Антифишинг
www.antiphish.ru

Цифровые атаки на людей

Технологии, классификация атак и меры противодействия

Сергей Волдохин sv@antiphish.ru

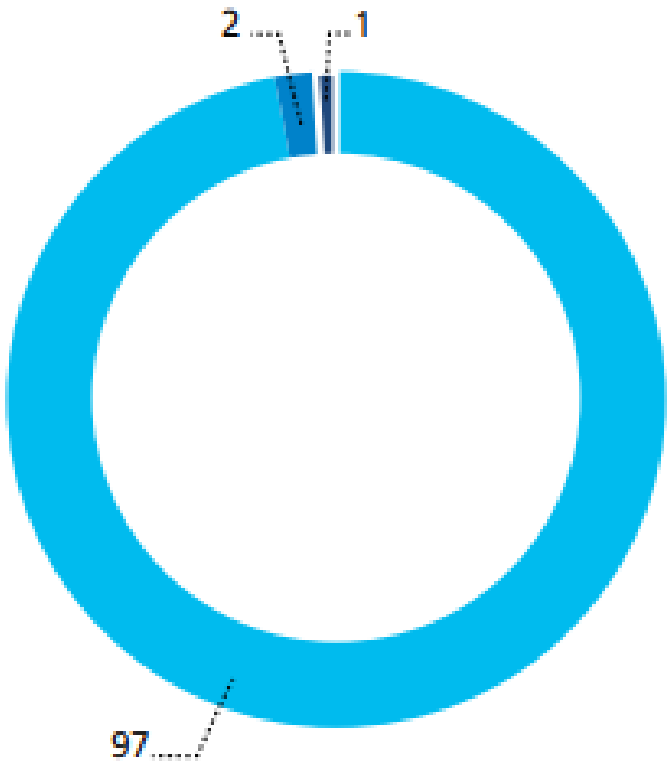
Самая большая проблема

Наша основная озабоченность на сегодняшний момент – это не технические атаки и вредоносное программное обеспечение. Нам понятно, как с этим бороться. Есть технические методы и методы через изменение законодательства.

Самая большая проблема – это социальная инженерия

Артем Сычев, первый заместитель директора департамента информационной безопасности Банка России – из обзора на XI Уральском форуме

Распределение по причинам
операций с использованием
(в соответствии с данными ф



Распределение по причинам совершения несанкционированных операций со счетов юридических лиц (%)

blog.antiphish.ru

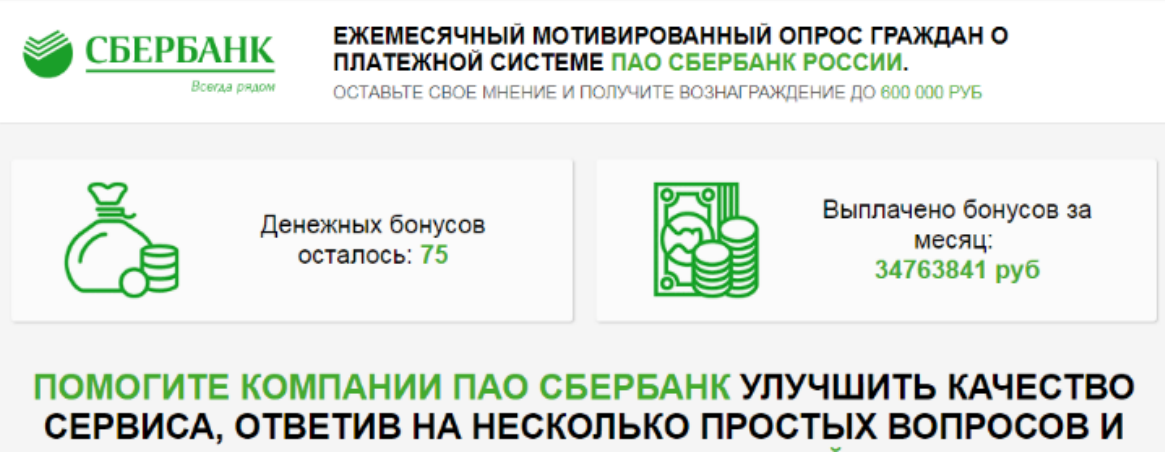
Антифишинг-дайджест №106 с 8 по 14 февраля 2019 года

Представляем новости об актуальных технологиях фишинга и других атаках на человека с 8 по 14 февраля 2019 года.

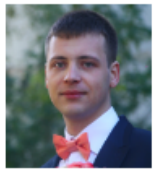
Сайты, почта и мессенджеры

Злоумышленники используют рекламные объявления Google для продвижения вредоносных сайтов.

Маскируясь под крупные банки, они предлагают пройти опрос и получить вознаграждение:



Андрей Жаркевич
редактор, ИТ-руководител



Артемий Богданов
технический директор

Сергей Волдохин
выпускающий редактор

antiphish.ru/classification

Outline

Антифишинг — сервис об...

Классификация цифровы...

Технологические векторы циф...

Электронная почта

Сайты

Социальные сети

Мессенджеры

Офис, рабочие помещения

Дополнительные технологиче...

Работа через устаревшие в...

Разнообразие версий опера...

Использование непицензио...

Психологические векторы атаки

Страх

«Ваш компьютер заражен и заблокирован. Кликните здесь»

Раздражение

«Чтобы отписаться, перейдите по ссылке»

Невнимательность

«www.sbernbank.ru», «www.gmall.com»

Любопытство

«Смотри, как ты отжигаешь на видео»

Жадность

«Скидка 50% при оплате прямо сейчас»

Желание помочь

«Кажется, ваш коллега потерял свои вещи. Дайте мне его номер»

Чт 07.02.2019 16:28

Zhdanov <comunicazione@mediatecatoscana.it>

заказ [redacted]

Кому [redacted]

Ваши документы

Добрый день!
Отправляю подробности

[redacted] Юрий Рудольфо

Менеджер Департамента

ООО [redacted]

СБИС
ЭЛЕКТРОННАЯ ОТЧЕТНОСТЬ
И ДОКУМЕНТООБОРОТ

[redacted]/documents/docs/

Печать документов на экран

**********Проверено Kaspersky Mail Checker **********

Внешняя

Желание помочь

СБЕРБАНК
Всегда рядом

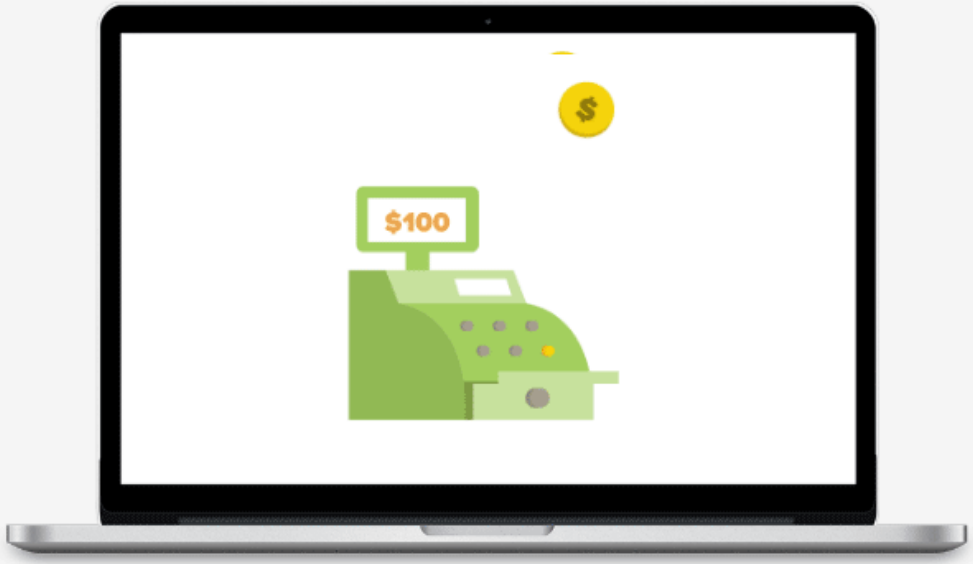
ЕЖЕМЕСЯЧНЫЙ МОТИВИРОВАННЫЙ ОПРОС ГРАЖДАН О ПЛАТЕЖНОЙ СИСТЕМЕ ПАО СБЕРБАНК РОССИИ.

ОСТАВЬТЕ СВОЕ МНЕНИЕ И ПОЛУЧИТЕ ВОЗНАГРАЖДЕНИЕ ДО 600 000 РУБ

Денежных бонусов осталось: 75

Выплачено бонусов за месяц: 34763841 руб

ПОМОГИТЕ КОМПАНИИ ПАО СБЕРБАНК УЛУЧШИТЬ КАЧЕСТВО СЕРВИСА, ОТВЕТИВ НА НЕСКОЛЬКО ПРОСТЫХ ВОПРОСОВ И ПОЛУЧИТЕ ДО 600 000 РУБЛЕЙ!



Личная

Авторитет

Жадность

СБЕРБАНК
Всегда рядом

Денежных бонусов осталось: 1

СРЕДСТВА УСПЕШНО ЗАЧИСЛЕНЫ НА ВНУТРЕННИЙ СЧЕТ!

СУММА ВОЗНАГРАЖДЕНИЯ, ГОТОВАЯ К ОТПРАВКЕ СОСТАВЛЯЕТ:

153 015 РУБЛЕЙ

В связи с лимитами платежных систем, перевод будет отправлен двумя равными частями **в течение 10 минут.**

Чтобы моментально и в полном размере получить выплату необходимо выполнить закрепительный платеж. С Вашей карты/кошелька будет списана сумма **150 руб.**

Личная

Срочность

Жадность

Личная

Срочность

Социальное одобрение

1	Заголовок письма	Открытие корреспондентского счета!
2	Текст письма	Добрый день! Я, Григоренко Дмитрий Федорович, Начальник отдела межбанковских операций и корреспондентских отношений ЗАО "Банк ICA". Вели с Вашим банком переговоры по открытию и обслуживанию корреспондентского счета. Прошу Вас в кратчайшие сроки рассмотреть заявку на открытие и обслуживание корреспондентского счета. Договор прилогаю в архиве и прошу его заполнить. Зарание Вам благодарен, жду ответа. С уважением, Начальник отдела межбанковских операций и корреспондентских отношений ЗАО "Банк ICA" Григоренко Дмитрий Федорович 455044 Россия Челябинская область, город Магнитогорск, улица Гагарина, дом 25

Внешняя

Срочность

Авторитет

Желание помочь

Что должны знать и уметь ваши сотрудники?

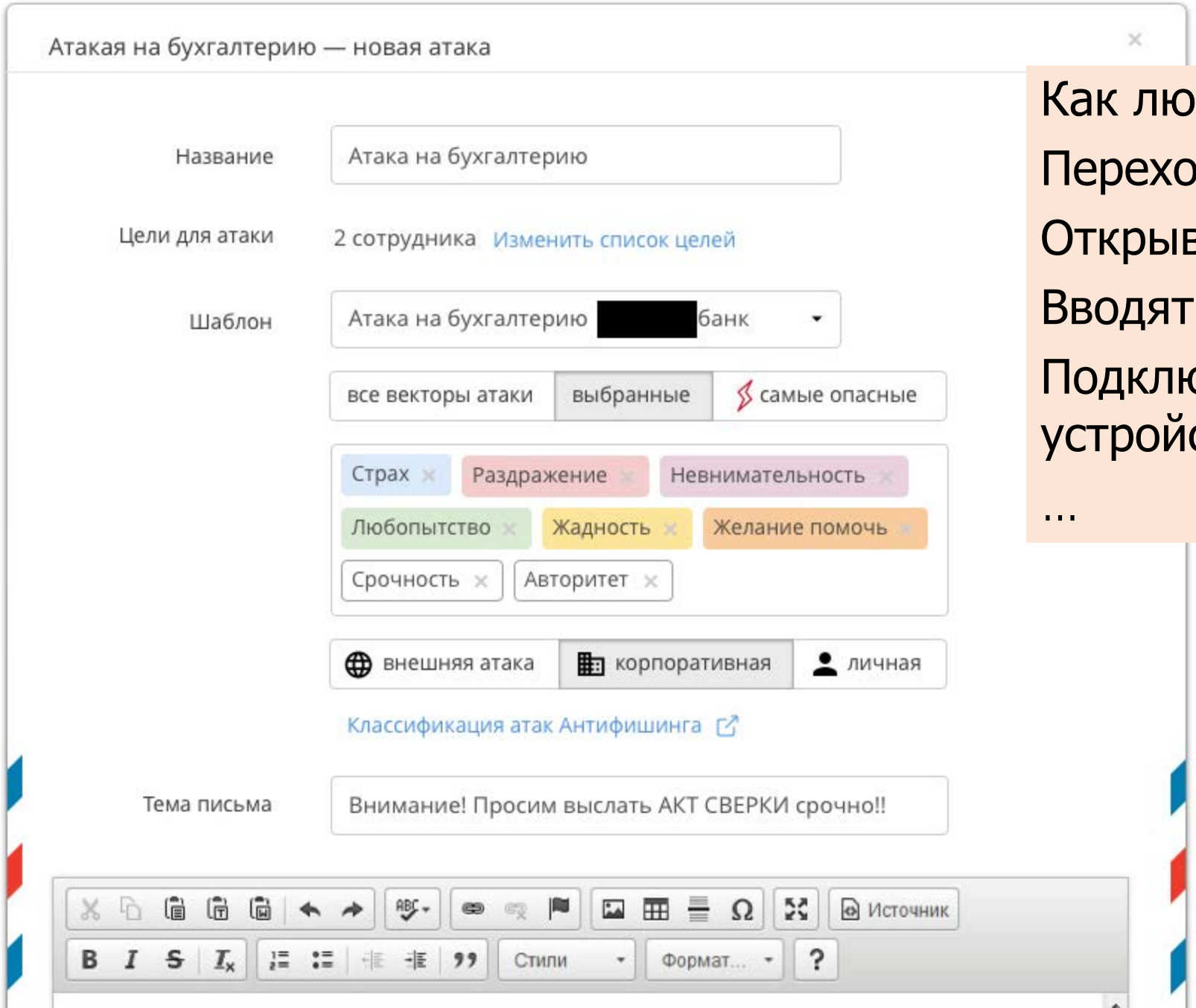
Какие навыки влияют на безопасность?

(Знания + Навыки) + Измерение

Тренируйте и измеряйте эти навыки

antiphish.ru/template

Ид	Сценарий	Вектора атаки	Технологии
1	Руководитель HR-отдела обращается к сотруднику по имени и сообщает, что заключен договор с новой компанией ДМС. Обещают бесплатную стоматологию и полный чек-ап в известном медицинском центре. Полный список услуг во вложении. Полисы в этом месяце получат только те, кто перейдет по ссылке.	Корпоративная Персональная Жадность Любопытство Срочность	Эл. письмо Вложение MS Word Ссылка



Как люди открывают письма

Переходят по ссылкам

Открывают вложенные файлы

Вводят данные в формы

Подключают съемные устройства

…

Атаки на сотрудников

Электронная почта Съемные устройства Создать атаку

Атака на бухгалтерию 127 целей

Страх × Раздражение × корпоративная

отчеты за 20 марта 12:09

Атака на все отделы 2 390 целей

Любопытство × Жадность × Желание помочь × внешняя

Невнимательность × Срочность × Авторитет ×

отчеты за 13 марта

Тестовая атака Секретари 22 цели

Жадность × Авторитет × личная

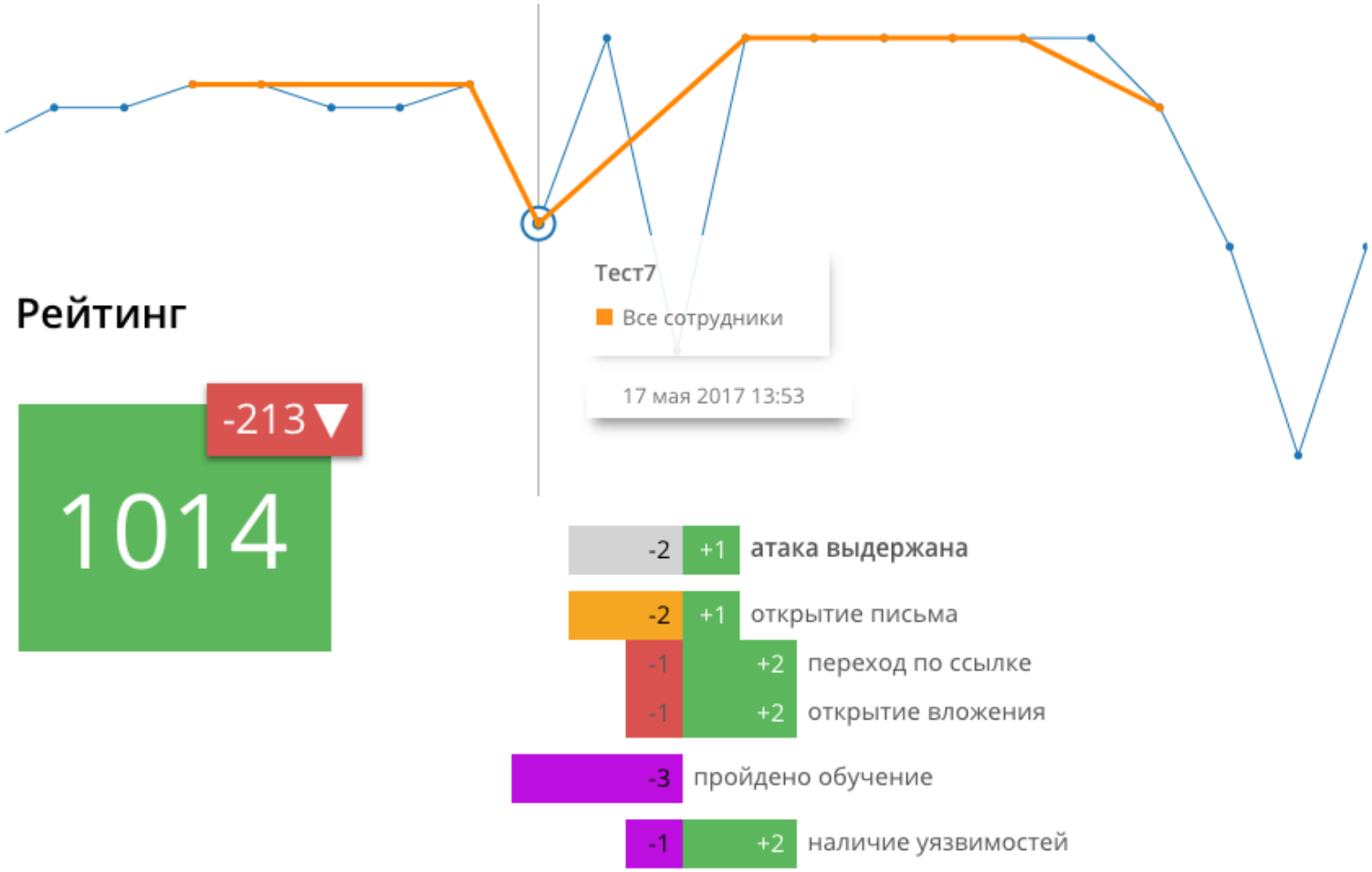
отчеты за 7 марта

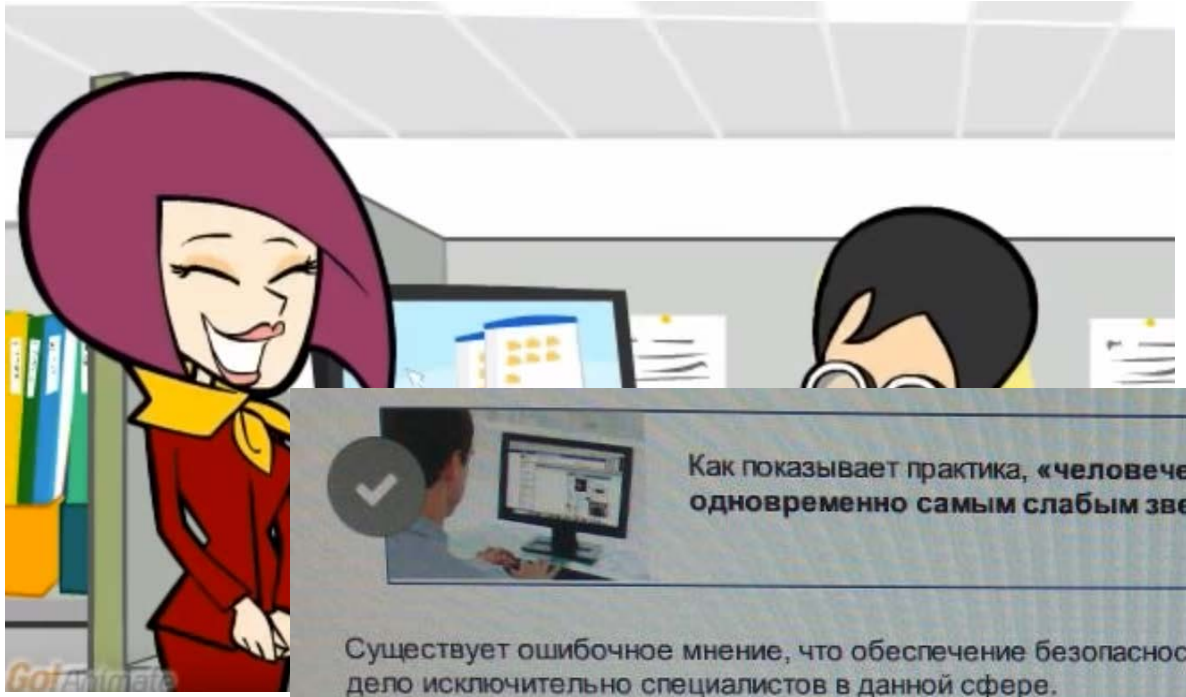
Все психологические векторы покрыты?

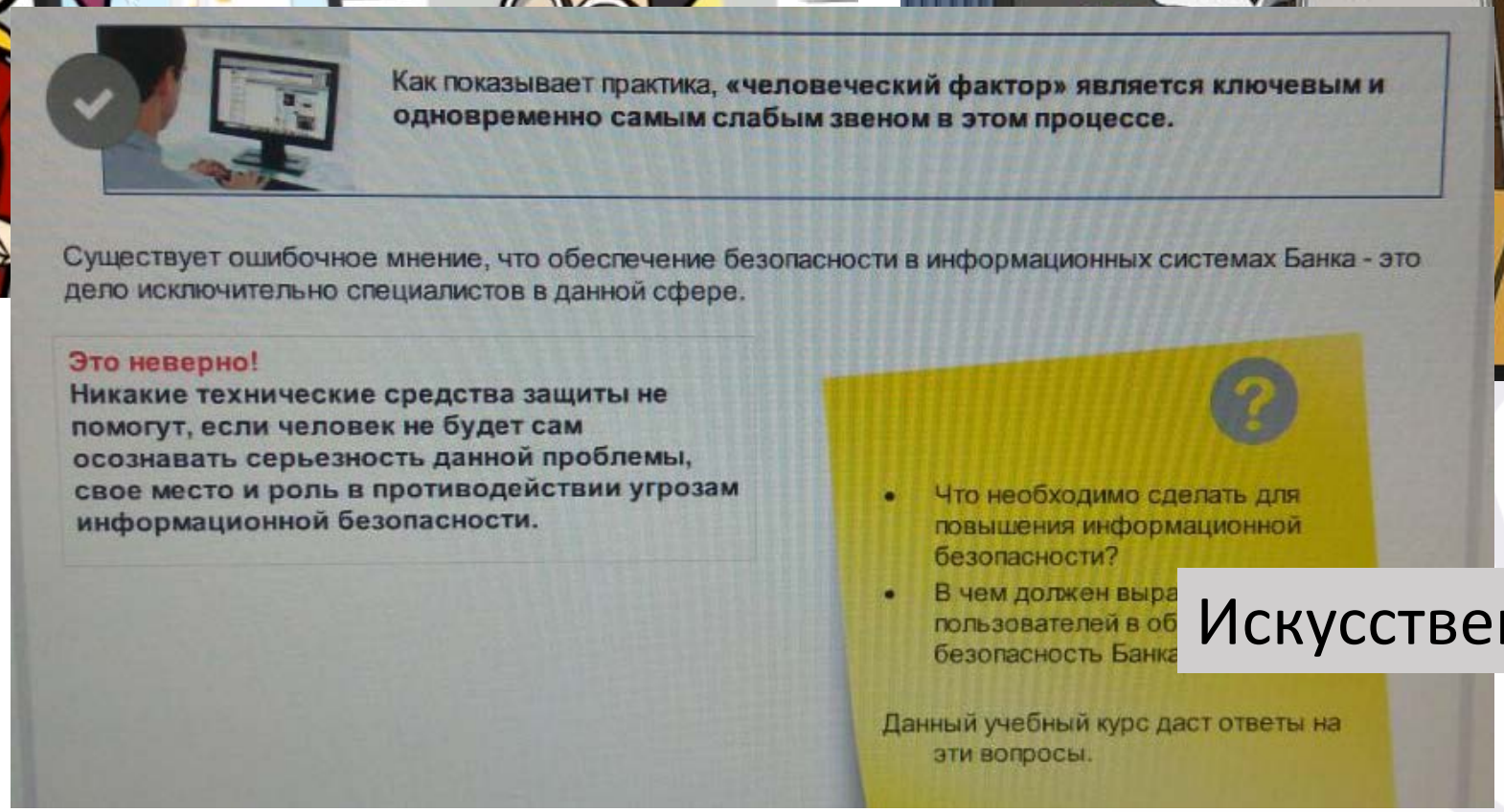
Организационные векторы?

Проверка навыков

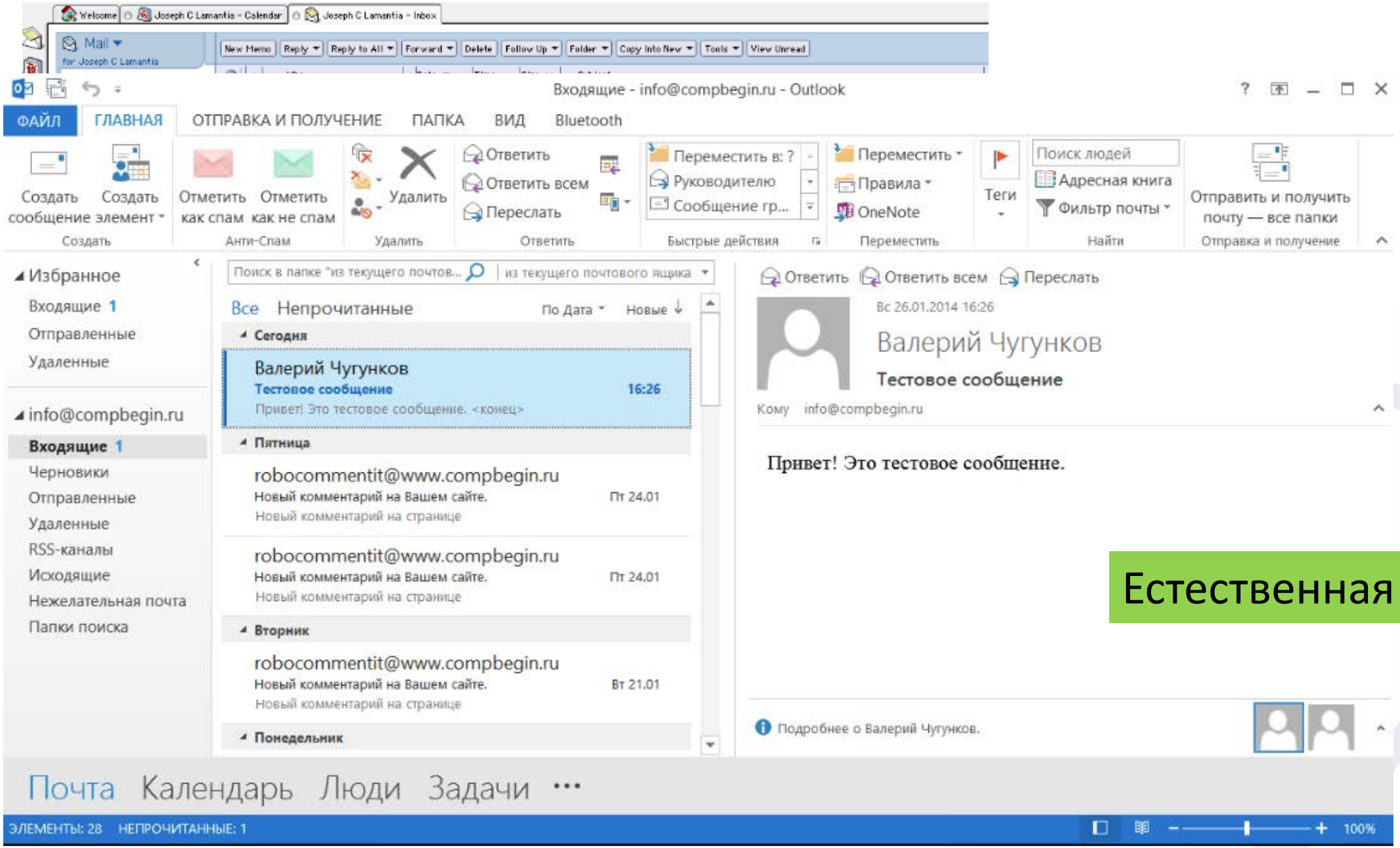
Как меняется поведение людей?







Искусственная среда



Естественная среда

[redacted]

16 ч ·

"Thanks #Aeroflot!"

Аэрофлот дает 2 бесплатных билета всем!
Отпраздновать 33-ю годовщину!

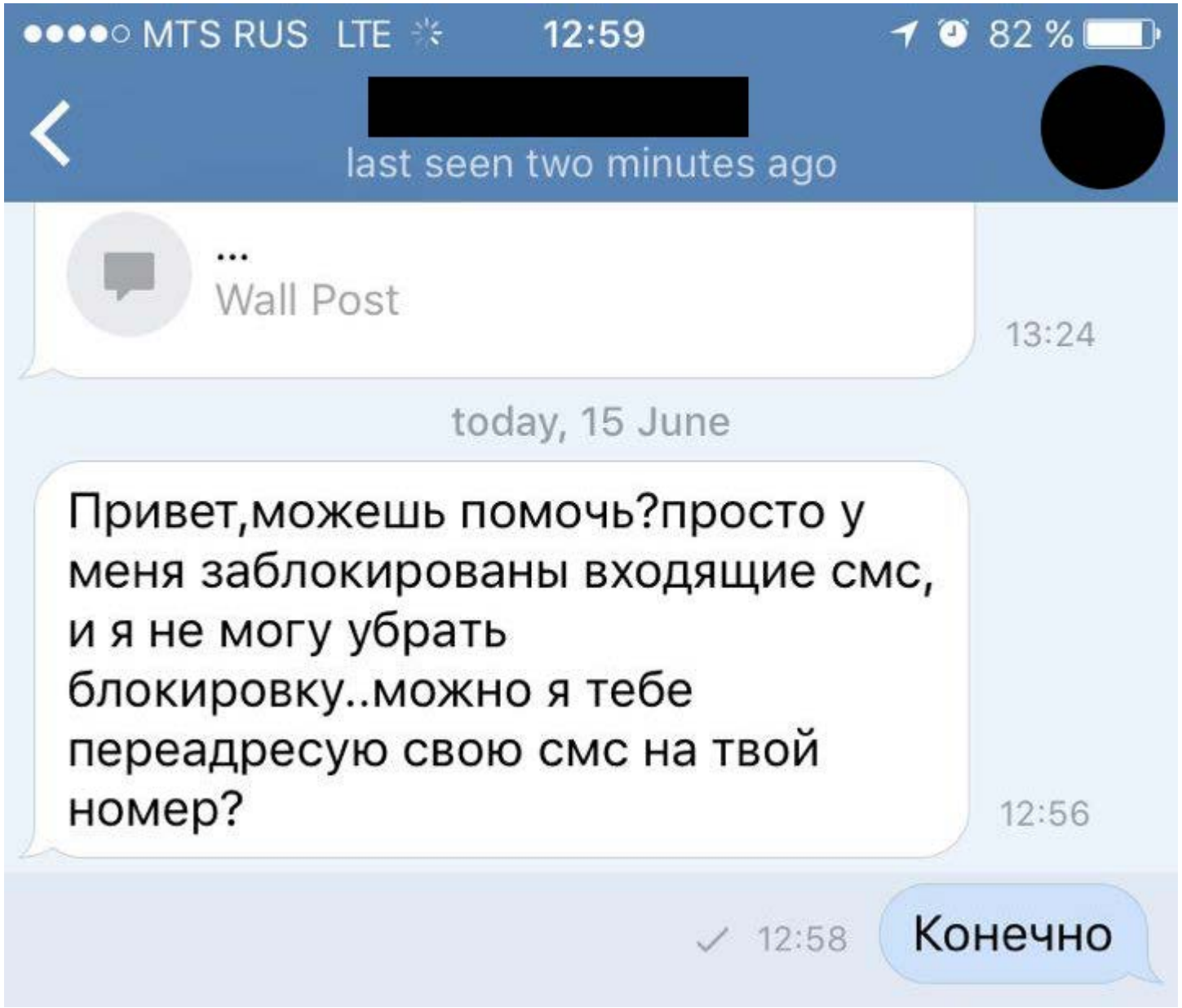
(2 билета) на человека AEROFLOT.COM

AIRGIFT.US

Личная

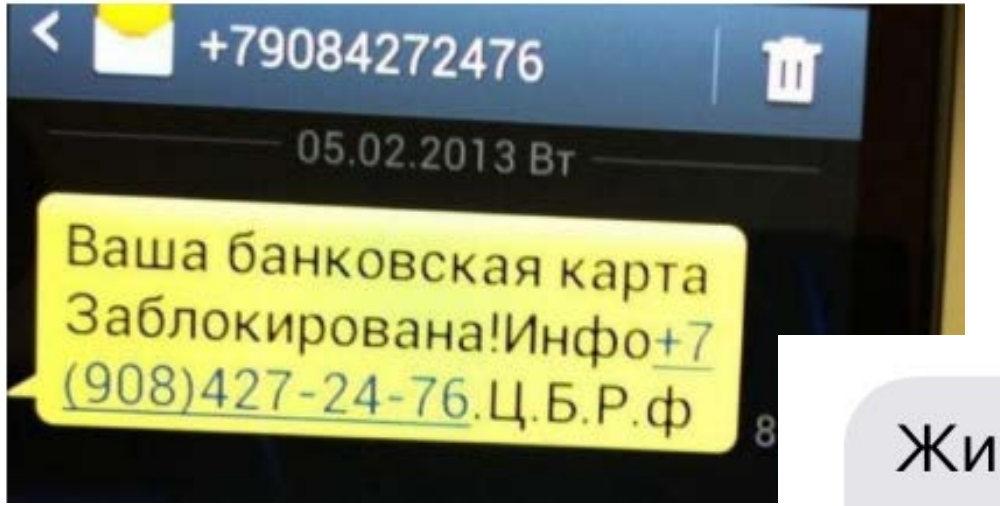
Жадность

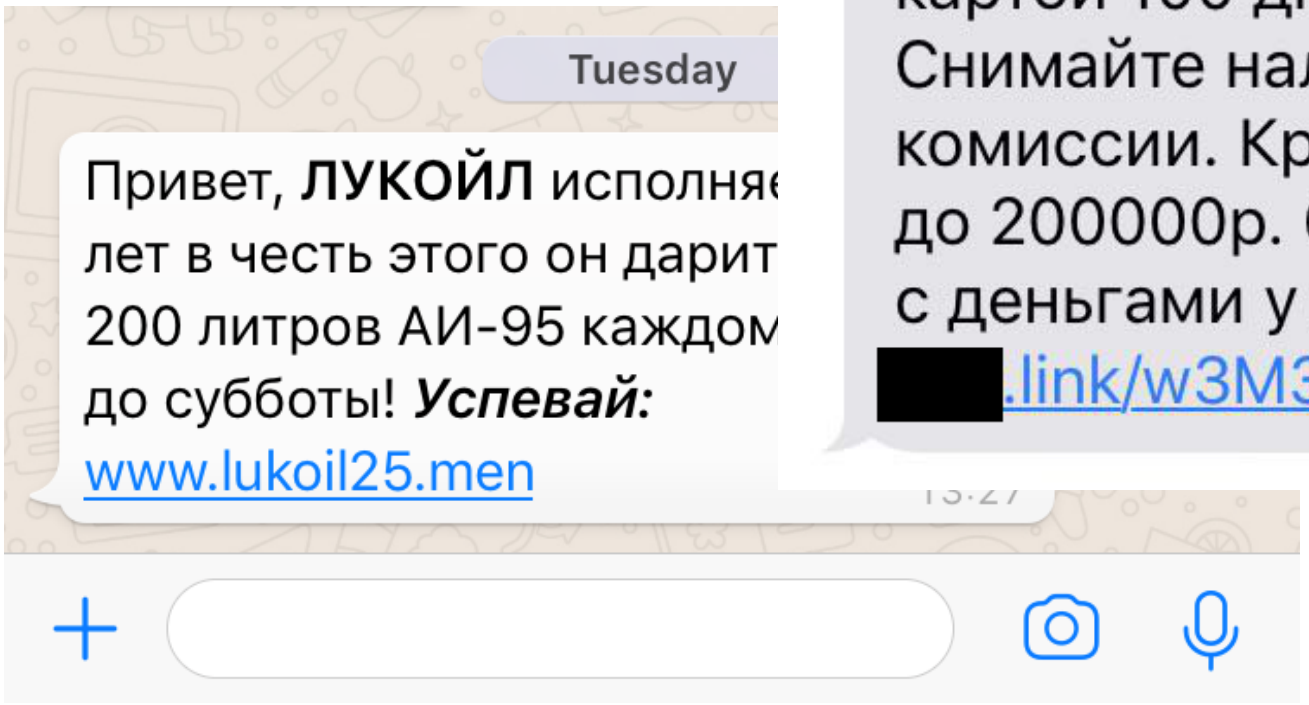
Любопытство



Личная

Желание помочь





Живите здесь и сейчас с картой 100 дней без %! Снимайте наличные без комиссии. Кредитный лимит до 200000р. 60 секунд и карта с деньгами у вас в смартфоне!
[redacted].link/w3M3

Личная

Страх

Жадность

Любопытство

Что делать? рекомендации ФинЦЕРТ

- Повышать киберграмотность населения … в рамках подпункта 2.12.3 Положения № 382-П
- Доводить до клиентов информацию о необходимости неукоснительного соблюдения рекомендаций
- Повышать качество работы операторов в области осведомления своих клиентов в вопросах киберграмотности.

Учитывайте в реализации

- Не воспринимается как реклама
- Не влияет негативно на ваш имидж
- Учитывает разные вектора атак на разные группы клиентов
- Показывает реальные и актуальные примеры

без бренда?

+ психологи

Не ведитесь на этот развод с фальшивым интернет-банком!

ИЗУМИТЕЛЬНЫЙ РАЗВОД РАСПРОСТРАНЕННОСТЬ: 💎💎 РИСК: 💰💰💰💰

Приглашаем протестировать новую версию мобильного приложения! Входящие ×

Bank Manager <test@bankname.com> 16:13 (27 мин. назад)
кому: я

В[redacted]к разрабатывает новую версию интернет-банка. Приглашаем действующих клиентов пройти тестовую регистрацию в системе.

Ждем вас в отделении банка по адресу: г. Москва, Мясницкая ул., д. 35.

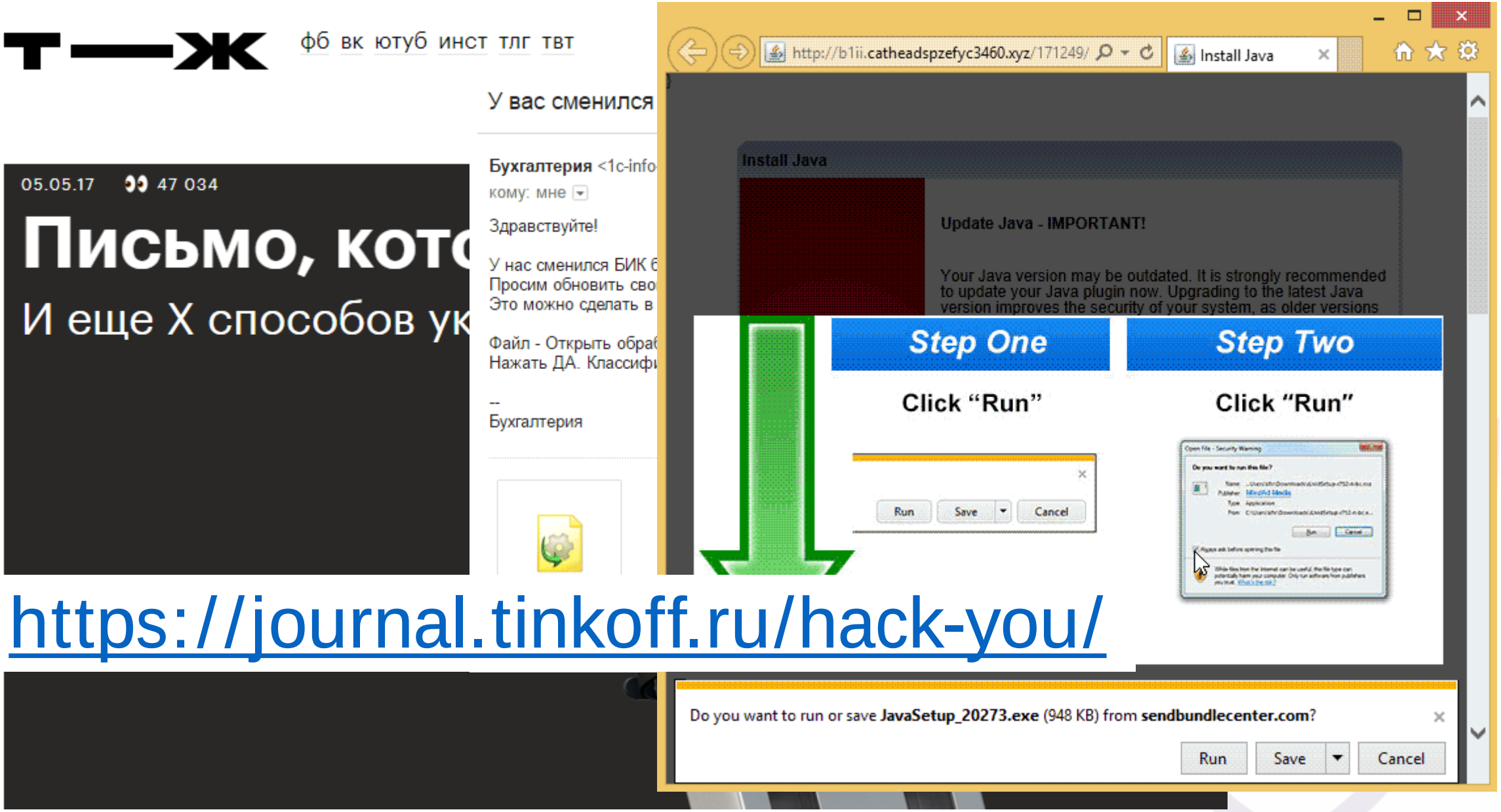
Для участия пришлите письмо с темой «Тестовая регистрация» на эл. адрес: Contact-Center-Bank@Ro.ru

В теме письма укажите:
1. Номер карты [redacted] Банка (16—18 цифр) или логин.
2. Код приглашения — 7842VTB9911 для участия в закрытом тестировании.

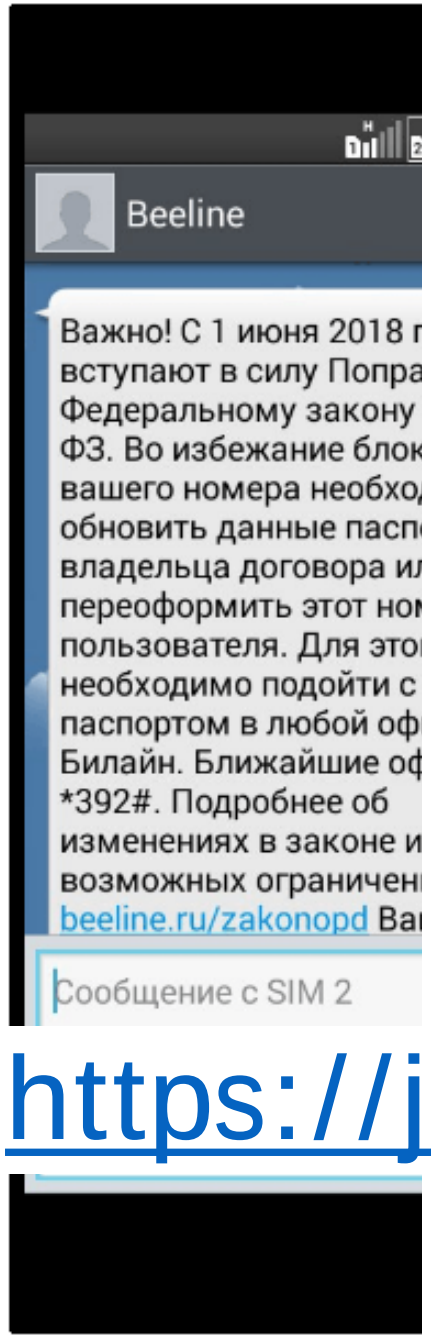
После регистрации на ваш мобильный будут отправлены реквизиты виртуальной банковской карты с балансом в 3000 ₽.

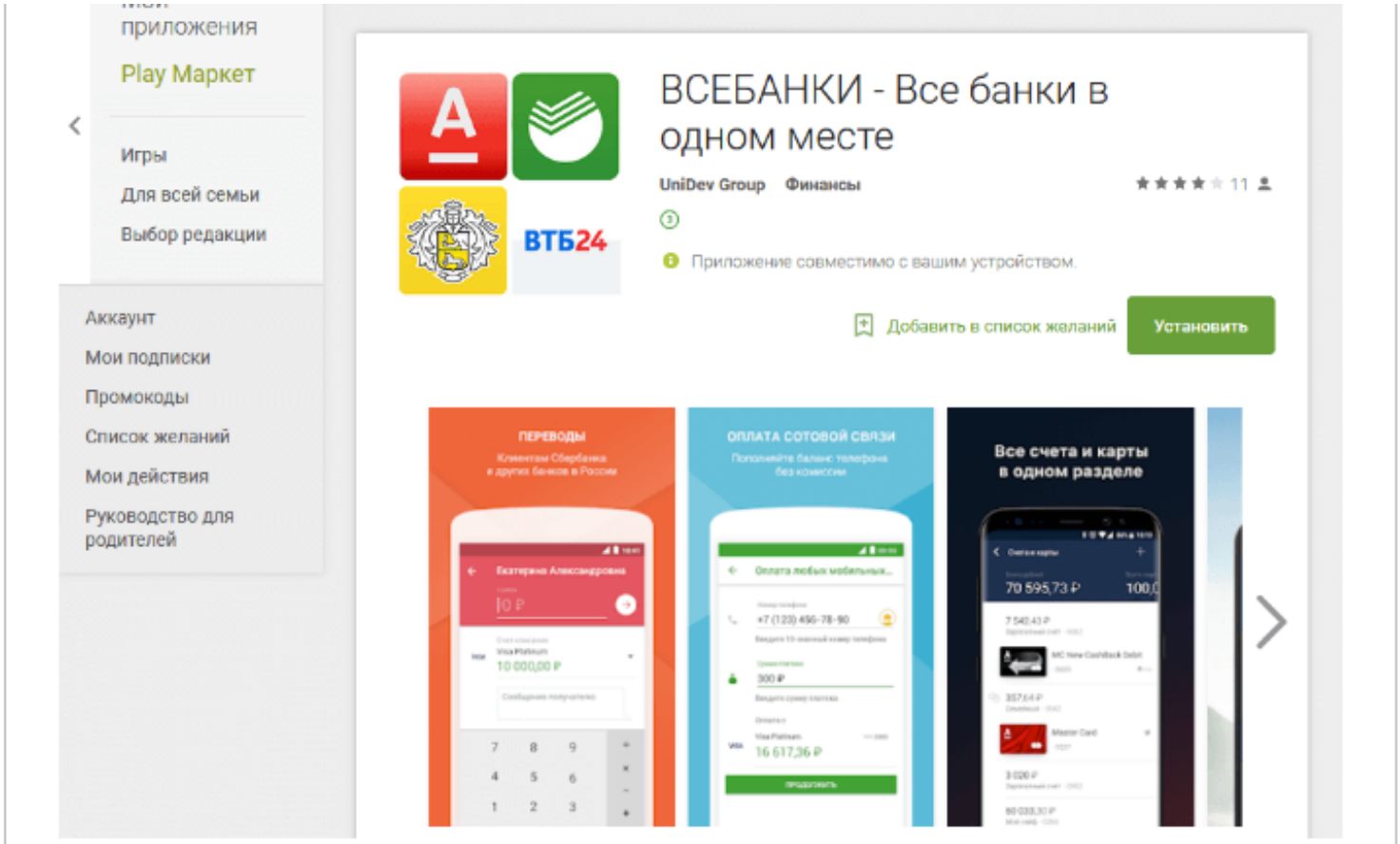
Количество вакантных мест ограничено — спешите зарегистрироваться!

https://journal.tinkoff.ru/hustle/



https://journal.tinkoff.ru/hack-you/





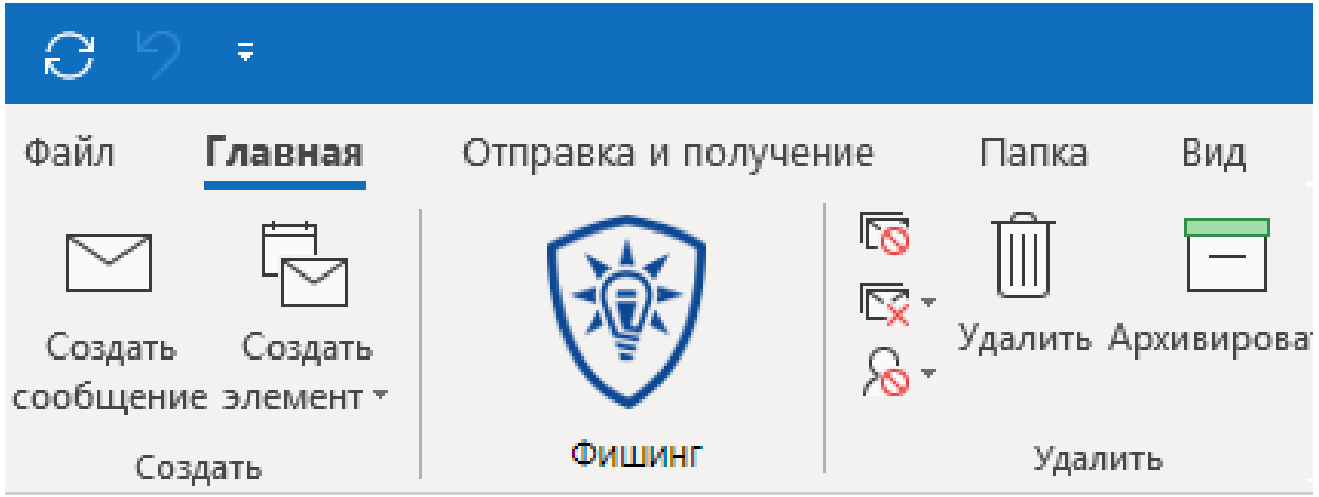
Вы хотите установить мобильный банк

ело держать несколько
бщим приложением для всех.
риант.

Установить | Не устанавливать

https://journal.tinkoff.ru/digest/

Собирайте обратную связь



👉 Знаете о похожих разводах? Знаете еще более лютый развод?

Расскажите нам!

Грамотные сотрудники и клиенты – лучшая защита.

Обучайте и тренируйте своих людей.

Антифишинг
www.antiphish.ru