

SECURITY is not complete without **U**

Computer Security Day

10 June 2010, Council Chamber and <http://cern.ch/SecDay>

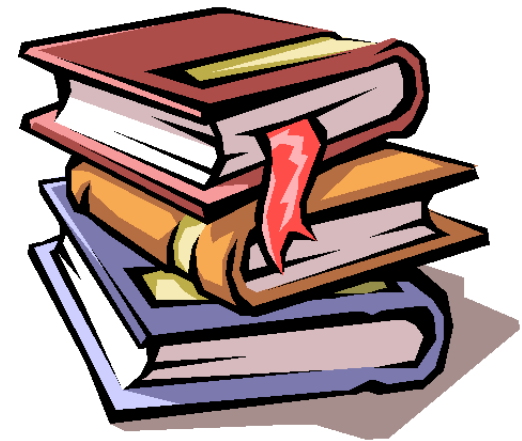
Secure Email and Web Browsing

Sébastien Dellabella – Computer Security Team

Overview

Computer.Security@cern.ch — “Computer Security Day” — slide 2

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



SECURITY is not complete without **U**

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.
- ▶ **Understanding the attack makes it ineffective**
 - ▶ Forged mail
 - ▶ Tabnabbing **NEW!**

User interaction needed



A screenshot of a Windows User Account Control (UAC) dialog box. The title bar reads "User Account Control". The main text says "An unidentified program wants to make changes to your computer. Don't run the program unless you are sure." Below this, it lists the program as "intelliadmin.exe" from "Unidentified Publisher". There are two buttons: "Cancel" (with the text "I don't know where this program came from") and "Allow" (with the text "I trust this program. I know what I'm doing"). To the right of the dialog box is a cartoon illustration of a person in a purple hooded cloak and mask, holding a magnifying glass over a woman sitting at a computer. The background of the slide shows a blurred computer screen with text like "Add...", "We will...", and "rm that".

SECURITY is not complete without **U**

Computer Security Day

10 June 2010, Council Chamber and <http://cern.ch/SecDay>

Consequences of Attacks

Consequences of Attacks

Computer.Security@cern.ch — “Computer Security Day” — slide 6

▶ 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)



SECURITY is not complete without **U**

Computer Security Day

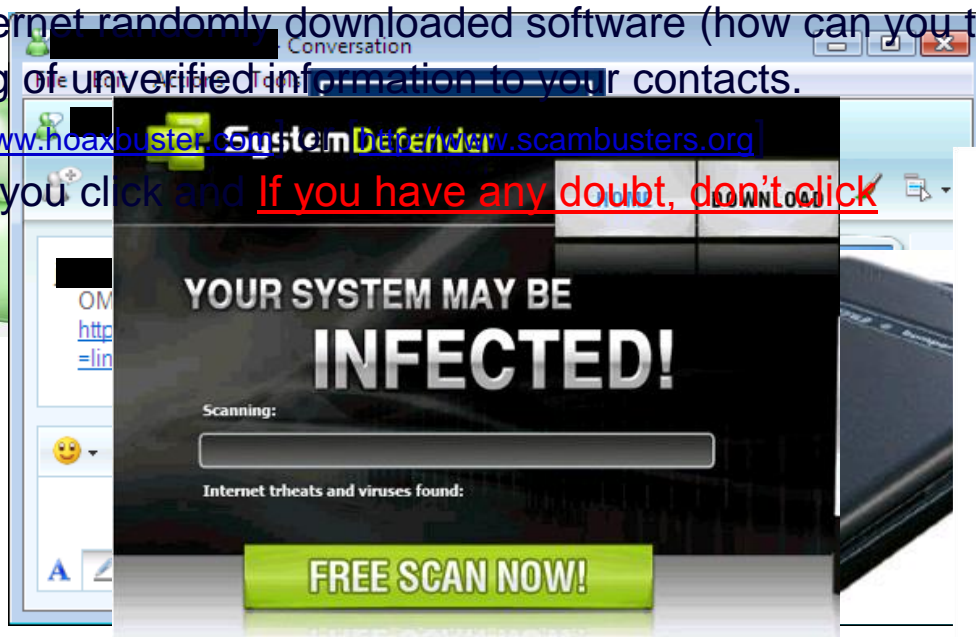
10 June 2010, Council Chamber and <http://cern.ch/SecDay>

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> or www.scambusters.org
- Read **before** you click and **If you have any doubt, don't click**



Survival Guide (2/2)

Computer.Security@cern.ch — “Computer Security Day” — slide 9

▶ 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**
[\[http://www.dshield.org/survivaltime.html\]](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 !**
[\[https://cern.ch/win/Help/?kbid=051092\]](https://cern.ch/win/Help/?kbid=051092)

Understanding the details

Computer.Security@cern.ch — “Computer Security Day” — slide 10

► 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 Resource Locator)
- What you see



the link below

[Dispute Transaction](#)

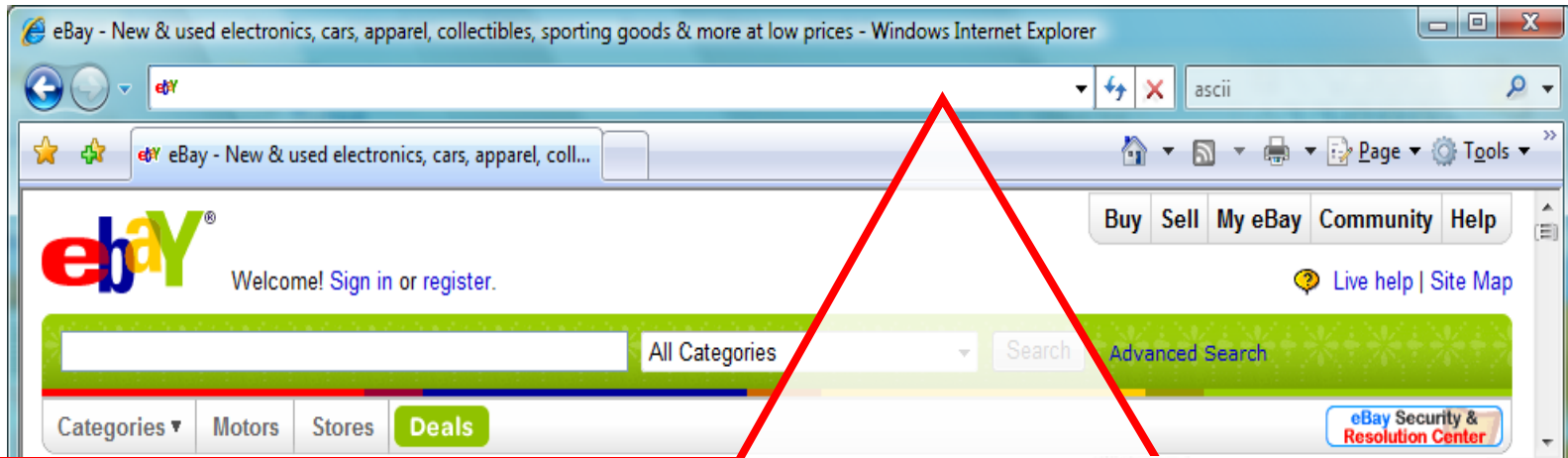
Thank you for using PayPal!
The PayPal Team

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

Computer.Security@cern.ch — "Computer Security Day" — slide 11



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?Sign>
- ✔ http://scgi.ebay.com/ws/eBayISAPI.dll?co_partnerid=2&usage=0&ru=http%3A&encRaflid=default

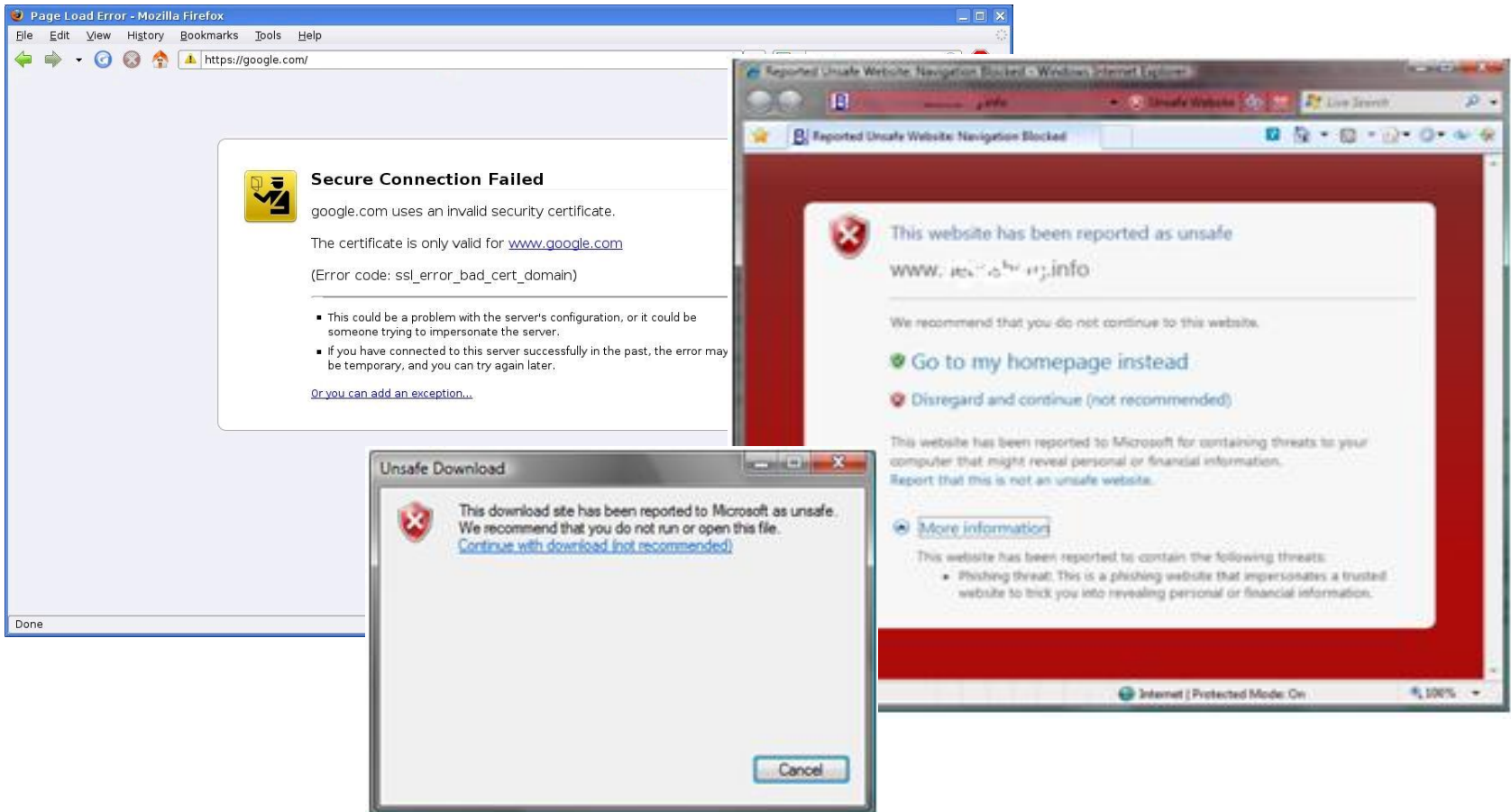
THIS IS NOT EVEN OBVIOUS FOR PROFESSIONALS !

Understanding the details

Computer.Security@cern.ch — “Computer Security Day” — slide 12

► Internet Browser improvements

- New heuristics & enhanced telemetry
- Anti-Malware support



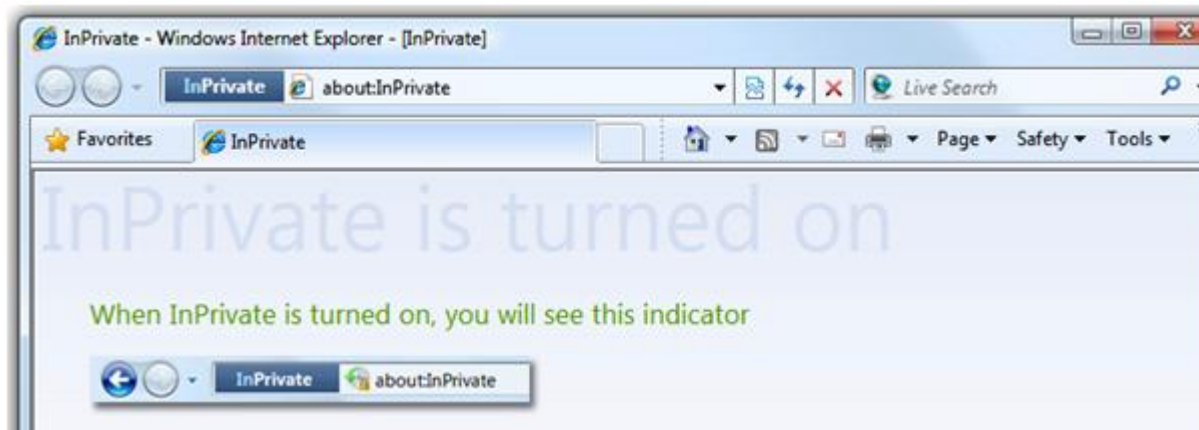
Understanding the details

Computer.Security@cern.ch — “Computer Security Day” — slide 13

► “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”





SECURITY is not complete without **U**

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

Examples

Examples

Computer.Security@cern.ch — “Computer Security Day” — slide 15

► Phishing (1/3)

Attn: CERN Webmail User! - Message (Plain Text)

Message Add-Ins

Reply Reply to All Forward Delete Move to Folder Create Rule Other Actions Block Sender Not Junk Categorize Follow Up Mark as Unread Find Related Select Send to OneNote

Extra line breaks in this message were removed.

From: **vinmike@dodo.com.au** Sent: mar. 14/04/2009 04:40
To: **Undisclosed recipients**
Cc:
Subject: Attn: CERN Webmail User!

Dear CERN Webmail User,
We are really sorry for the inconvenience we are making you pass through, we are having problem with our database due to our recent upgrade and we can not find your data. Please we need to rectify this problem before the next 24-hours if not, you may not be able to send or receive email with your CERN e-mail address.

Please provide your account details below so we can rectify this problem as soon as possible:
USERNAME (LOGIN):
PASSWORD:
COUNTRY:

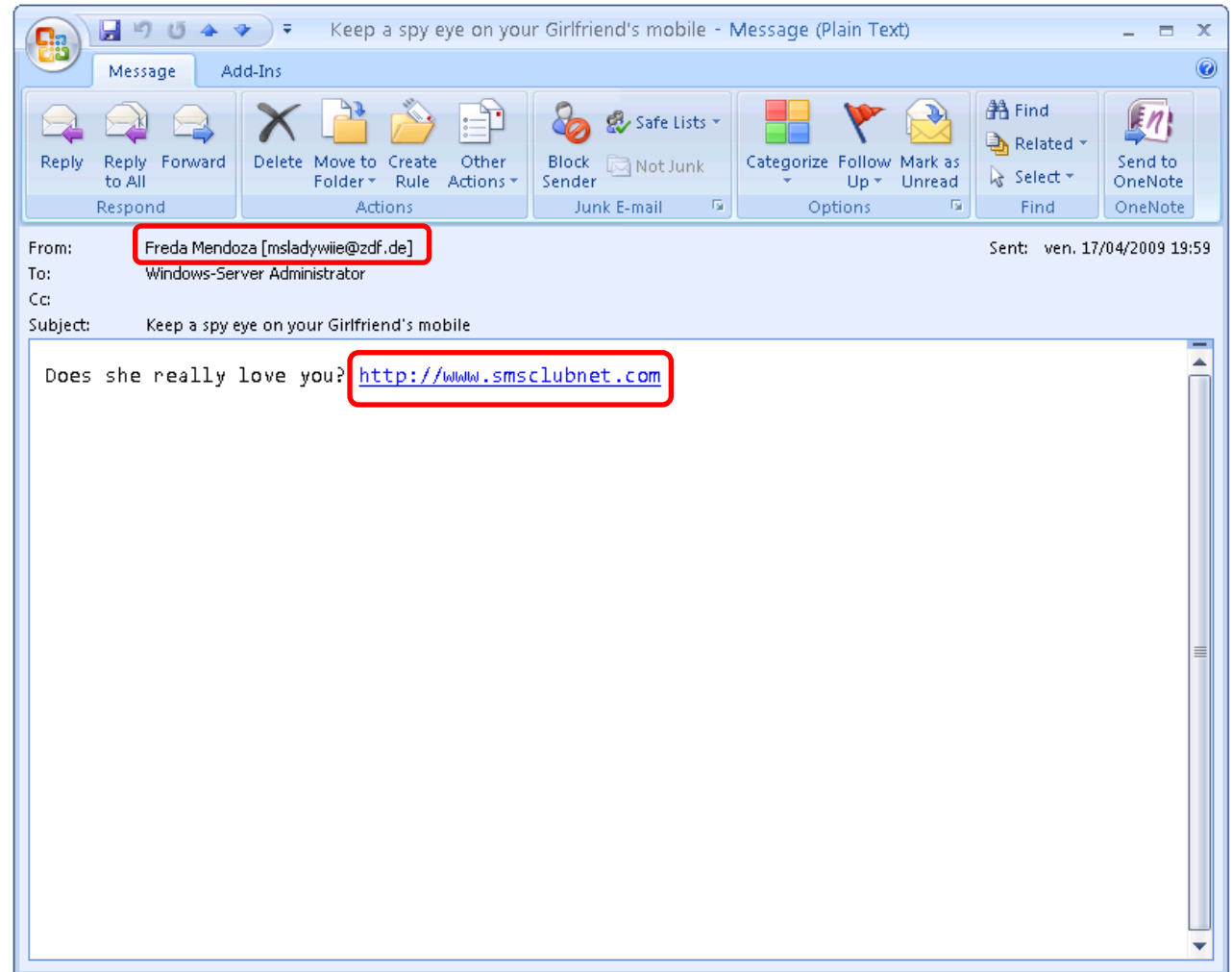
NOTE: Your data and information will not be tampered or interfered with, We'll just record your data back into our database and send you a new confirmation alphanumeric password that will only be valid during this period and can be changed after this process.
Please respond to this notice to enable us provide you better online services.

—
This message was sent using Dodo Webmail - www.dodo.com.au

Examples

Computer.Security@cern.ch — “Computer Security Day” — slide 16

► Phishing (2/3)



Examples

► Phishing (3/3)

The screenshot shows a Mozilla Firefox browser window displaying a phishing website. The address bar shows the URL `https://ysb.web.cern.ch/YSB/`. The page content includes a skull and crossbones icon, a "Personal banking" section with a "Filbanque : your accounts" form, and a "welcome to YSB group's Website" banner. A warning dialog box is overlaid on the page, displaying the following text:

The page at `https://ysb.web.cern.ch` says:

⚠ Please try again later!

This service is currently unavailable for technical reasons. We apologize for the inconvenience.

Meanwhile, we have recorded your credentials...

Your password is: mypassword

OK

The background website features a "euro converter" tool, a "Settling in France" link, and contact information for YSB, including a phone number and email address.

Examples

► Tabnabbing

The screenshot shows a Mozilla Firefox browser window with the title "Gmail: Email from Google - Mozilla Firefox". The address bar displays "https://www.google.com/accounts/ServiceLogin?service=mail&passive=true". The tab bar shows several tabs, with the active tab titled "Gmail...". The main content area displays the Gmail login page, including the "Welcome to Gmail" header, a "Sign in with your Google Account" section, and a "New to Gmail? It's free and easy." link. The browser's status bar at the bottom shows "Done".

Examples

Computer.Security@cern.ch — “Computer Security Day” — slide 19

► Untrusted software: Scareware



The screenshot shows the IE Antivirus Security Center interface. The title bar reads "IE Antivirus - Security Center". The main header area includes the "IE Antivirus 3.3 Security Center" logo and navigation buttons for "Scan", "Update", "Settings", "Help", and "Register".

The "Scan & Clean" section displays a progress bar and a "Start Scan" button. Below this, it indicates "Found 8 threats" and provides a "Remove Threats" button.

The "Malware Found" section contains a table with the following data:

Name	Status	Comments
Adult Content Dialer	Spy	x.cab identified by SpywareBlaster
awmdabest.com	Spy	IESPYADS Restricted Site
ClearStream Accelerator	Spy	identified by SpywareBlaster
IEHelperObject	Malware	avicodex.ocx Detected as Dial/260 by F-Prot
MSCache Installer	Spy	identified by SpywareBlaster
Sweetsex	Spy	IESPYADS Restricted Site
WorldAnywhere Toolbar	Adware	waeb.cab Added by Adware-WorldAnywhere ADAWARE!

At the bottom of the window, a warning message states: "Unregistered version! Click here to register your copy..." with a link to <http://IE-AntiVirus.com>.

Summary

Computer.Security@cern.ch — “Computer Security Day” — slide 20

▶ 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

Computer.Security@cern.ch — “Computer Security Day” — slide 21

Questions ???

Resources

Computer.Security@cern.ch — “Computer Security Day” — slide 22

- ▶ **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 !