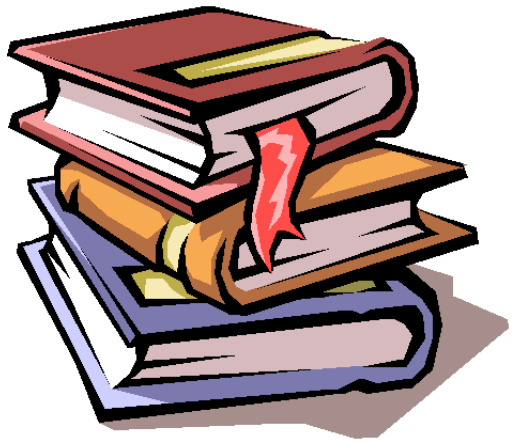
Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

Secure Email and Web Browsing

Sébastien Dellabella – Computer Security Team

Overview

- Main attack types
- Consequences of a successful attack
- Survival guide on the wild Internet
- Understanding the details
- Examples



Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

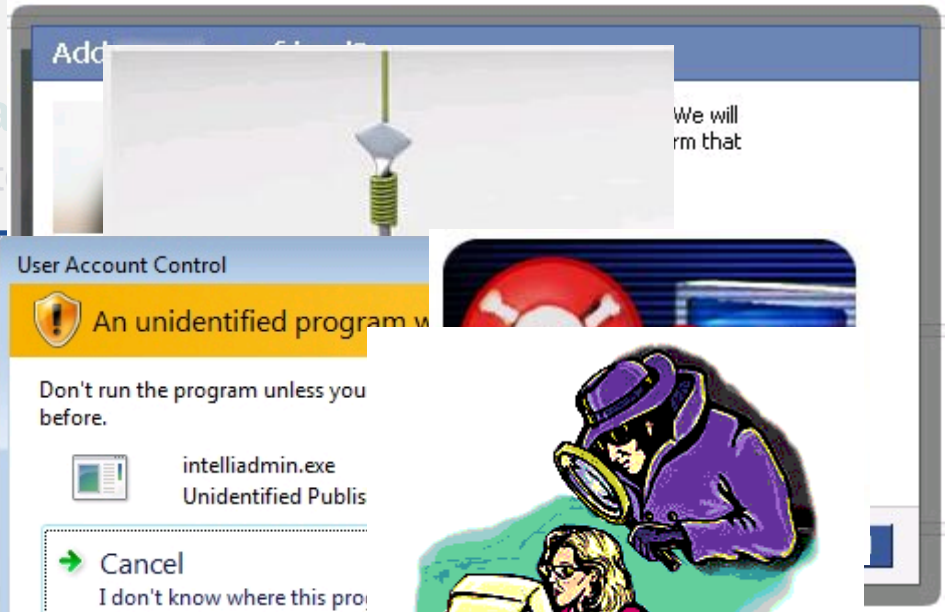
Main attacks types

Main attacks types

- **Social Engineering**
  - Someone calls you and asks you for personal information
  - Someone lost an USB Stick and you found it.
- **Password Phishing**
  - Forged mail
  - Tabnabbing NEW!

Understanding the attack makes it ineffective

User interaction needed



Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

Consequences of Attacks

Consequences of Attacks

- **Computer remotely controlled to:**
  - Send SPAM
  - Infect other machines on the local network
  - Host illegal or copyrighted data (software, movies, porn, banking data, private data)
  - Relay illegal connections

- **Computer used for criminal purpose:**
  - Loss of confidential work
  - Money extortion (private data encryption)
  - Join BotNet to attack other systems on the Internet (DoS)

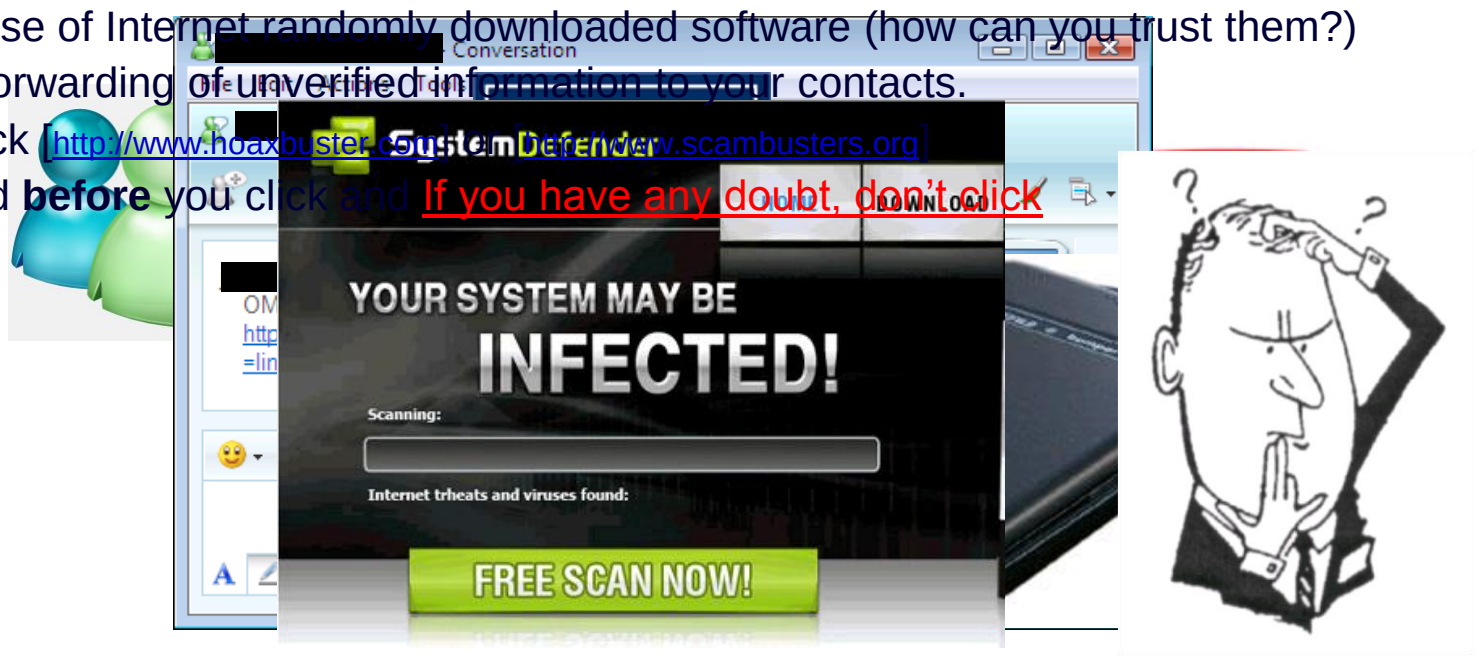
Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

Survival Guide

Survival Guide (1/2)

User awareness

- **No** credentials (login/password) over email
- **No** same password for different place/software/service (CERN email, MSN, private email account, banking, Facebook, etc.)
- **No** clicking on links sent by your online contacts before confirmation (mail, phone call, etc.)
- **No** use of untrusted media (USB stick you found in the street, CD, DVD or hard-drive your friend gave to you)
- **No** use of Internet randomly downloaded software (how can you trust them?)
- **No** forwarding of unverified information to your contacts.
  Check [http://www.hoaxbuster.com] [http://www.scambusters.org]
- Read **before** you click and If you have any doubt, don’t click



Survival Guide (2/2)

- **Work without “Administrator” rights**
  - Standard on Windows VISTA, Windows 7, MAC, Linux
  - Use “NICE Admin” on Windows XP
- **Up-to-date OS and software**
  - Average survival time of a machine on the Internet is: 4min
    [http://www.dshield.org/survivaltime.html]
  - CMF updates at CERN
  - Windows Update at home
- **Antivirus with latest pattern files**
  - Install CERN Antivirus at home, it’s **FREE for CERN users !**
    [https://cern.ch/win/Help/?kbid=051092]

Understanding the details

- **Why you can’t trust messages you receive**
  - By E-mail
  - By Instant Messenger (MSN, Skype, ICQ, etc.)
  - By contacts on social networking website (Facebook, etc.)

- **What is the U**
  - URL (Uniform
  - What you see

e link below

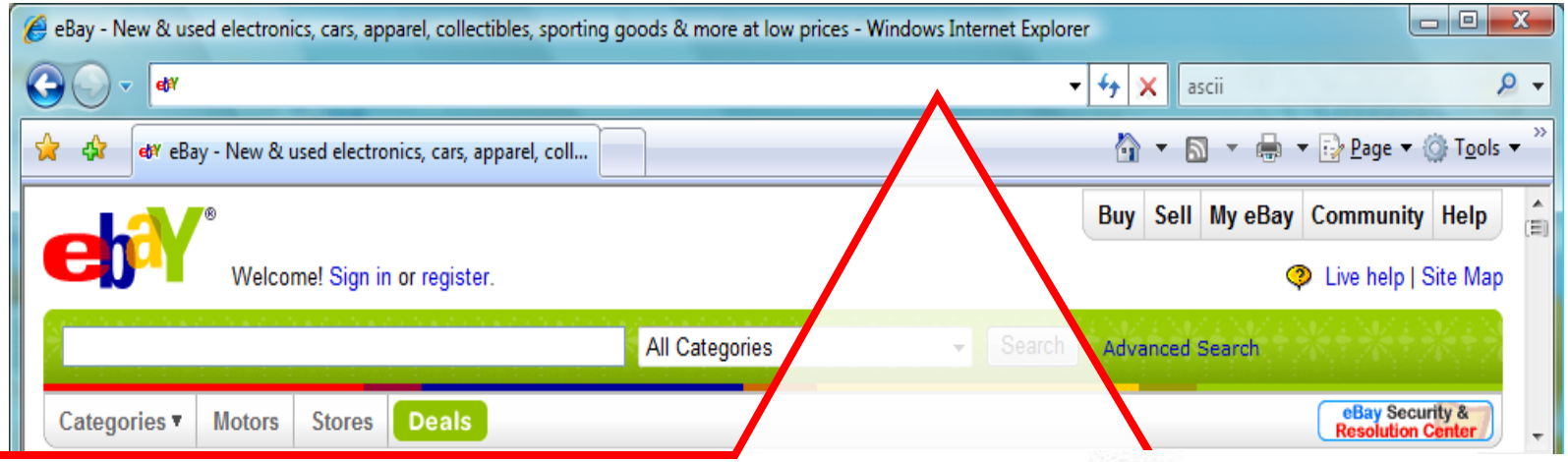
Dispute Transaction

Thank you for using PayPal!
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

PayPal Email ID PP120

Understanding the details

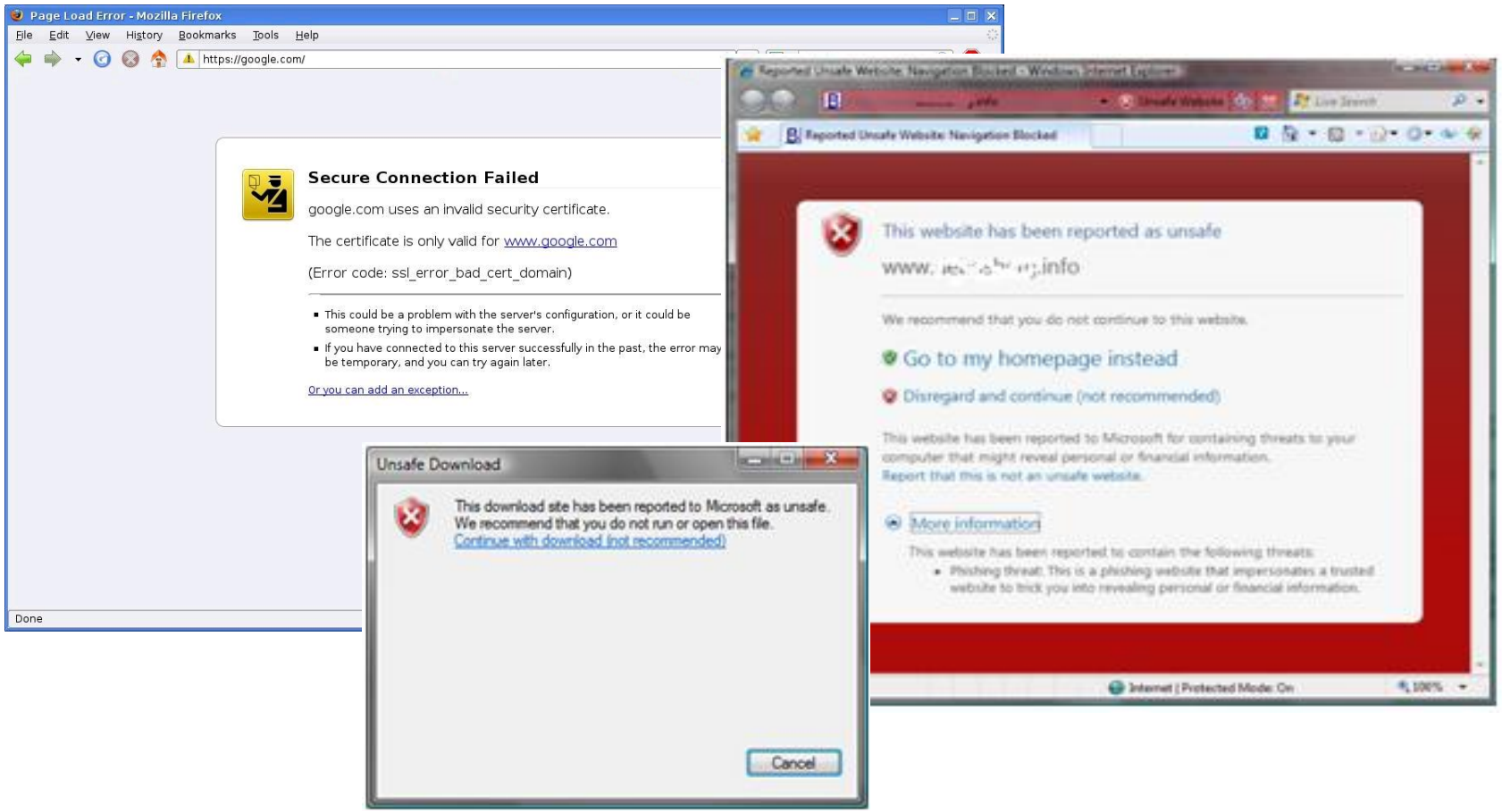


What links to www.ebay.com ?

- ✘ http://secure-ebay.com
- ✘ http://www.ebay.com\cgi-bin\login?ds=1%2C
  %2e%31%33%38%2e%31%33%37%2e%
- ✘ http://www.ebay.com/ws/eBayISAPI.dll?Sig
- ✓ http://scgi.ebay.com/ws/eBayISAPI.d
  co_partnerid=2&usage=0&ru=http%3
  &encRafId=default

Understanding the details

- **Internet Browser improvements**
  - New heuristics & enhanced telemetry
  - Anti-Malware support



Understanding the details

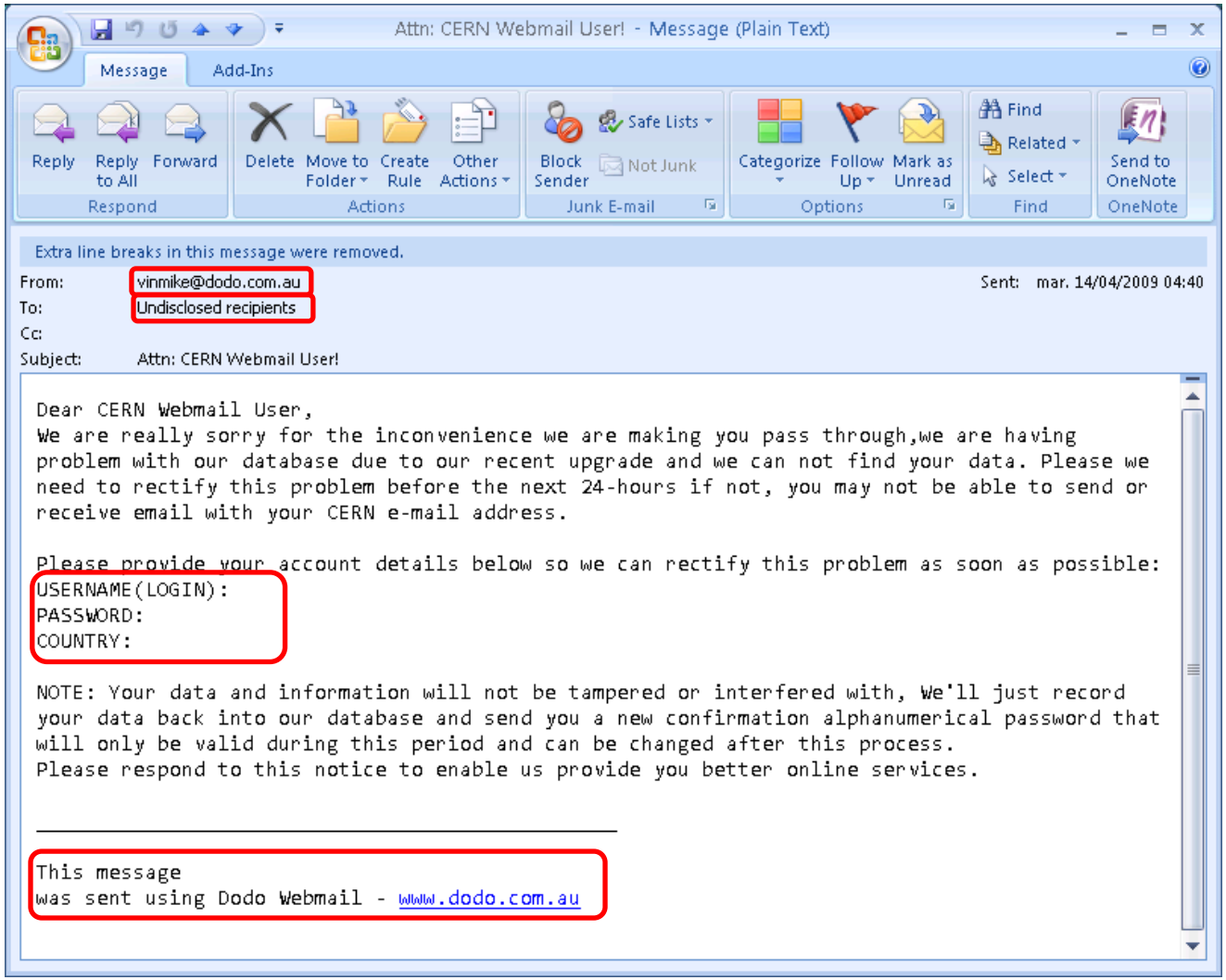
- **“In Private” Browsing**
  - Available on Internet Explorer 8 and Firefox:
    - lets you control whether or not the browser saves your browsing history, cookies, and other data
    - Internet Explorer: “Safety -> In Private Browsing”
    - Firefox: “Tools -> Start Private Browsing”

Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

Examples

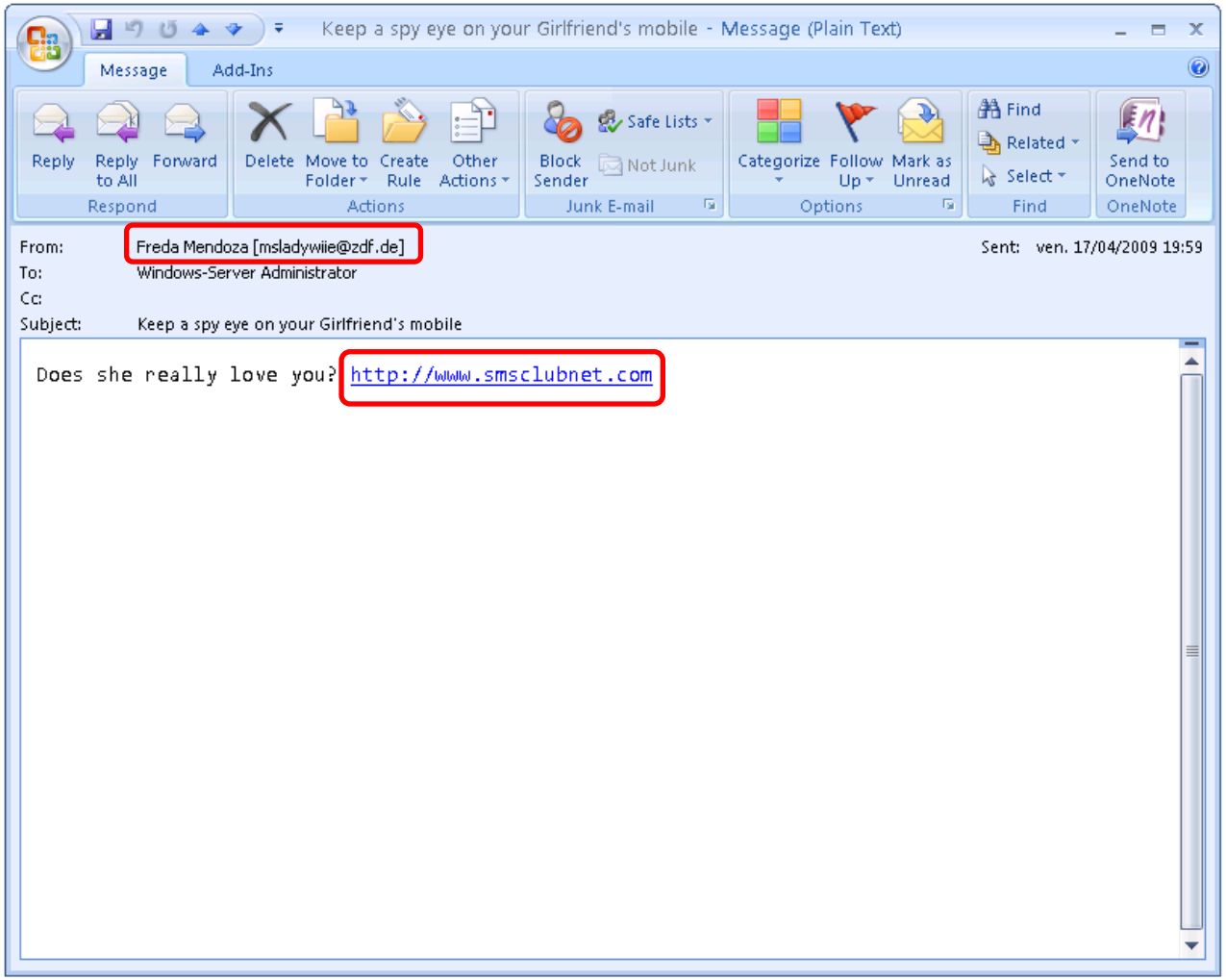
Examples

- **Phishing (1/3)**



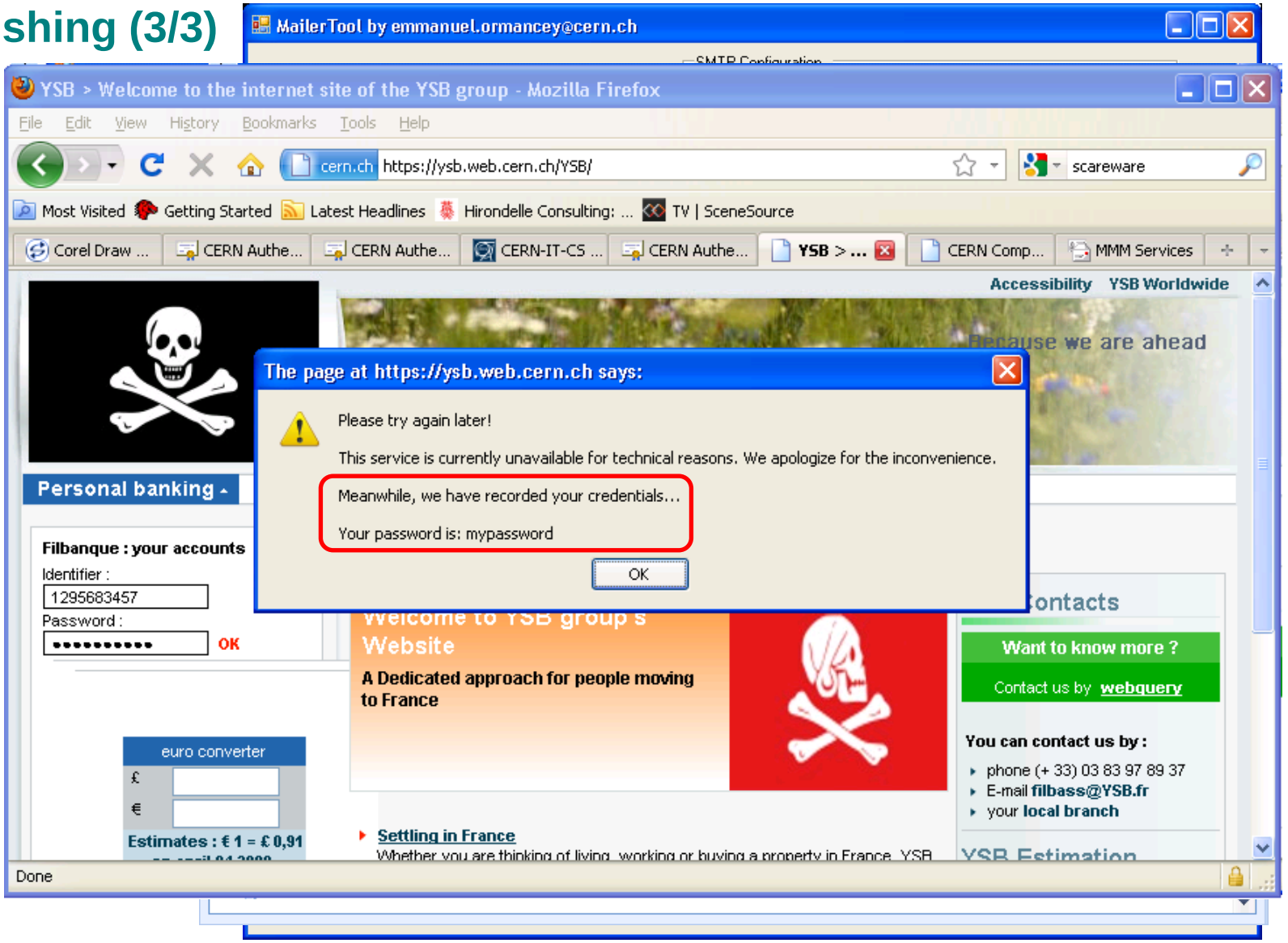
Examples

Phishing (2/3)



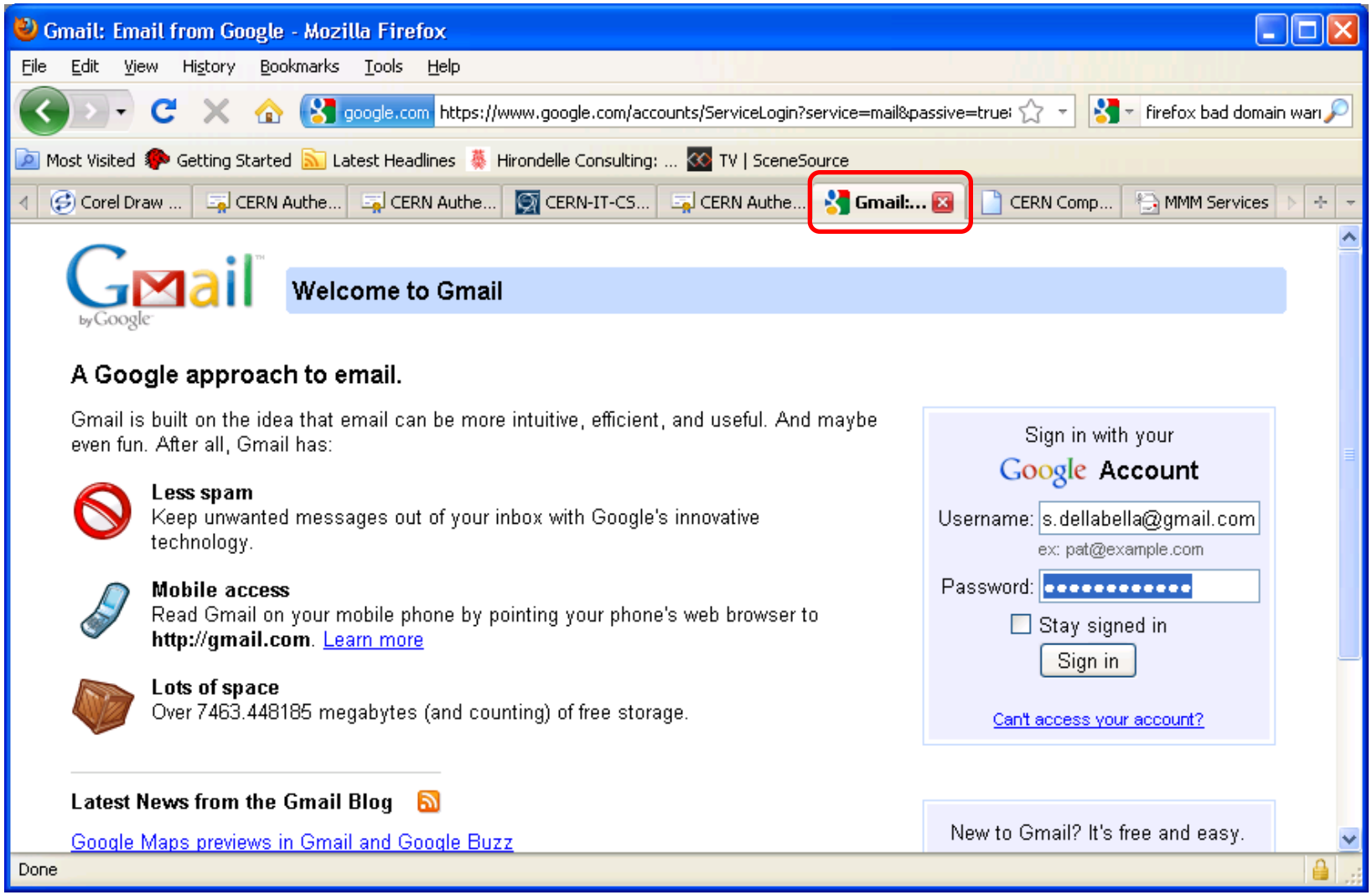
Examples

- Phishing (3/3)



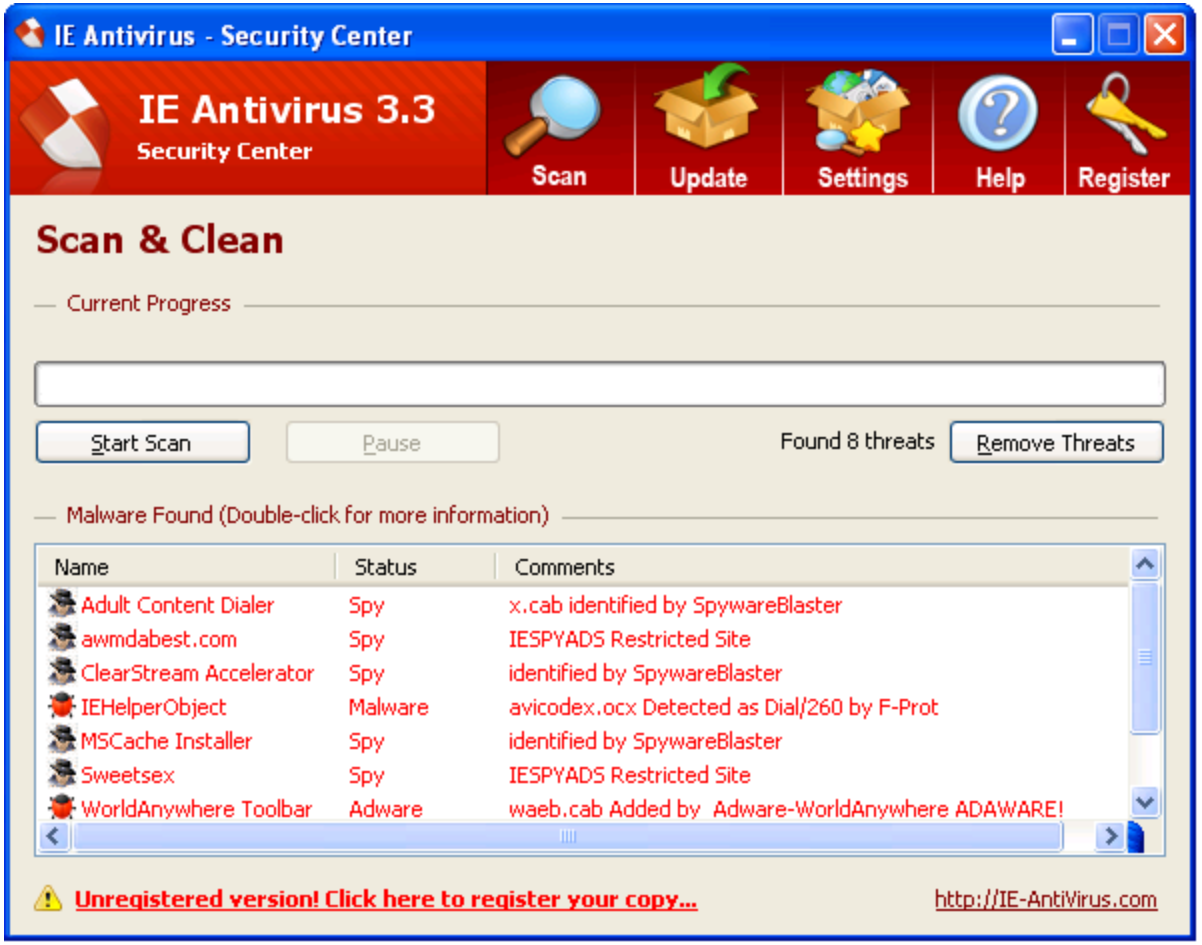
Examples

- **Tabnabbing**



Examples

- **Untrusted software: Scareware**



Summary

- **User awareness**
  - **No** credentials (login/password) over email
  - **No** same password for different place/software/service
  - **No** clicking on links sent by your contacts before confirmation.
  - **No** use of untrusted media (USB stick, CD, DVD, Hard-drive)
  - **No** use of Internet randomly downloaded software
  - **No** forwarding of unverified information to your contacts
  - Read before you click and If you have any doubt, don’t click
- **Up-to-date OS, Antivirus and software**
- **Work without “Administrator” rights**
  - Standard on Windows VISTA, Windows 7, Mac OS, Linux
  - Use “NICE Admin” on XP
- **SEC_RITY is not complete without U !**
  - The Security Team is ready to help you: computer.security@cern.ch

Q&A

Questions ???

Resources

- **CERN Computer Security web site**
  - http://cern.ch/security
- **CERN Antivirus Help Section**
  - https://cern.ch/win/Help/?fdid=13
- **NICE Services – How to install Antivirus at home?**
  - https://cern.ch/win/Help/?kbid=051050
- **CERN Security – Advice on SPAM**
  - http://cern.ch/security/recommendations/en/bad_mails.shtml
- **NICE Services – Spam fighting configuration**
  - https://cern.ch/mmm/Help/?kbid=101030

Thank you !