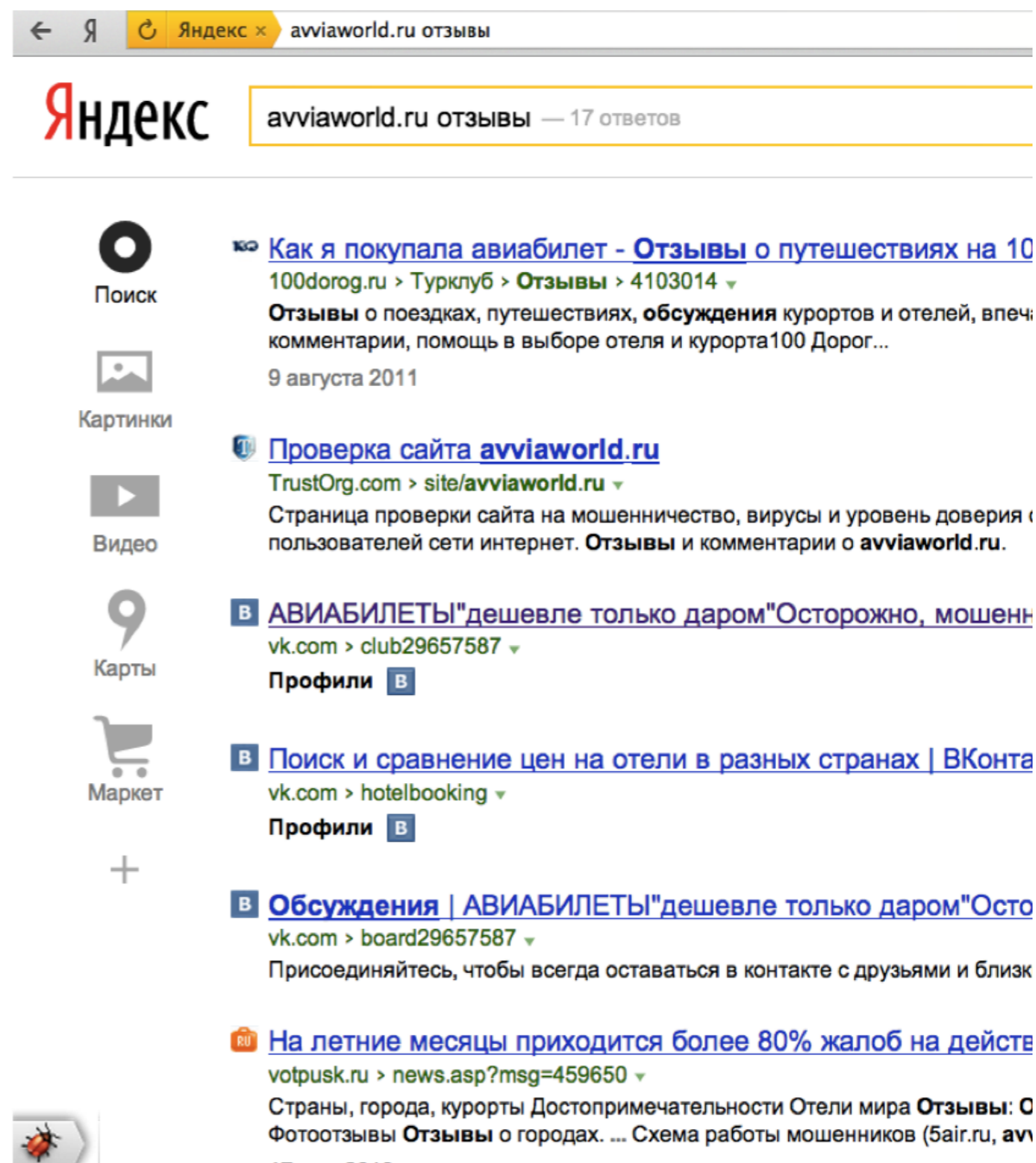
Сценарии

- Письмо о вакансии за рубежом, но перед выездом надо оплатить разрешение на проживание и работу
- Жертве сообщается о выигрыше в лотерею. Получатель письма должен заплатить, чтобы получить свой выигрыш.
- Жертве предлагается взять приличный кредит под бизнес, не требуя ни залога, ни стартового взноса. Все, что требуется — лишь оплатить издержки банка на оформление кредита

Фальшивые сайты авиабилетов

Выход:

Искать отзывы о неизвестном вам ранее сайте, прежде чем совершать покупку



The screenshot shows a Yandex search results page for the query "avviaworld.ru отзывы". The browser's address bar shows "Яндекс" and "avviaworld.ru отзывы". The search bar contains "avviaworld.ru отзывы" with "17 ответов" (17 answers) shown below it. On the left side, there is a vertical navigation menu with icons for "Поиск" (Search), "Картинки" (Images), "Видео" (Video), "Карты" (Maps), "Маркет" (Market), and a plus sign for more options. The main content area displays several search results:

- 100dorog.ru > Турклуб > Отзывы > 4103014**
Отзывы о поездках, путешествиях, обсуждения курортов и отелей, впечатления, комментарии, помощь в выборе отеля и курорта 100 Дорог...
9 августа 2011
- TrustOrg.com > site/avviaworld.ru**
Страница проверки сайта на мошенничество, вирусы и уровень доверия к пользователям сети интернет. Отзывы и комментарии о avviaworld.ru.
- vk.com > club29657587**
Профили
- vk.com > hotelbooking**
Профили
- vk.com > board29657587**
Присоединяйтесь, чтобы всегда оставаться в контакте с друзьями и близкими
- votpusk.ru > news.asp?msg=459650**
Страны, города, курорты Достопримечательности Отели мира **Отзывы:** О Фотоотзывы **Отзывы** о городах. ... Схема работы мошенников (5air.ru, av...

Фальшивые интернет-магазины

- По продаже ноутбуков
- И даже мотоциклов
- Товаров из-за границы

Выход:

- Искать отзывы о неизвестном вам ранее сайте, прежде чем совершать покупку

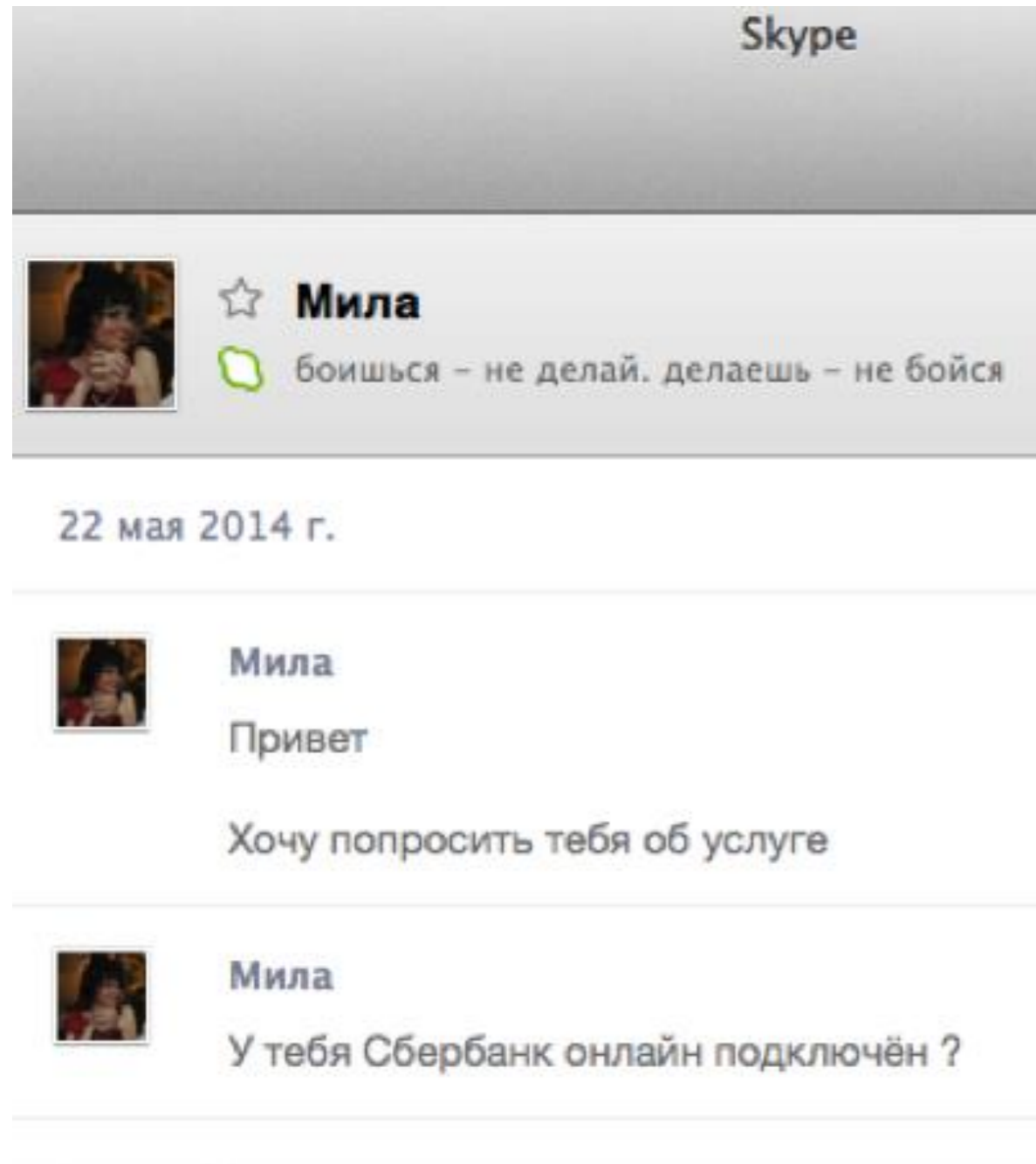
«Выгодные» покупки

- Новый iPhone за 3 тысячи рублей
- Распродажа товаров, якобы конфискованная на границе

Выход:

- Поверить, что халявы не бывает даже в интернете
- Поискать отзывы о магазине, прежде чем совершать покупку

Выпрашивание денег



- Со взломанных во ВКонтakte аккаунтов

- Со взломанных аккаунтов Skype

Выход:

- Перезвонить другу и уточнить информацию

- Задать «контрольный» вопрос, на который может ответить только друг

Халява с подпиской

Чтобы подключить доступ к Подписке на услугу
введите номер телефона:

– Я согласен с [Правилами](#) предоставления подписки на услугу

Введите свой номер мобильного телефона в формате +79161111111

Вам придет SMS с кодом для проверки номера телефона.
Пробный доступ дается ровно на 24 часа 📱, то есть на одни сутки.
Второй раз на вторые сутки пробный период не предоставляется.

**Правила предоставления подписки на услугу при активации
доступа к Подписке на Услугу через web-сайт контент-
провайдера**

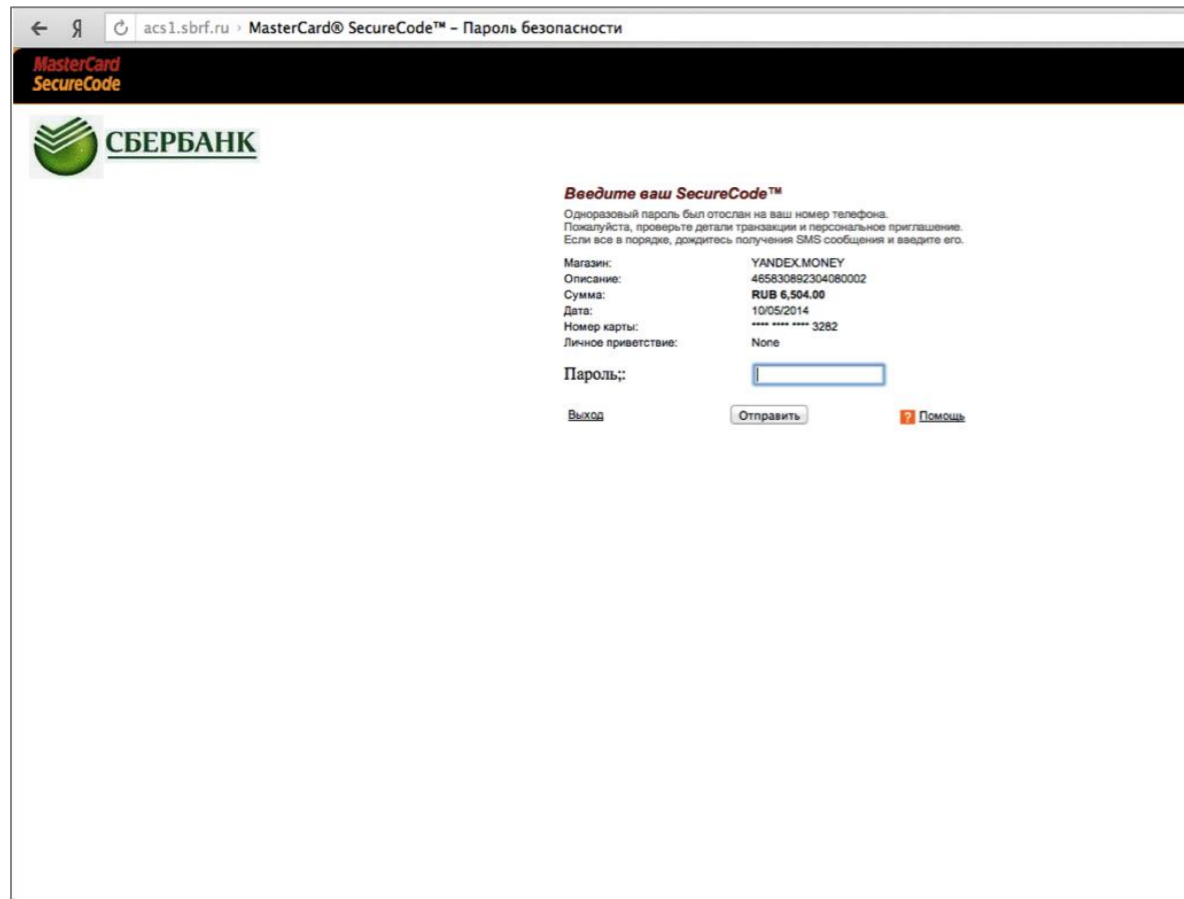
Выход:

- Не вводить номер своего телефона во время скачивания файлов
- Пользоваться легальными сервисами для прослушивания музыки (например, Яндекс.Музыка), просмотра фильмов (например, Amediateka, ivi.ru), чтения книг (Литрес, iBooks)

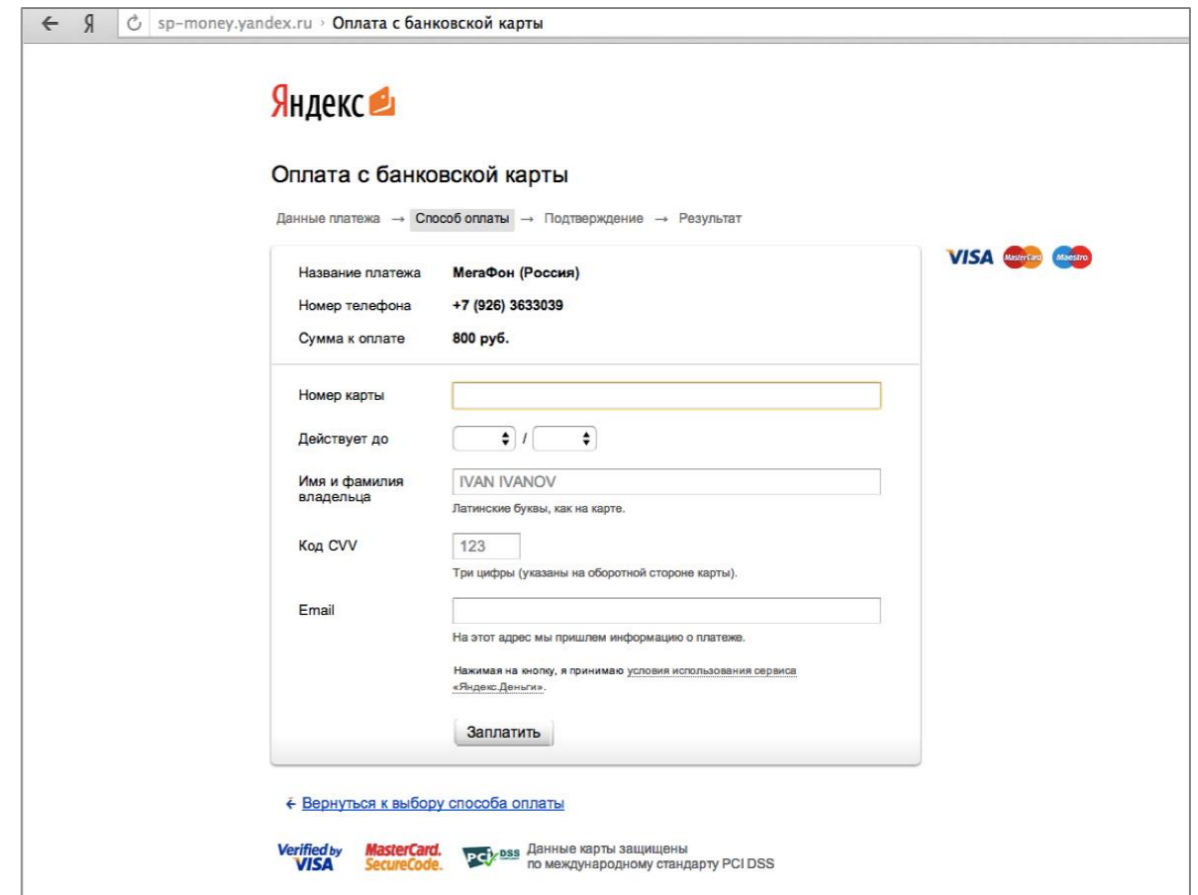
Что нужно знать о своей
банковской карточке?



Что нужно знать о платежах банковской картой?



The screenshot shows the Sberbank SecureCode page. The browser address bar displays 'acs1.sbrf.ru'. The page header includes the 'MasterCard SecureCode' logo and the Sberbank logo. The main heading is 'Введите ваш SecureCode™'. Below it, there is a message: 'Одноразовый пароль был отслан на ваш номер телефона. Пожалуйста, проверьте детали транзакции и персональное приглашение. Если все в порядке, дождитесь получения SMS сообщения и введите его.' To the right, transaction details are listed: 'Магазин: YANDEX.MONEY', 'Описание: 465830892304080002', 'Сумма: RUB 6,504.00', 'Дата: 10/05/2014', 'Номер карты: **** * 3282', and 'Личное приветствие: None'. A password input field is labeled 'Пароль:'. At the bottom, there are buttons for 'Выход', 'Отправить', and 'Помощь'.



The screenshot shows the Yandex Money payment page. The browser address bar displays 'sp-money.yandex.ru'. The page header includes the Yandex logo and the heading 'Оплата с банковской карты'. Below the heading, there is a progress bar with steps: 'Данные платежа' (selected), 'Способ оплаты', 'Подтверждение', and 'Результат'. To the right, there are logos for VISA, Mastercard, and Maestro. The main form contains the following fields: 'Название платежа: МегаФон (Россия)', 'Номер телефона: +7 (926) 3633039', 'Сумма к оплате: 800 руб.', 'Номер карты' (input field), 'Действует до' (date range), 'Имя и фамилия владельца: IVAN IVANOV' (with a note 'Латинские буквы, как на карте.'), 'Код CVV: 123' (with a note 'Три цифры (указаны на оборотной стороне карты).'), and 'Email' (input field with a note 'На этот адрес мы пришлем информацию о платеже.'). At the bottom of the form is a 'Заплатить' button. Below the form, there is a link: '← Вернуться к выбору способа оплаты'. At the very bottom, there are logos for 'Verified by VISA', 'MasterCard SecureCode', and 'PCI DSS' with the text 'Данные карты защищены по международному стандарту PCI DSS'.

Обращайте внимание на адрес сайта, на котором совершаете платеж

PCI DSS, иконки Mastercard и Visa

Базовые правила гигиены для электронного кошелька

- Одноразовый пароль на каждую операцию
- Лицензионный антивирус на компьютере
- Оплата с защищенного устройства (не общий wi-fi, не общий компьютер)

Если карта или кошелек скомпрометированы

- Срочно звонить в службу поддержки, не теряя ни секунды, и просить заблокировать операции
- Перевыпустить карту \ восстанавливать доступ к кошельку, следуя рекомендациям службы поддержки

**Как самостоятельно
вырыть себе яму?**



| Сфотографировать свою
карточку и выложить ее в
интернете. Красивая же!

Решение

- Не выкладывайте фото своей карты в интернет
- Если очень хочется, затирайте минимум 8 цифр
- Никогда никому не сообщайте CVC-код (три цифры с обратной стороны)



Рассекретить пароль

- Написать на бумажке и хранить на видном месте
- Дать пароль «на минутку» - особенно через сообщение в соцсетях
- Сообщить его по телефону «сотруднику банка» или «платежного сервиса»

Решение

- Использовать одноразовые пароли: SMS-пароли, таблицы кодов
- Даже одноразовые пароли никому не сообщать
- Включить sms-уведомления об операциях

Спасибо за внимание!