



MessageLabs®

Be certain

# Messaging threats

Warren Sealey – Technical Consultant

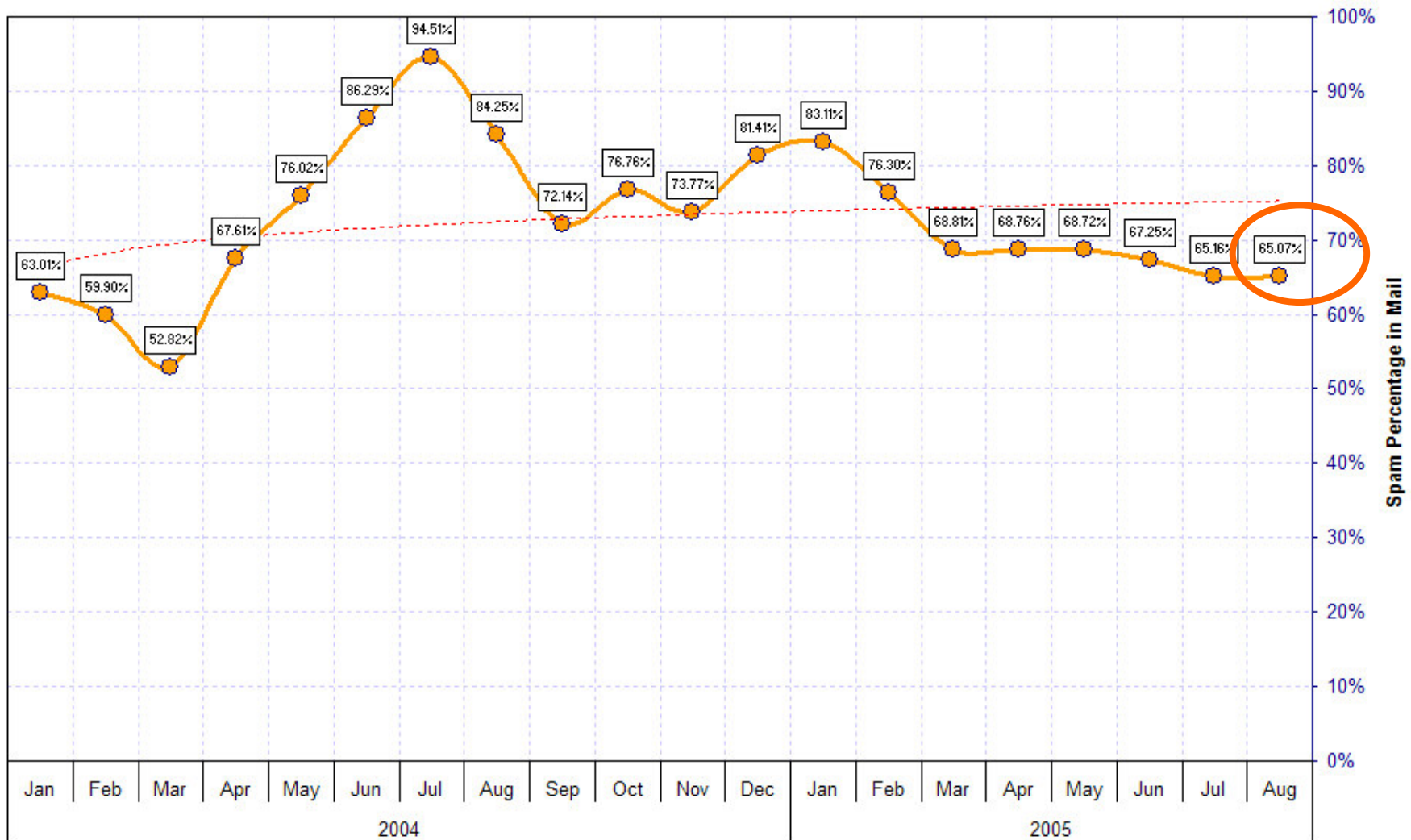
28 October, 2005

# Agenda



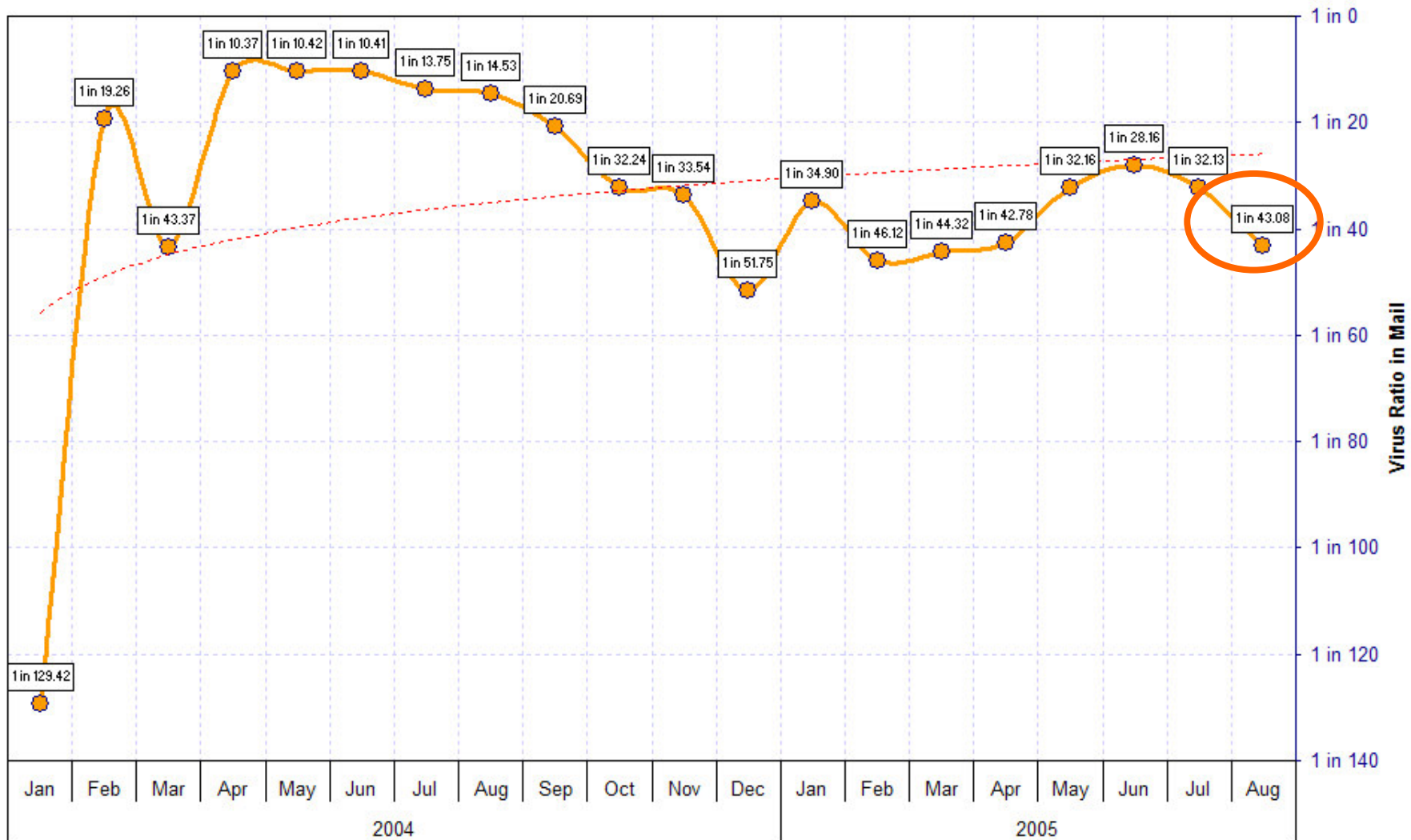
- The traditional threats
- The emerging threats
- Internet Level solutions

# State of play: *Email Spam Trends*

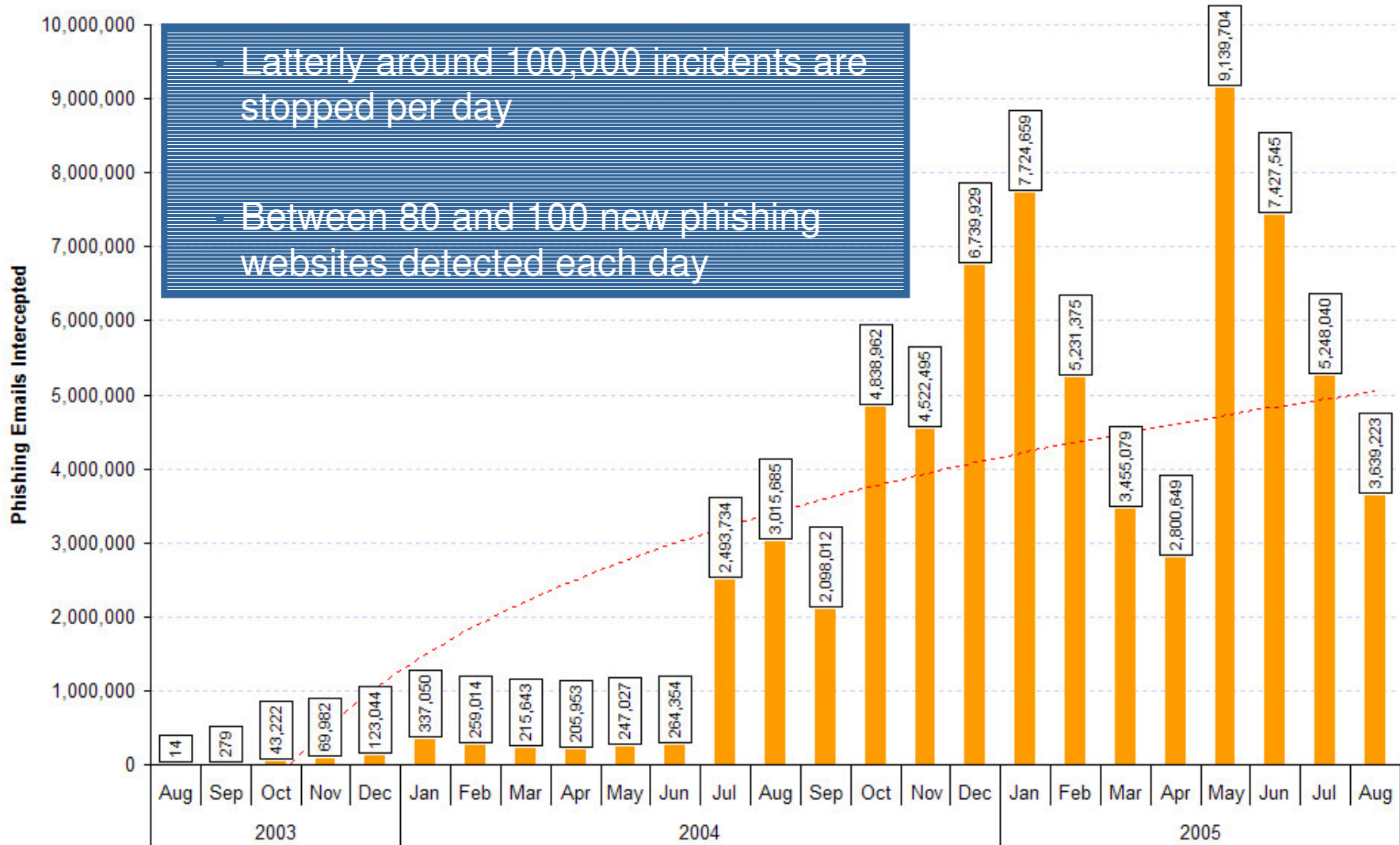


# State of play:

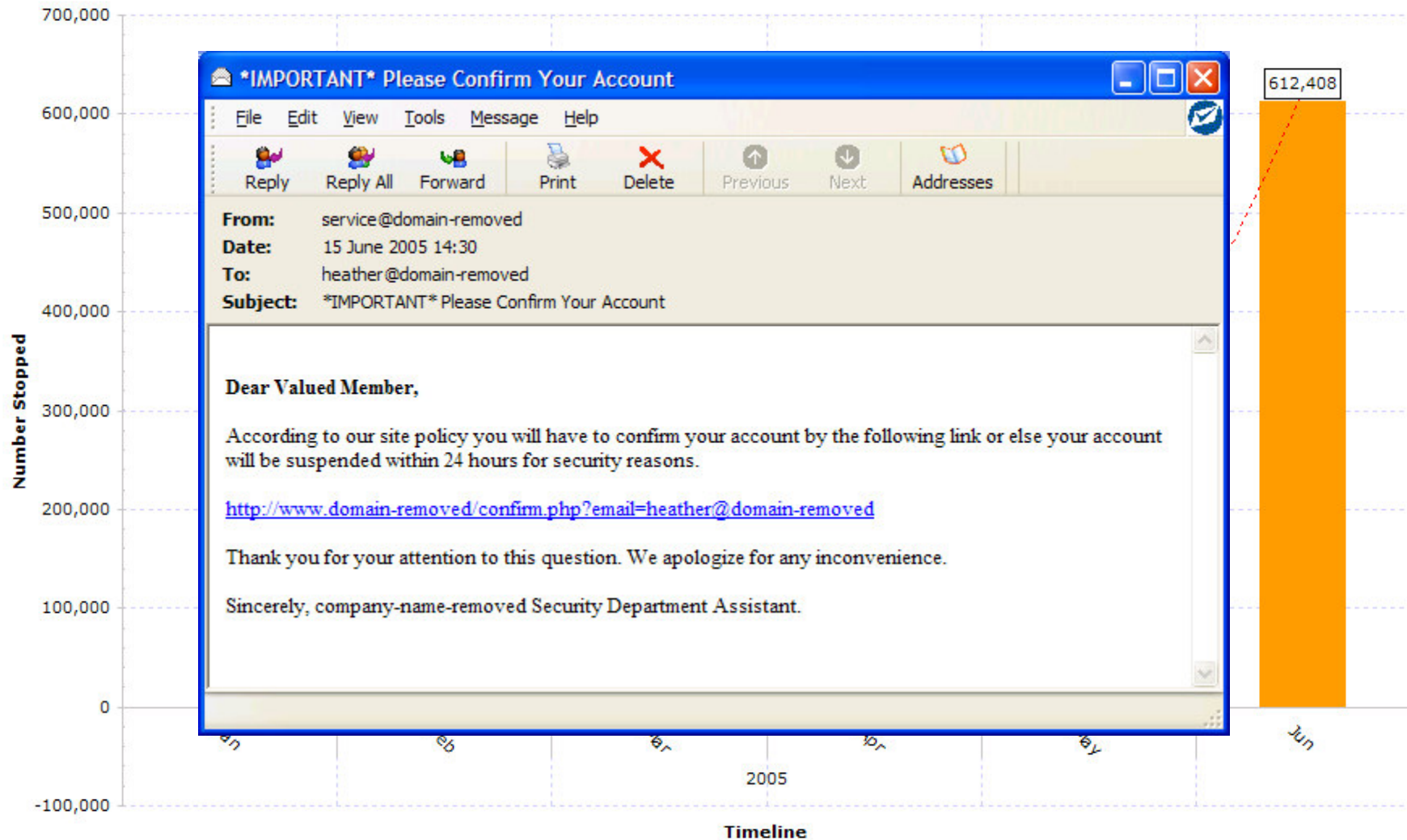
## *Email-borne Virus Patterns*



# Emerging threats: *Phishing and Identity Theft*



# Emerging threats: *Phishing and Identity Theft*



# Spam and Phishing Already

## SPF Compliant

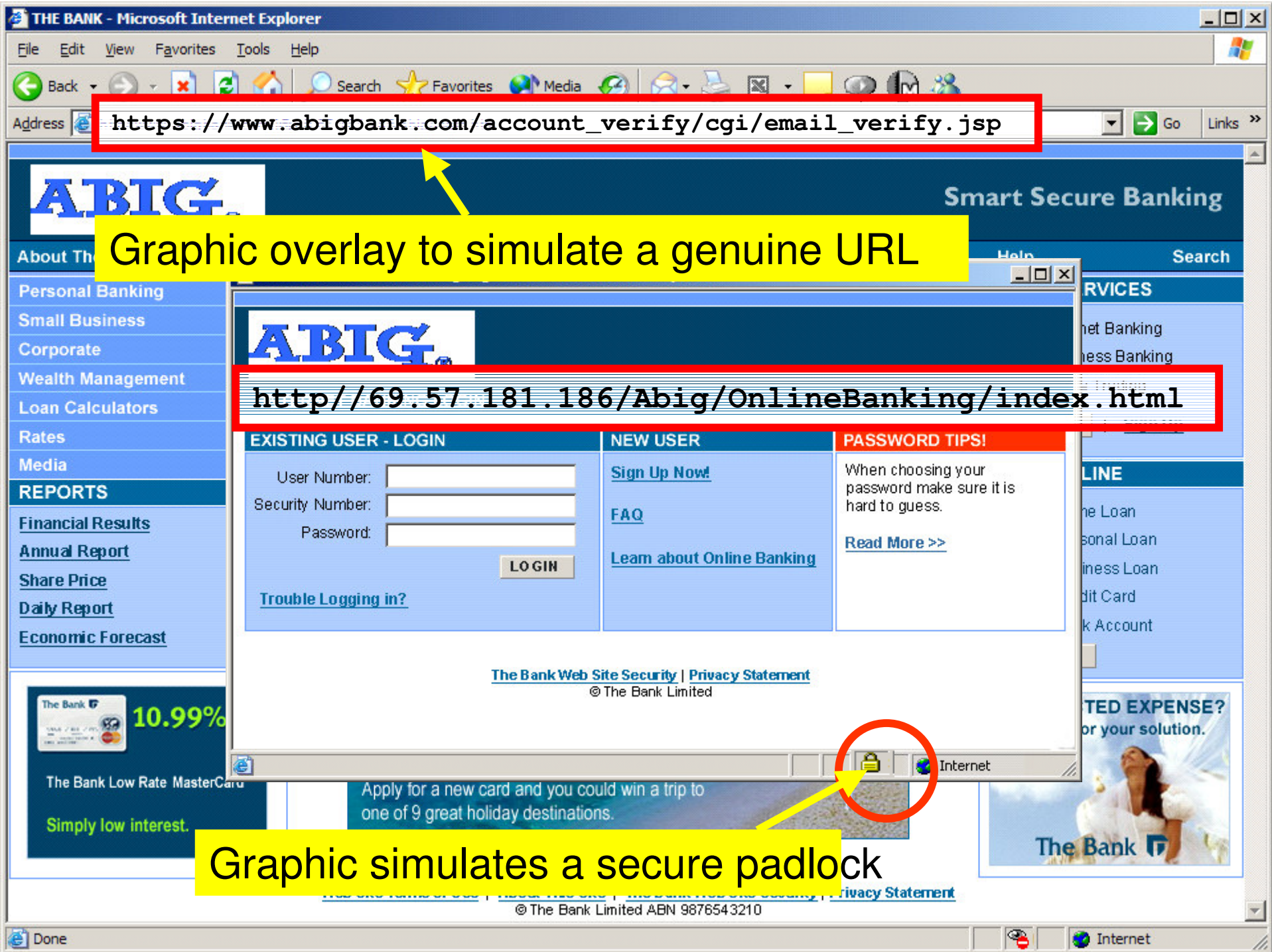


Return-Path: <support@**a-bigbank.com**>  
Received: from aamta01-winn.mailhost.ntl.com ([212.250.162.8])  
by #domain removed with SMTP  
id <20041223032143.GYUR15581.#domain removed#aamta01-winn.mailhost.ntl.com>;  
Thu, 23 Dec 2004 03:21:43 +0000  
Received: from adsl-84-226-53-22.adslplus.ch ([84.226.53.22])  
by aamta01-winn.mailhost.ntl.com with SMTP  
id <20041223032142.SLMI15415.aamta01-winn.mailhost.ntl.com@adsl-84-226-53-22.adslplus.ch>;  
Thu, 23 Dec 2004 03:21:42 +0000  
X-Message-Info: GMDGE+lq0+ve+EQP+12/762120335026282  
Received: (qmail 59631 invoked by uid 009); Thu, 23 Dec 2004 05:18:37 +0200  
Date: Wed, 22 Dec 2004 22:20:37 -0500  
Received: from congratulate.support@abigbank.com ([75.138.240.200]) by po0-vvs95.support@abigbank.com with Microsoft SMTPSVC(5.0.5.2600.5512); Thu, 22 Dec 2004 21:19:37 -0600  
Received: from purchase.support@abigbank.com ([4.175.0.24]) by antiperspirant.support@abigbank.com with MailEnable ESMT; Thu, 22 Dec 2004 06:20:37 +0300  
Message-Id: <2798367853.52202@support@abigbank.com>  
From: Abig Bank <support@abigbank.com>  
To: Herman G. Wilberforce <pwood@messagelabs.com>  
Subject: Important Online Abig Banking Alert  
MIME-Version: 1.0 (produced by bronchitisbuild 7.5)  
Content-Type: multipart/alternative;  
boundary="--98132360999210355"

**a-bigbank.com. IN TXT "v=spf1 ip4:84.226.53.0/24 ptr ~all"**

Content-Transfer-Encoding: quoted-printable  
Content-Description: harrison trouble credible  
<html>... ..

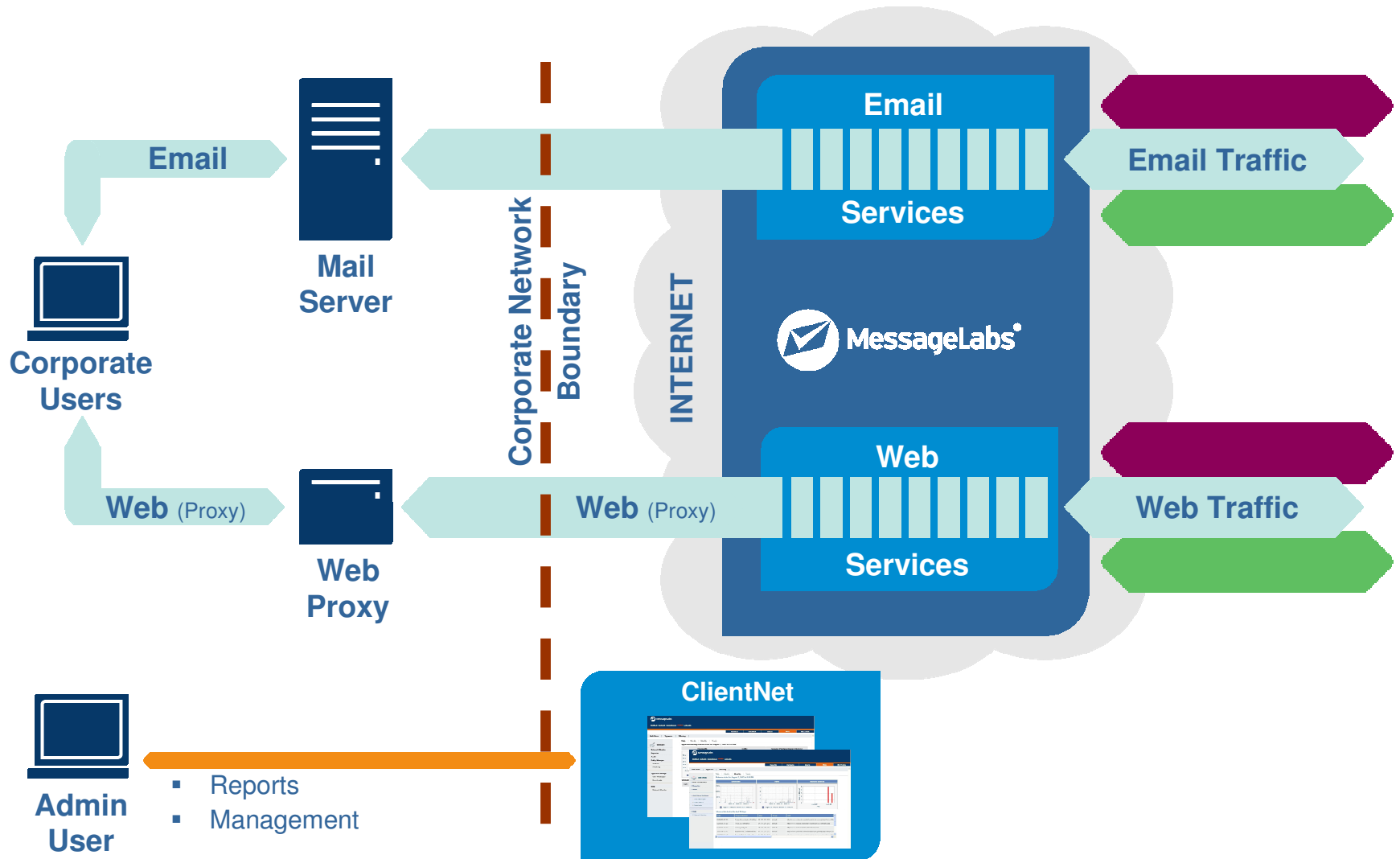
- “a-bigbank.com” does not belong to Abig plc.
  - Abig plc’s online banking domain should be “abigbank.com”
  - Abig *did not* register this doppelganger domain as a precaution
- Valid SPF record published
  - Will pass any SPF check as a valid record, otherwise “soft-fail”
- Sent via Open-Proxy
  - DSL account, a running backdoor trojan horse program



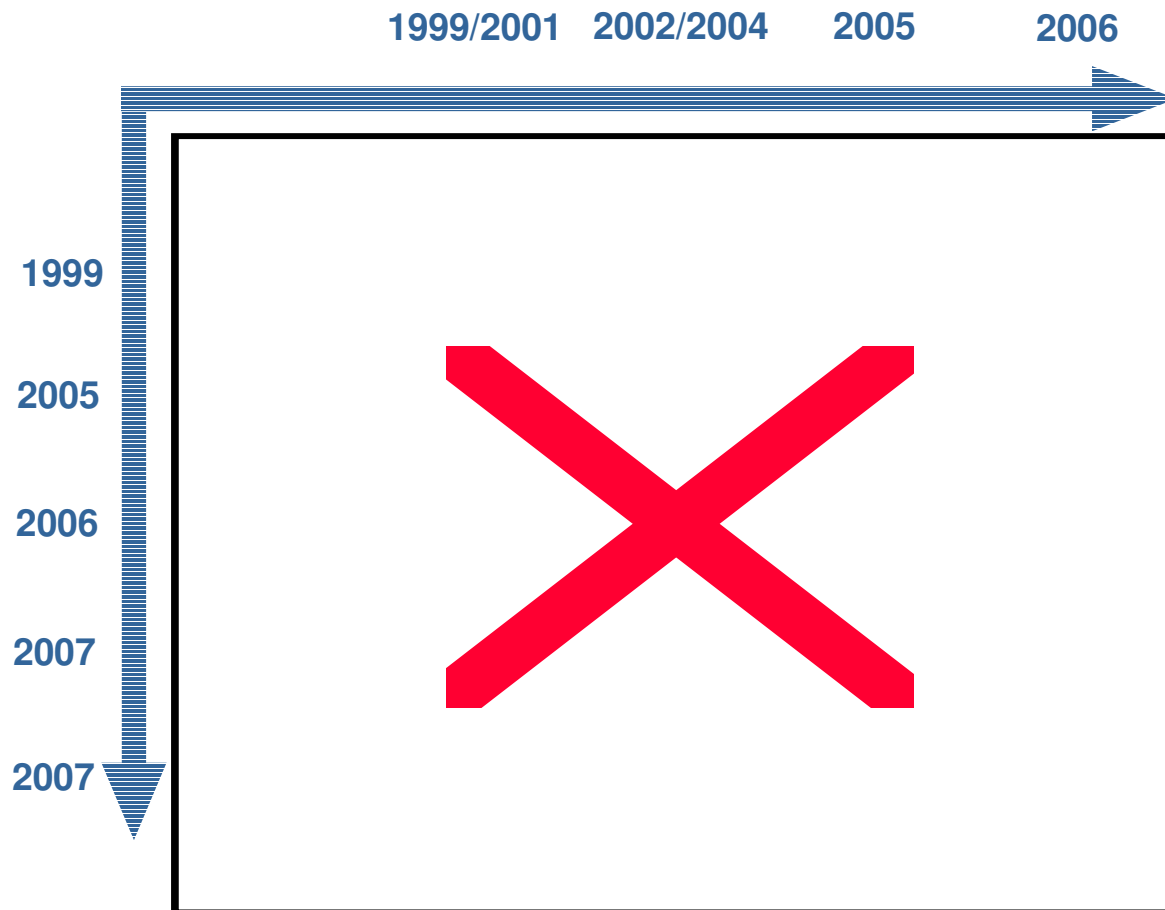
- TCO
- “virtual team” of security specialists
- Global view of threats
- Stay abreast of latest technology
- Reliability and redundancy
- Break the technology refresh cycle

# Web Scanning Services:

*Anti-virus and spyware screening*



# Beyond Email to New Forms of Messaging



- Services aligned with business drivers
- New email services
  - Deeper functionality
  - Market-driven feature sets
  - Focus on policy
- New areas of messaging:
  - HTTP
  - IM
  - Mobile
  - Voice (VoIP)



MessageLabs®

Be certain

# Questions?

Warren Sealey – Technical Consultant

28 October, 2005