

ДСОУА

Превращение Осведомленности
В Предотвращение



Чем Мы Занимаемся

Создаём безопасные фишинг-симуляции с
целью ознакомления с угрозами,
повышения осведомленности и
преобразования в активную защиту

Зачем Мы Этим Занимаемся

“Человеческая ошибка является причиной

95% *из всех инцидентов информационной-*

безопасности, исследованных в 2014-2016 годах. Наиболее распространенной формой является переход по вредоносной ссылке, найденной в фишинговом сообщении.”

“IBM Security Services 2016 Cyber Security Intelligence Index”

“91%

из всех кибератак начинаются с сообщения типа Фишинг”

TrendMicro 2016

↑17% по сравнению с 2014



Зачем Мы Этим Занимаемся



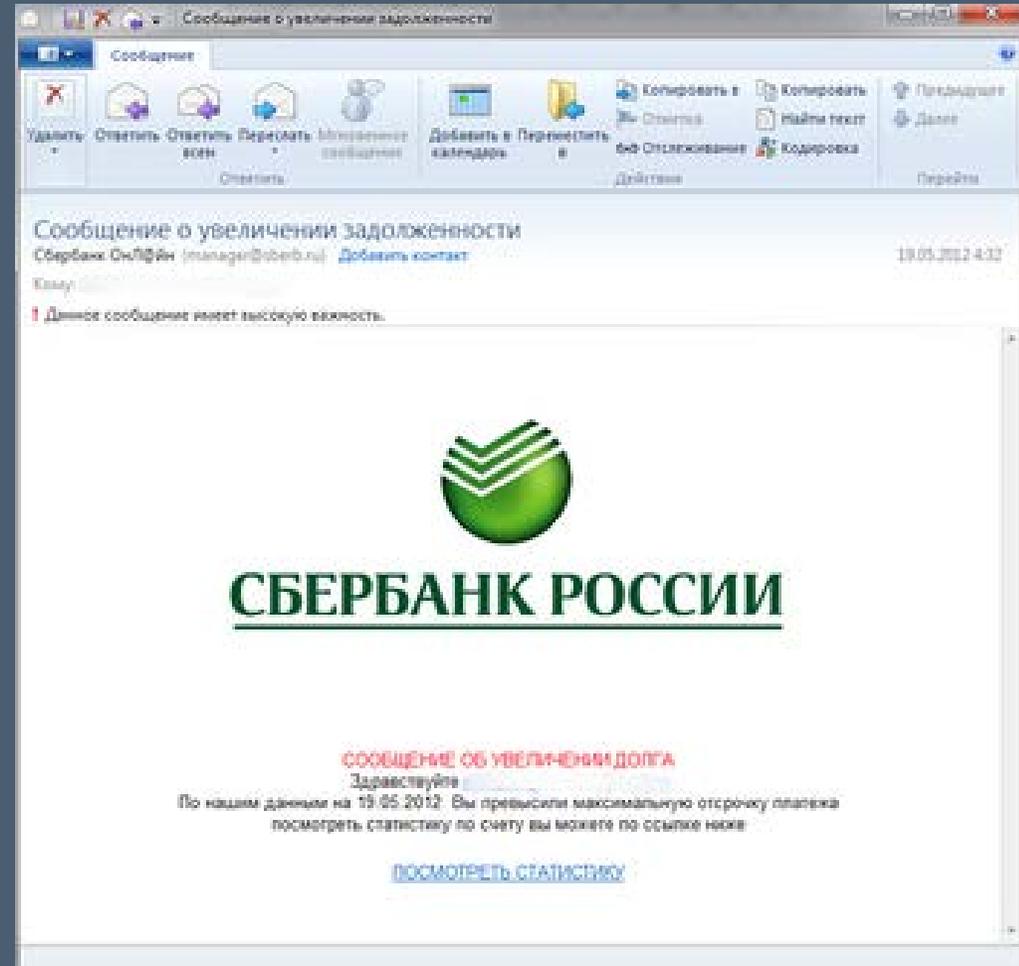
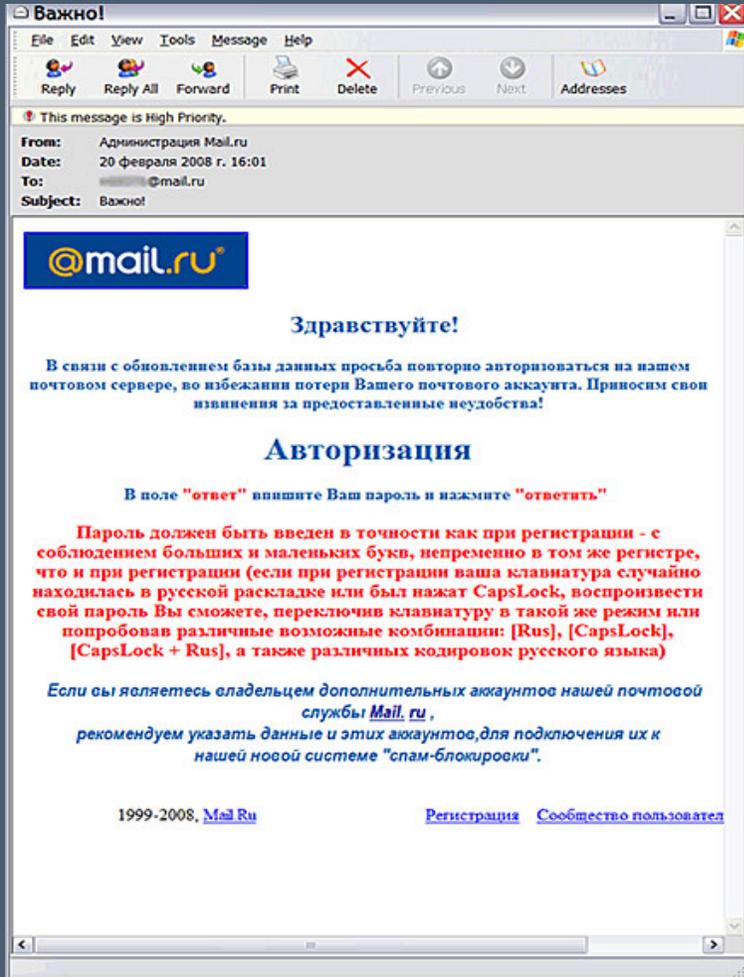
*“Каждая 5-я из 6-ти компании
были целью Фишинг Атак.”*

Symantec’s Internet Security Threat study 2016

Вымогательство Процветает



Примеры Фишинга



Анализ Ситуации

- Организации инвестируют в технологии, хотя любая технология проницаема
- Только 0%-1% от бюджета ИТ инвестировано в обучение работников
- Хакеры используют эту ситуацию и подбирают метод действия основанный на социальной инженерии для того чтобы проникнуть в организации

Предотвращение Начинается с Осведомленности



1. Осведомленность

Непрерывная образовательная программа, сосредоточенная на текущих угрозах.

2. Выявление

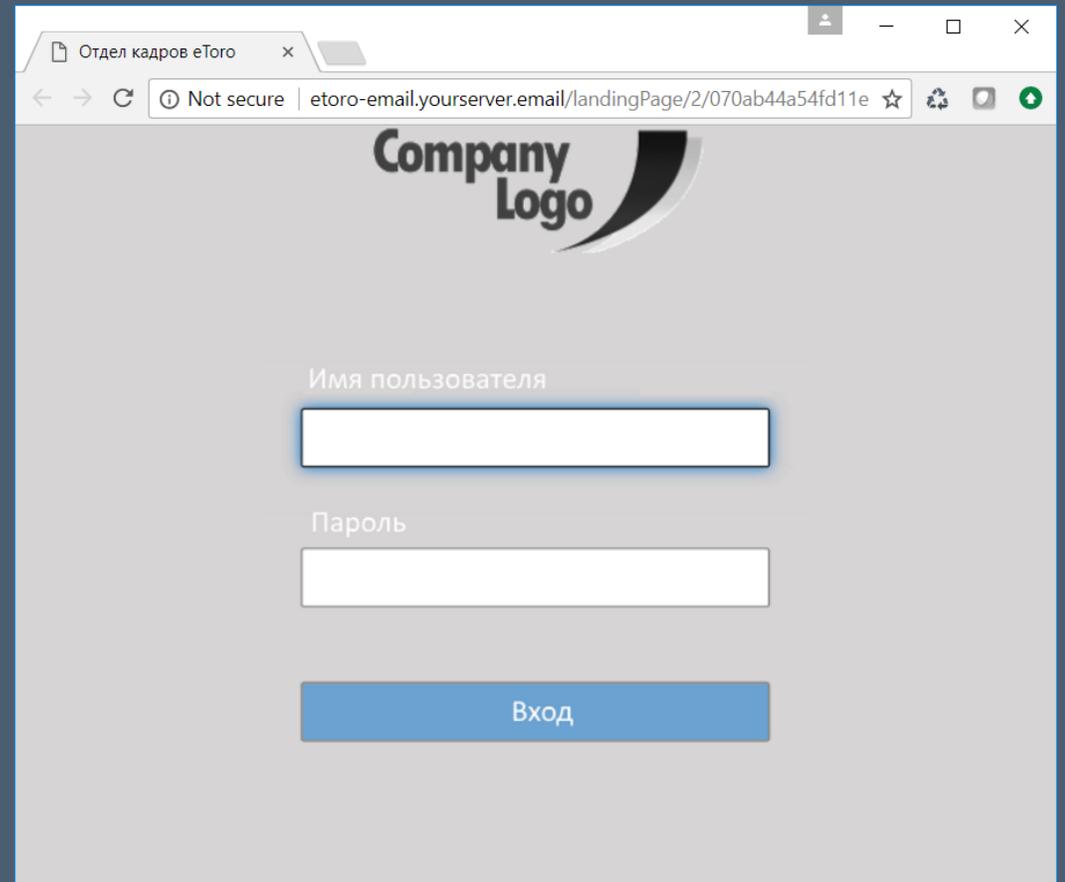
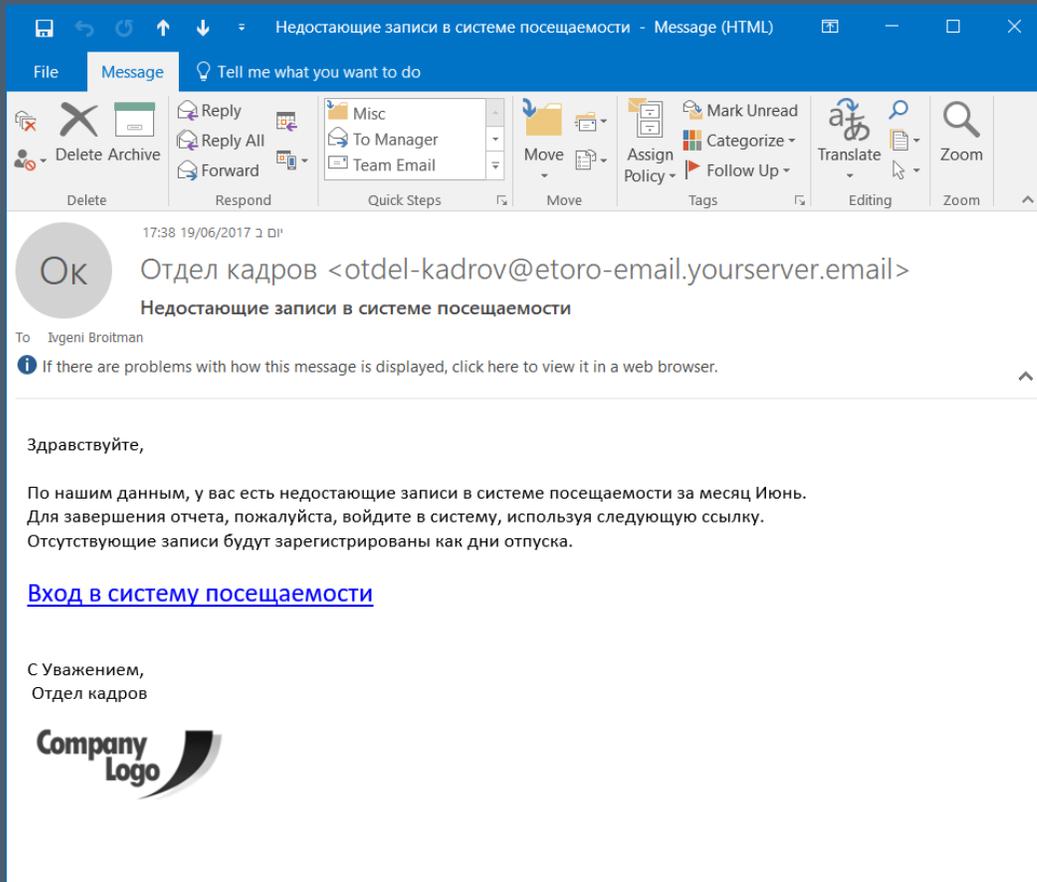
Максимальное взаимодействие сотрудников, которые получают возможность сообщать о подозрительных письмах в отдел безопасности.

3. Предотвращение

Предотвращение атак, быстро идентифицируя и изолируя подозрительные сообщения.

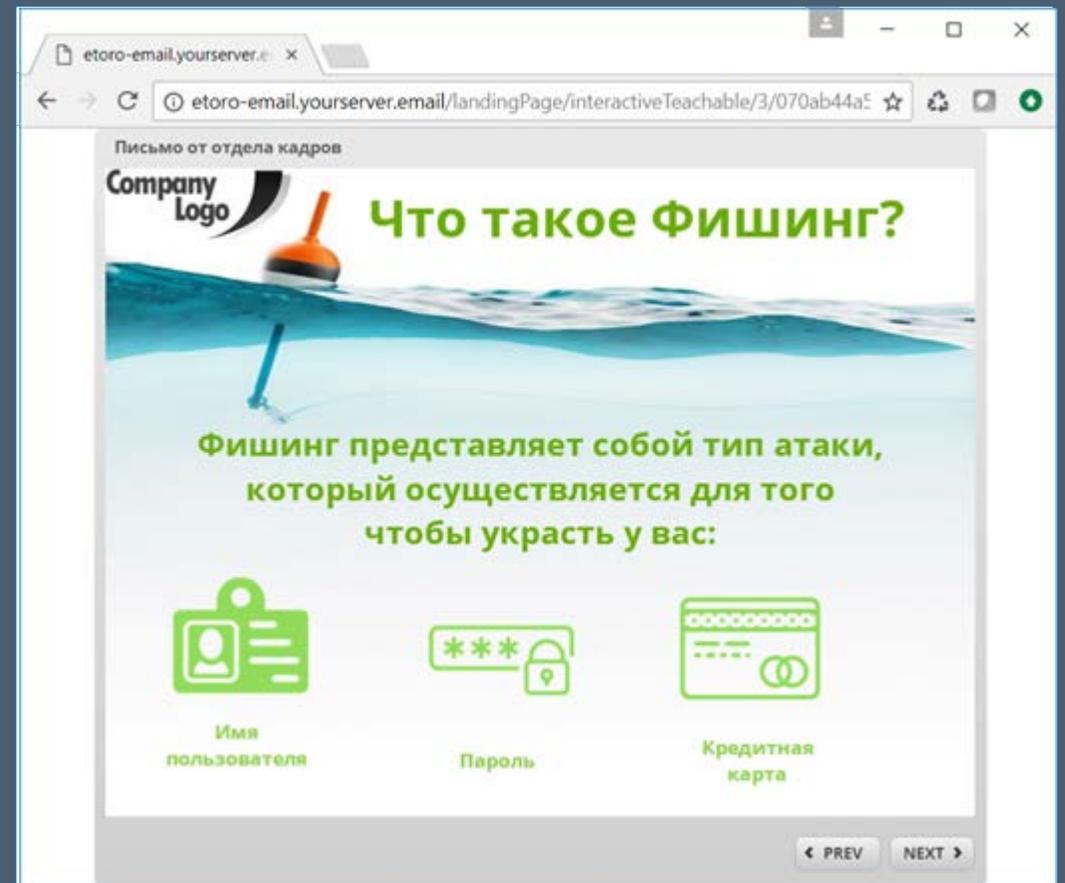
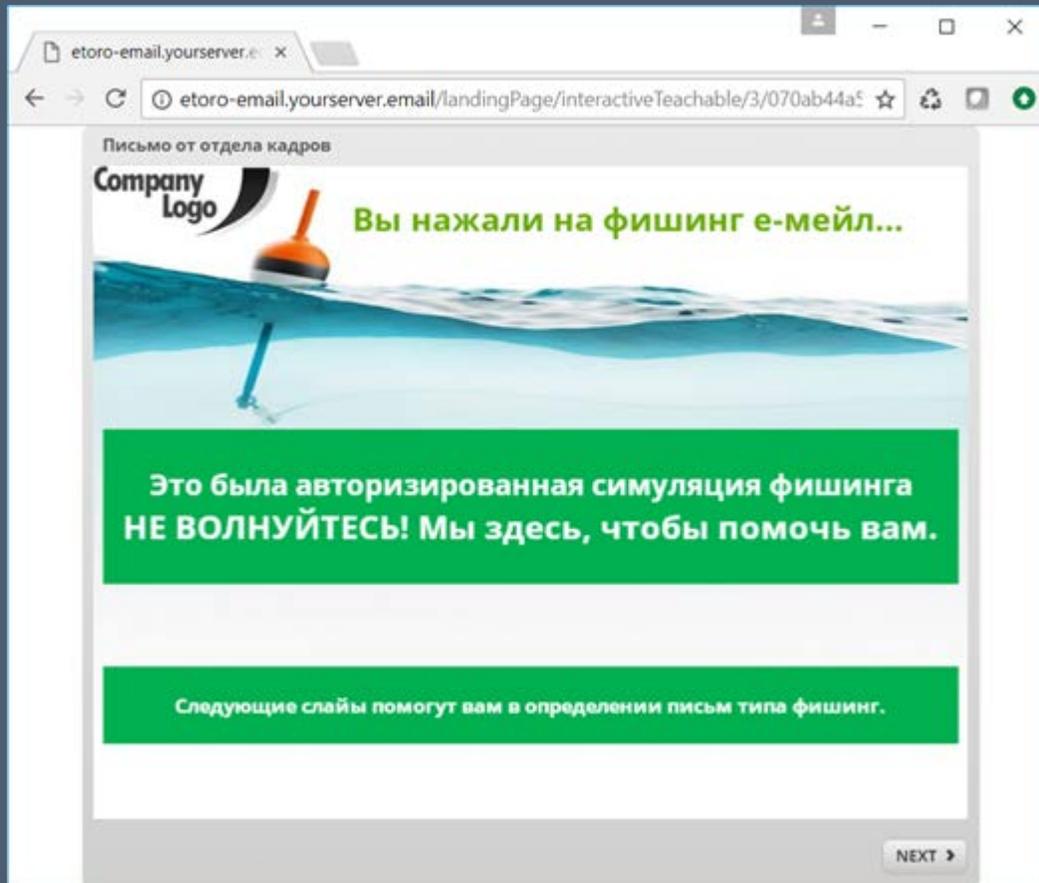
Примеры Симуляций

Письмо из Отдела Кадров



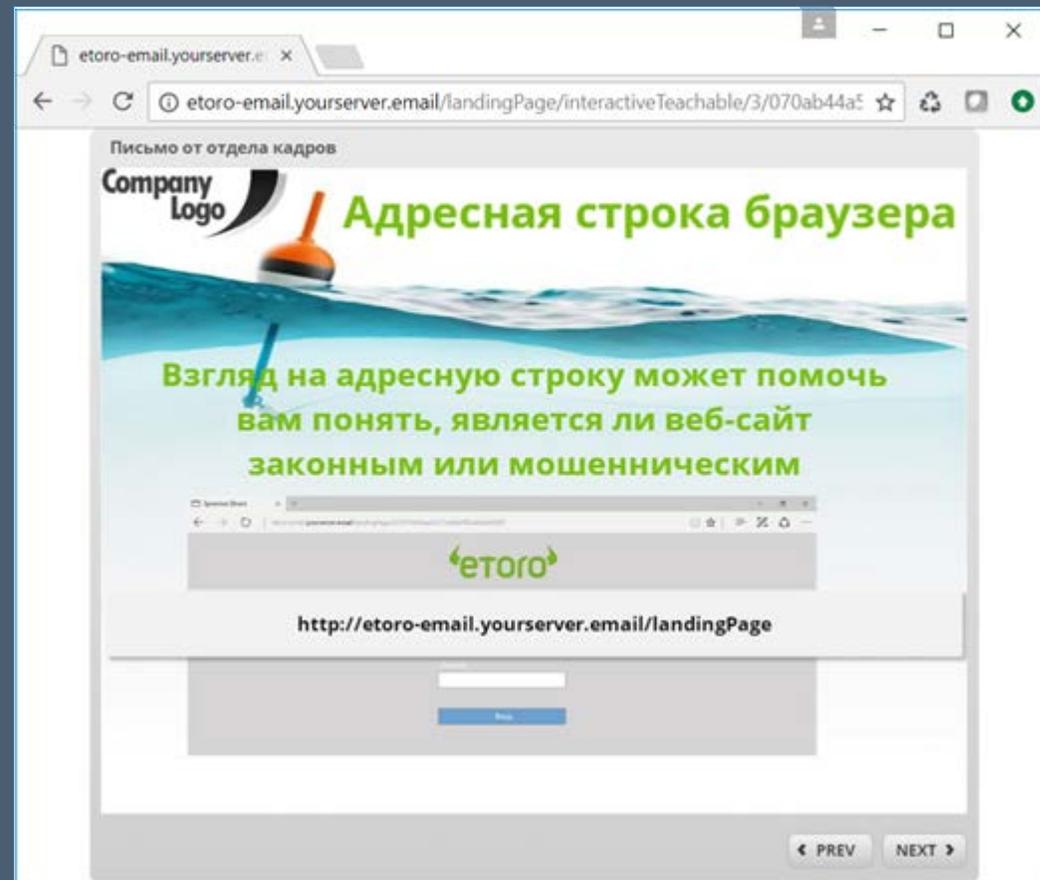
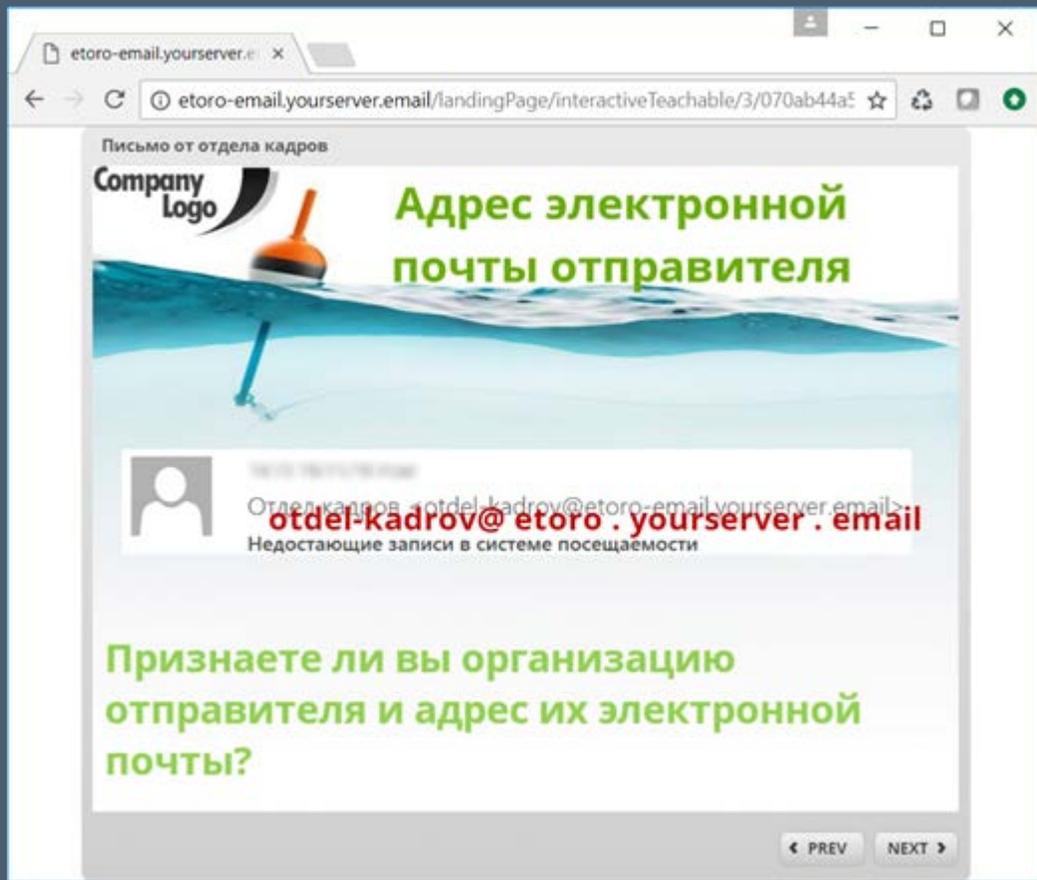
Примеры Симуляций

Письмо из Отдела Кадров



Примеры Симуляций

Письмо из Отдела Кадров



Примеры Симуляций

Квитанция от Фирмы Apple

Ваша квитанция от компании Apple - Message (HTML)

File Message Tell me what you want to do

Delete Archive Reply Reply Forward Forward All Team Email Move Move Assign Policy Categorize Follow Up Translate Zoom Zoom

20:04 19/06/2017 1 DP

A Apple <no_reply@apple.yourserver.email>
Ваша квитанция от компании Apple

To Ivgeni Broitman
Retention Policy Junk Email (30 days) Expires Never

APPLE ID lvgeni@dcova.com	Заказчик Visa ... XXXX Ivgeni Broitman	ВСЕГО \$599.99
ДАТА 20 Июня 2017		
НОМЕР ЗАКАЗА 2016-ZLTBNV	ДОКУМЕНТ № 568113251521	

Магазин приложений	ТИП	КУПЛЕНО У	ЦЕНА
Магазин приложений #1 - Подписка - один год Сообщить о проблеме	Покупка в приложениях	Ivgeni's iPhone	\$599.99

[Посмотреть Квитанцию](#)

ВСЕГО	\$599.99
-------	-----------------

Управлять Apple ID

Not secure | apple.yourserver.email/landingPage/2/60bf78fe551111e796ef02afb0dd936f

Mac iPad iPhone

Apple ID

Apple ID

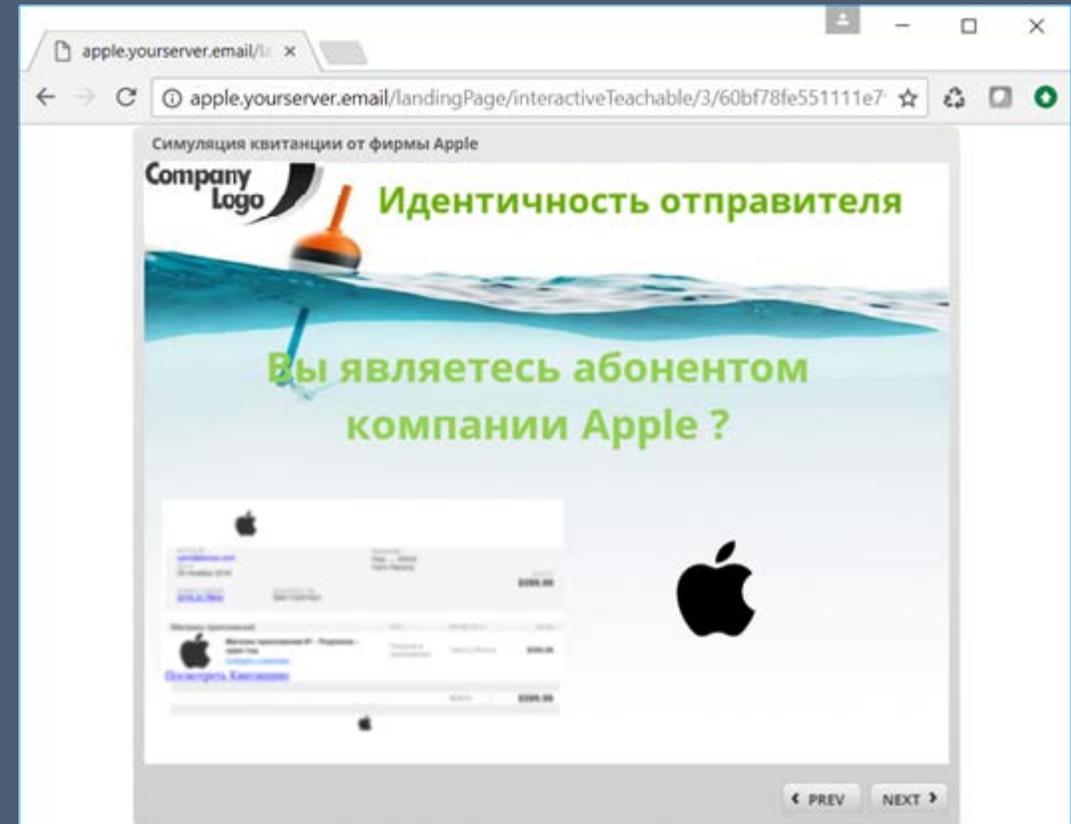
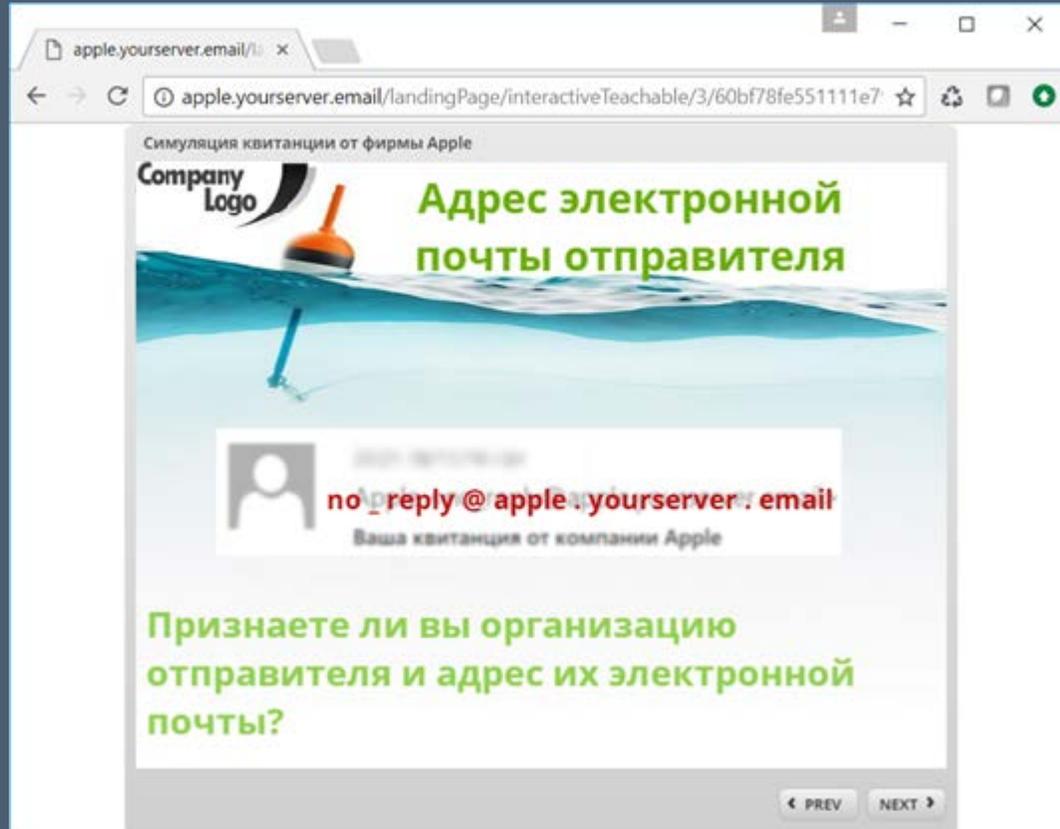
Управление учетной записью Apple

Apple ID

Password

Примеры Симуляций

Квитанция от Фирмы Apple



Разновидность Симуляций

Типы Рассылки

Массовый

Одиночный

Уэйлинг



Категории Симуляций

Ссылка

Сбор
Информаций

Вложения

СМС
Сообщение

Учебный Материал

Интерактивные
Тренировки

Видео
Ролики

Текстовые
Страницы

What is Phishing Attack ?

Phishing is a tool, used by malicious parties to facilitate cyber attacks through innocent looking emails, in order to reveal the following information about you and your organization:

- Credit card numbers
- Personally Identifiable Information
- Credentials
- Even most sensitive organizational data

Let's Continue

First, think - does the email look too tempting?

You have participated in a phishing simulation

Don't worry, this is an authorized simulation by Dcoya and your company. It was sent to you to help you learn how to avoid real phishing attacks. Please don't share your experience with colleagues, so they can learn too.

Next time, please note the following:

Пакет Услуг

Специально Подобранные Симуляции на Любом Языке

Годовая Программа Обучения

Неограниченный Симулятор

Функциональная Веб-Панель Управления

Информационные Отчеты и Рекомендации

Полное Управляемое Обслуживание

Dcoya Advantive

Вспомогательный Модуль Для Почтовой Программы

1

Позволяет сотрудникам немедленно сообщать о подозрительных письмах в отдел безопасности

2

Преобразует сотрудников в "датчиков" обнаружения фишинга

3

Даёт возможность сотрудникам чувствовать себя влиятельными и быть частью процесса

Развертывание Системы

1

Общественное Облако

2

Частное Облако

3

Клиентский Сервер

Часть наших Клиентов

Правительственные Учреждения



The Knesset



Ministry of Finance

Международные Фирмы



Здравоохранение



Финансовые Учреждения



THE ROTHSCHILD FOUNDATION



Муниципалитеты



ДКОУА

Спасибо за Внимание
