



Unmasking the fake Microsoft support scammers!

david.jacoby@kaspersky.com

Senior Security Researcher – GReAT – Kaspersky Lab



David Jacoby

Senior Security Researcher

Global Research and Analysis Team

Malware on Unix/Linux and alternative system

Web Application Security / Penetration testing

Vulnerability and Threat Management

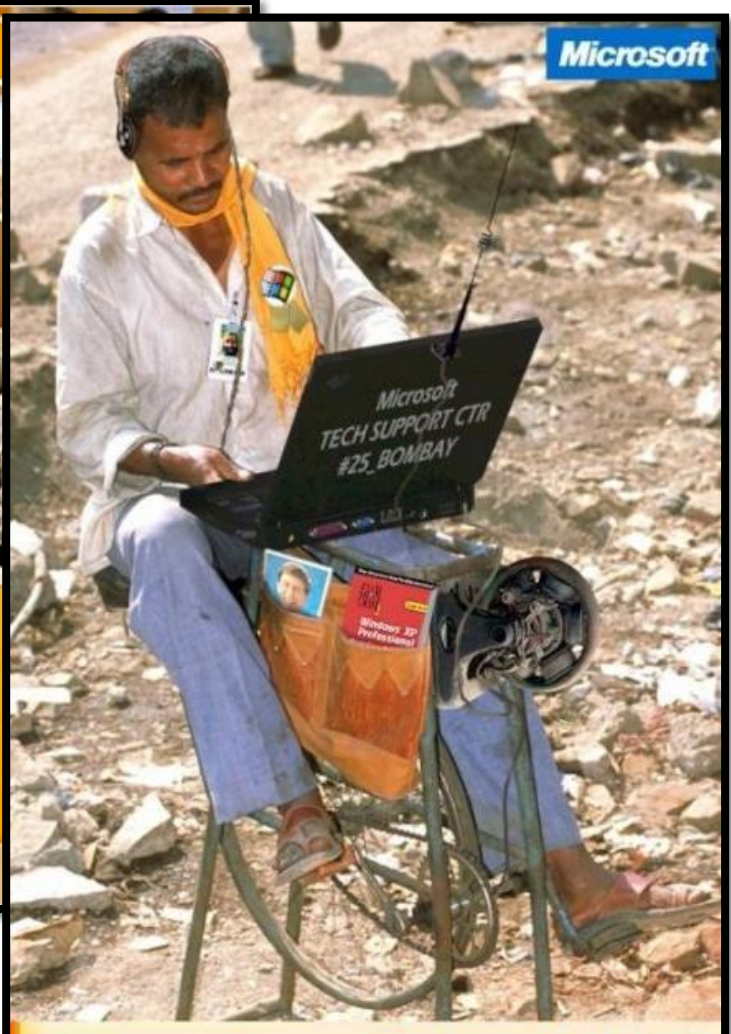
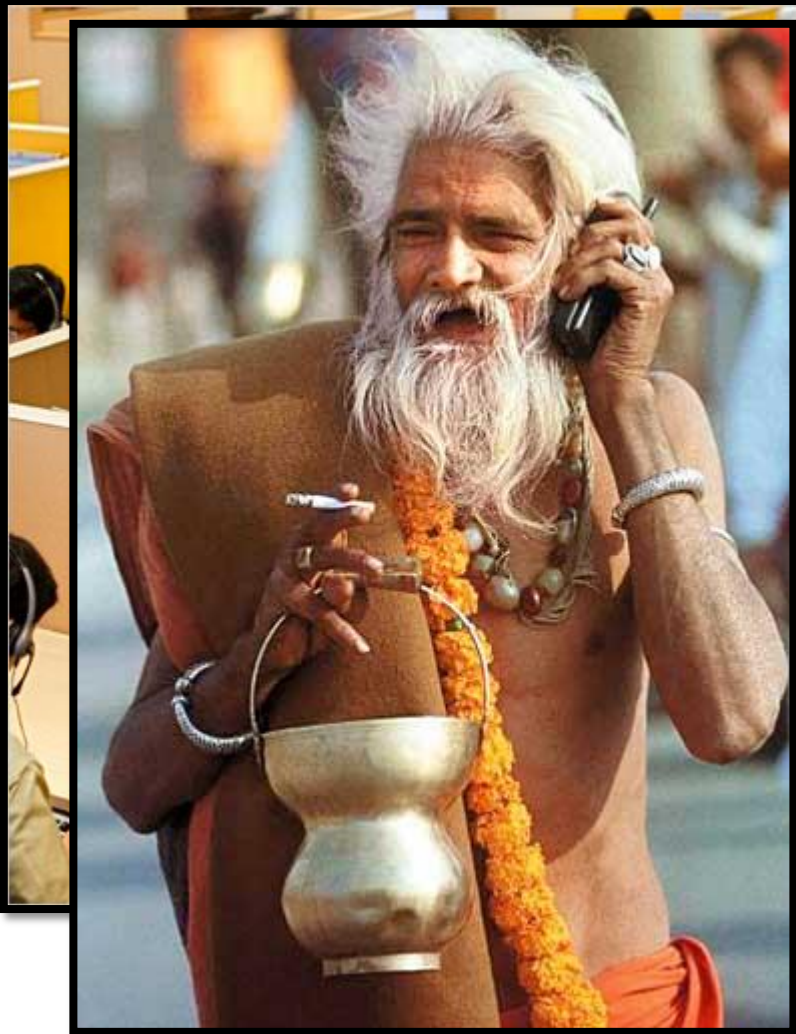


WHAT IS THE PROBLEM?

WHAT GOOGLE THINKS PHONE SUPPORT IS



WHAT IS REALLY IS!



Global Support Centre Employee of the Month

WHAT ARE WE FACING?

MailOnline

1,000 Britons a day hit by Indian call centre swindle: Police believe fraudsters have made £10million from UK victims

WHAT ARE WE FACING?

Rough estimation of profit

\$350 000 profit PER DAY!

* source New York Times

WHAT ARE WE FACING?

- Pretend to be calling from
 - California
 - Hasselt
 - London
 - Los Angeles
 - New York

- Company claiming to work working at
 - Apple
 - Microsoft
 - Windows
 - Microsoft Windows Help Centre
 - Windows Office

WHAT ARE WE FACING?

- Allowed method of payment
 - Mastercard
 - VISA
 - Western Union
 - (PayPal)

- "Remote Access Control" tool used
 - Aplemix
 - Ammyy
 - LogMeIn
 - TeamViewer

WHAT ARE WE FACING?

- Excused of calling
 - Computer infected with virus
 - Errors detected by Microsoft
 - Computer is in danger/hacked
 - Speed up the computer
 - License expired
 - Computer has been hacked (by **Afghanistan** hackers)

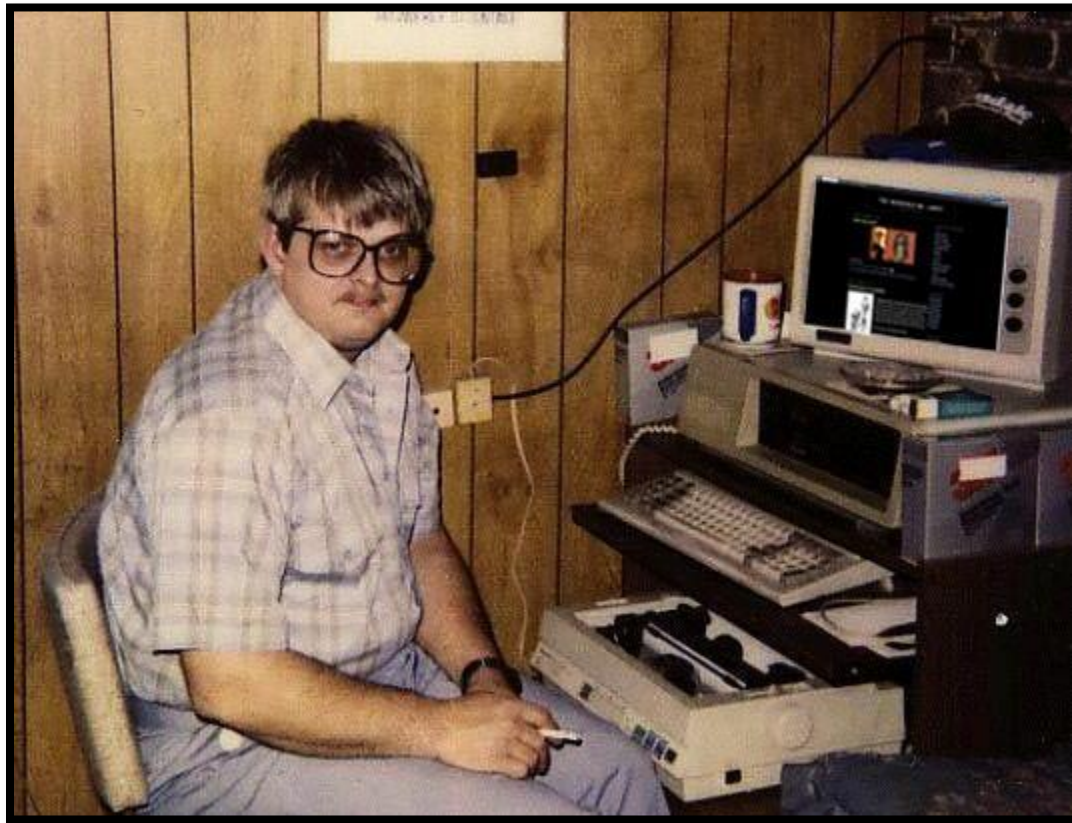
WHAT ARE WE FACING?



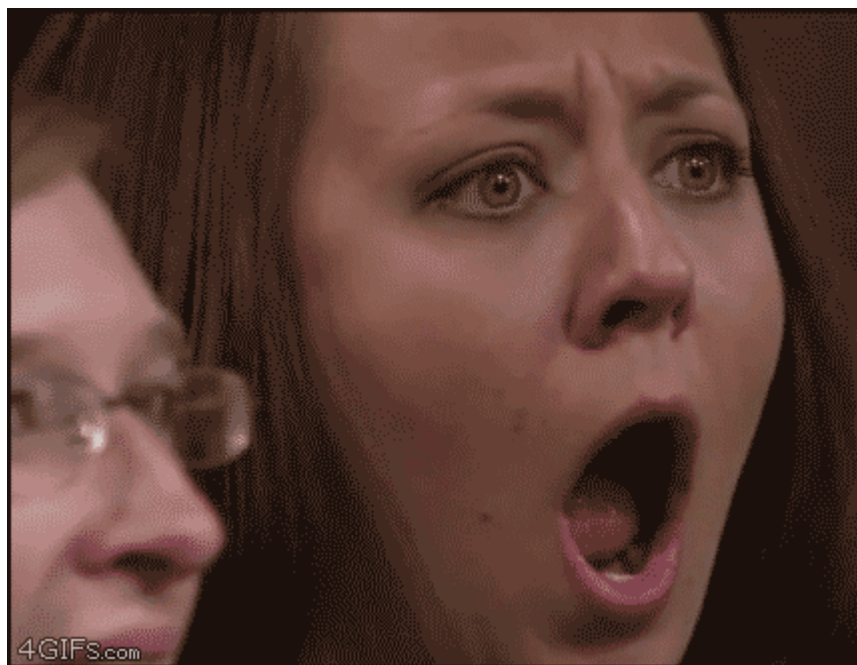
MY STORY

MY STORY

I WAS WORKING AT HOME AS USUAL



THEY TOLD ME MY COMPUTER WAS INFECTED (how they thought i reacted)

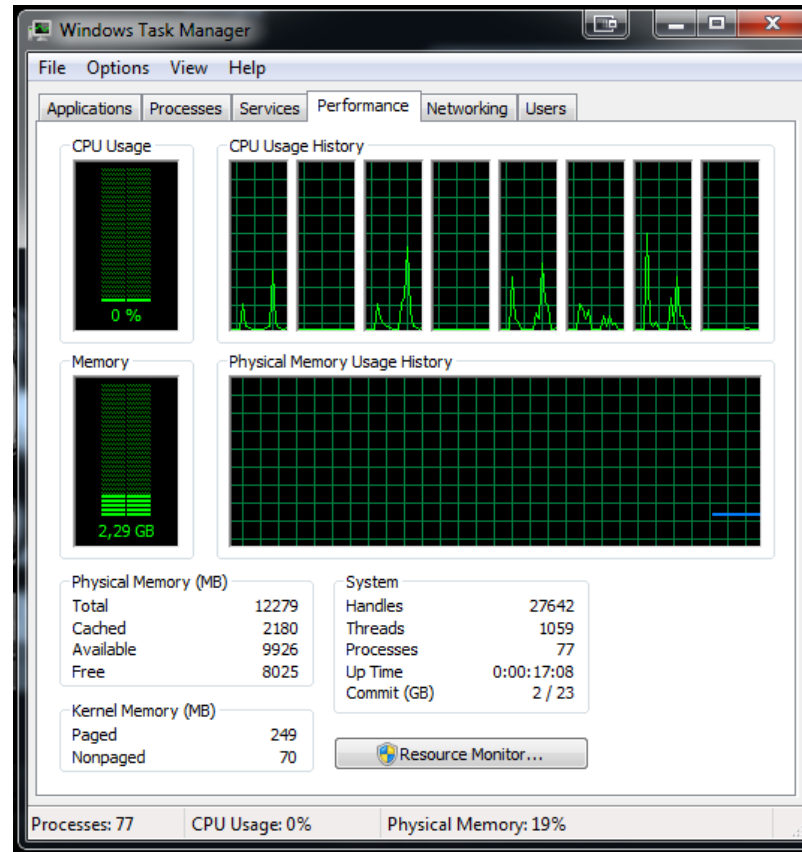


THEY TOLD ME MY COMPUTER WAS INFECTED (how i REALLY reacted)



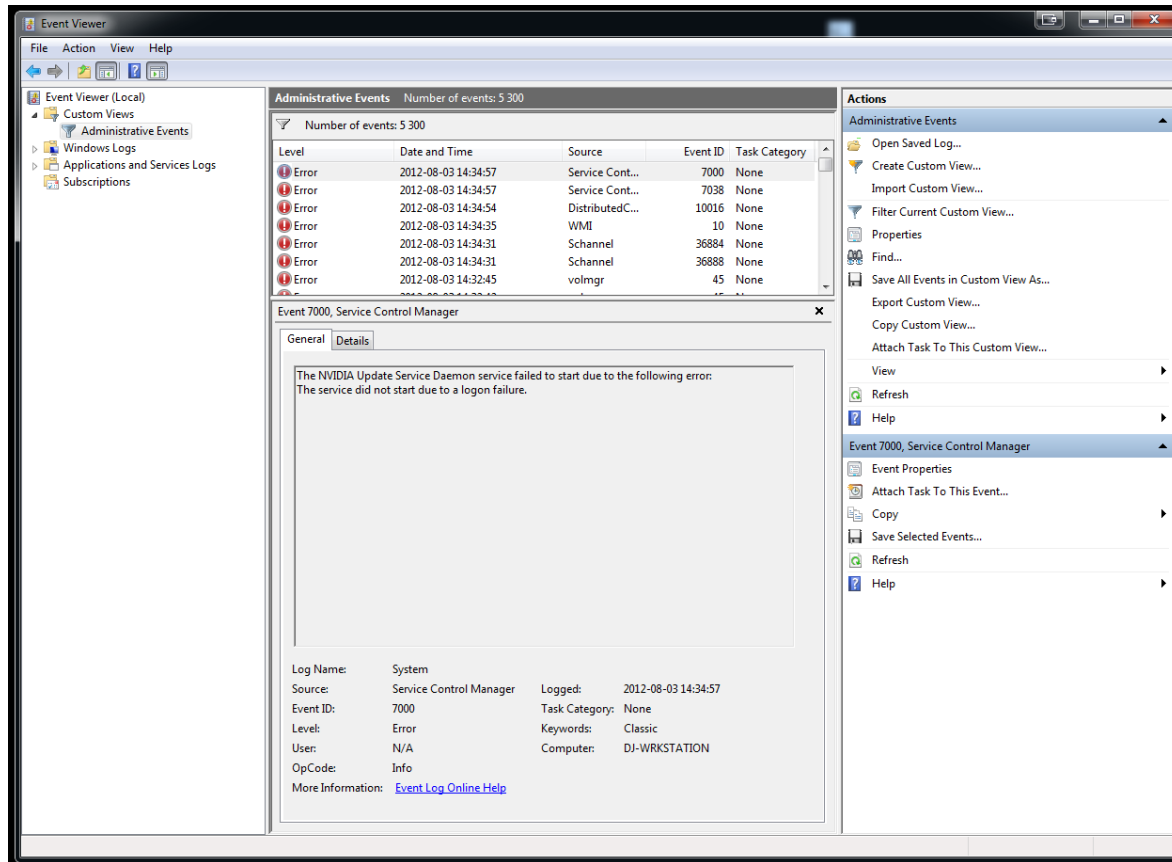
THEIR TRICKS

MY COMPUTER WAS ONLY WORKING AT **0%**



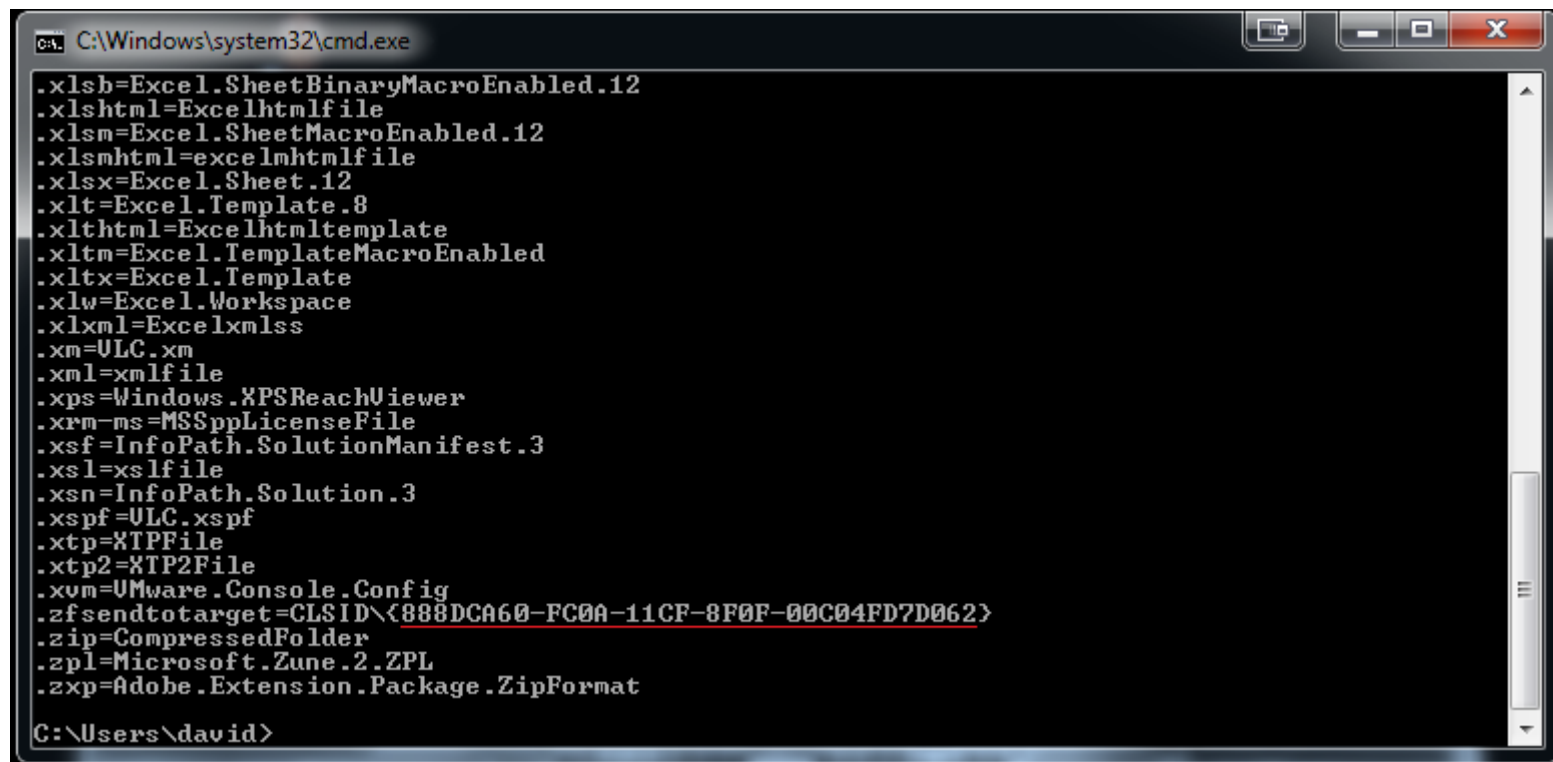
THEIR TRICKS

HAD TONS OF ERRORS



THEIR TRICKS

APPARENTLY MY **UNIQUE COMPUTER ID** WAS **INFECTED**



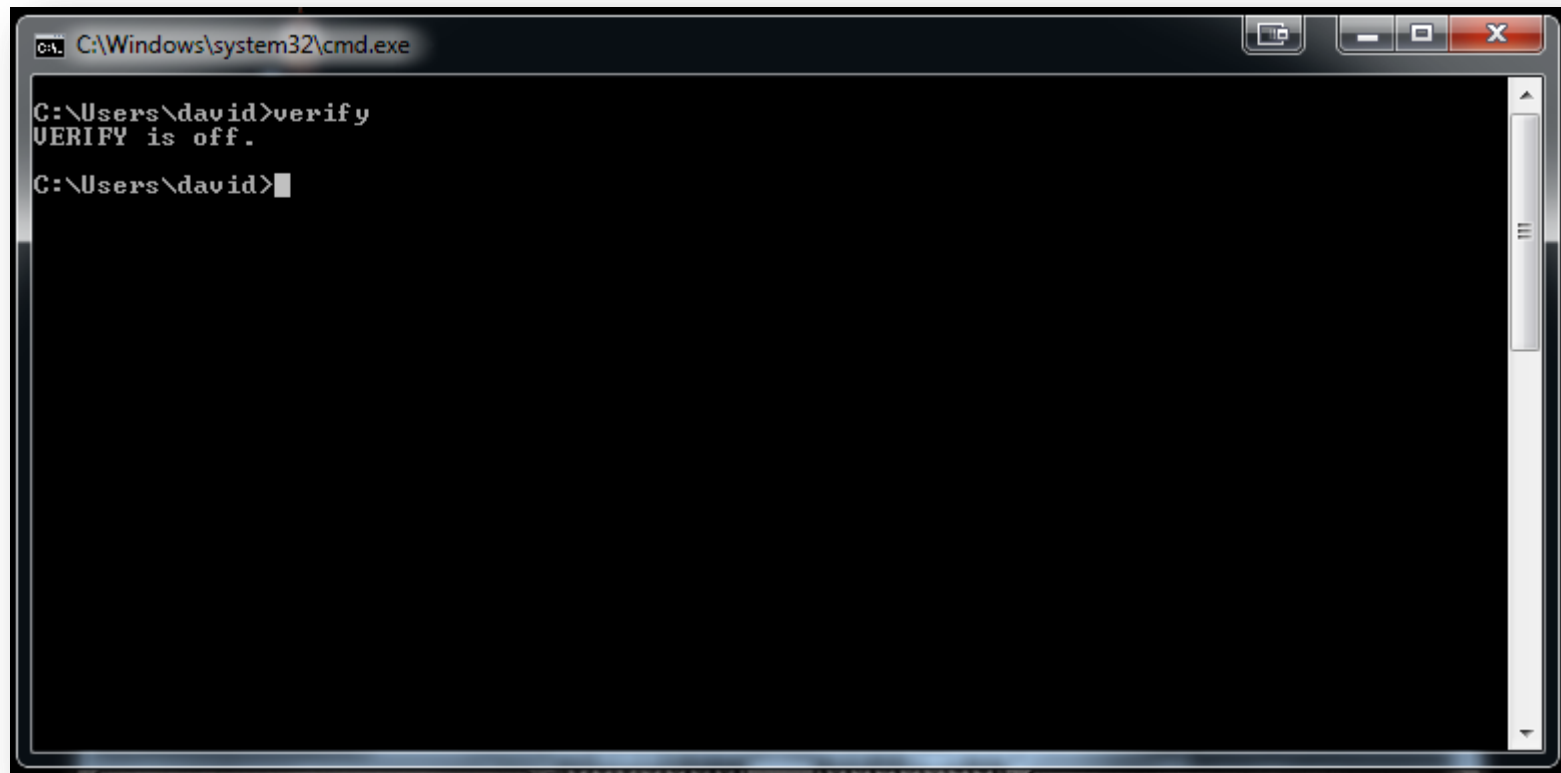
```
C:\Windows\system32\cmd.exe

.xlsb=Excel.SheetBinaryMacroEnabled.12
.xlshtml=Excelhtmlfile
.xlsm=Excel.SheetMacroEnabled.12
.xlsmhtml=excelmhtmlfile
.xlsx=Excel.Sheet.12
.xlt=Excel.Template.8
.xlthtml=Excelhtmltemplate
.xltm=Excel.TemplateMacroEnabled
.xltx=Excel.Template
.xlw=Excel.Workspace
.xlsxml=Excelxmlss
.xm=ULC.xm
.xml=xmfile
.xps=Windows.XPSReachViewer
.xrm-ms=MSSppLicenseFile
.xsf=InfoPath.SolutionManifest.3
.xsl=xslfile
.xsn=InfoPath.Solution.3
.xspf=ULC.xspf
.xtp=XTPFile
.xtp2=XTP2File
.xvm=UMware.Console.Config
.zfsendtotarget=CLSID\{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}
.zip=CompressedFolder
.zpl=Microsoft.Zune.2.ZPL
.zxp=Adobe.Extension.Package.ZipFormat

C:\Users\dauid>
```

THEIR TRICKS

AND MY LICENS IS NOT **VERIFIED**



```
C:\Windows\system32\cmd.exe
C:\Users\dauid>verify
UERIFY is off.
C:\Users\dauid>
```

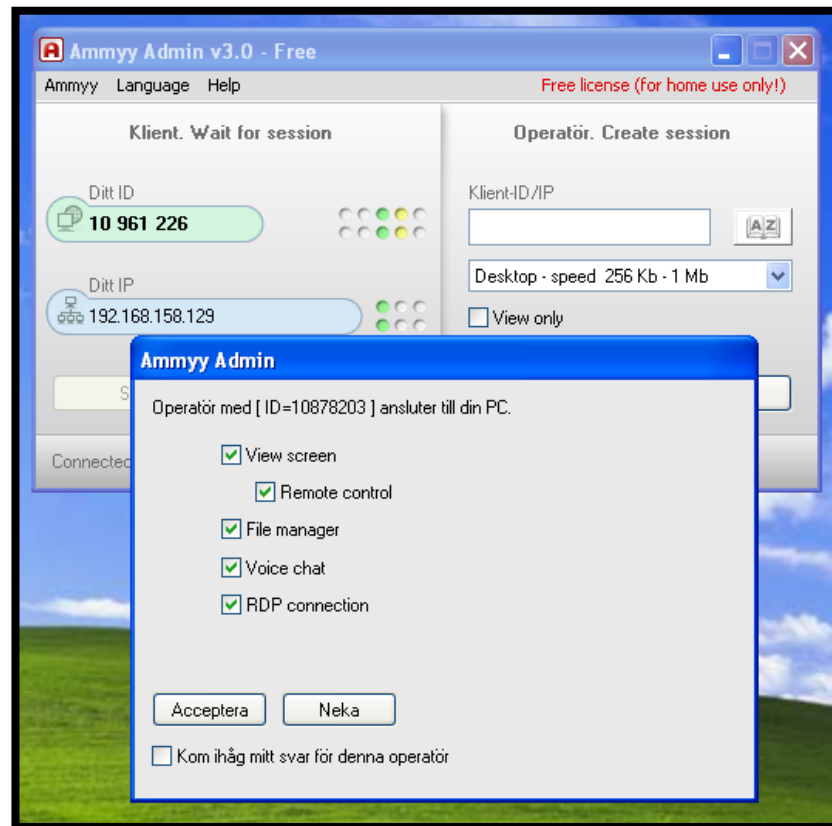
MY STORY

THIS JUST WENT ON AND ON!



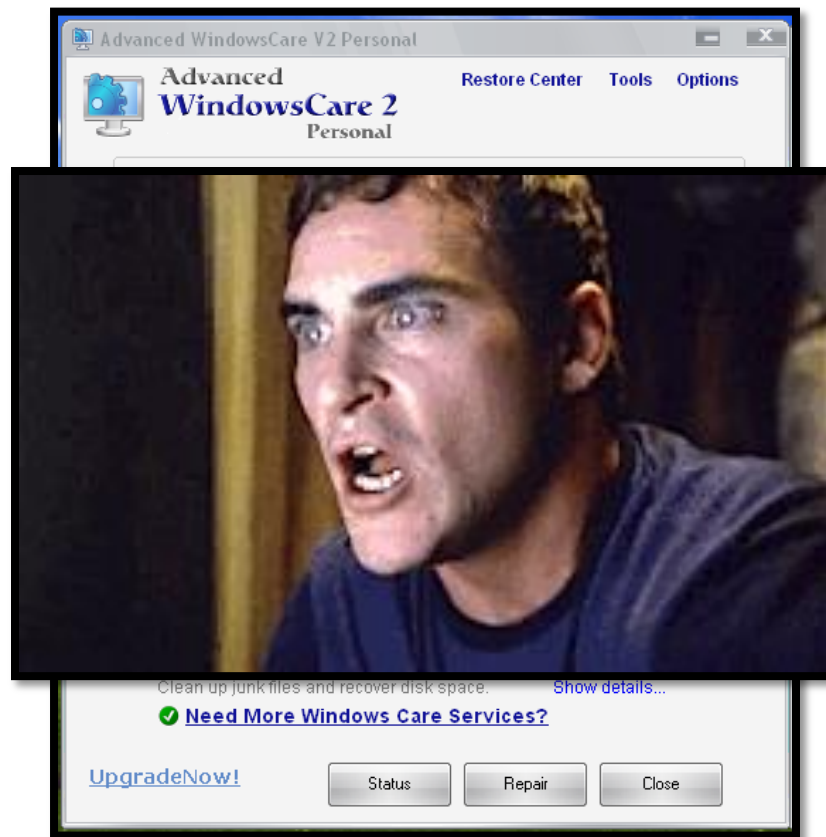
THEIR TRICKS

FINALLY DID THEY ENABLE REMOTE ACCESS



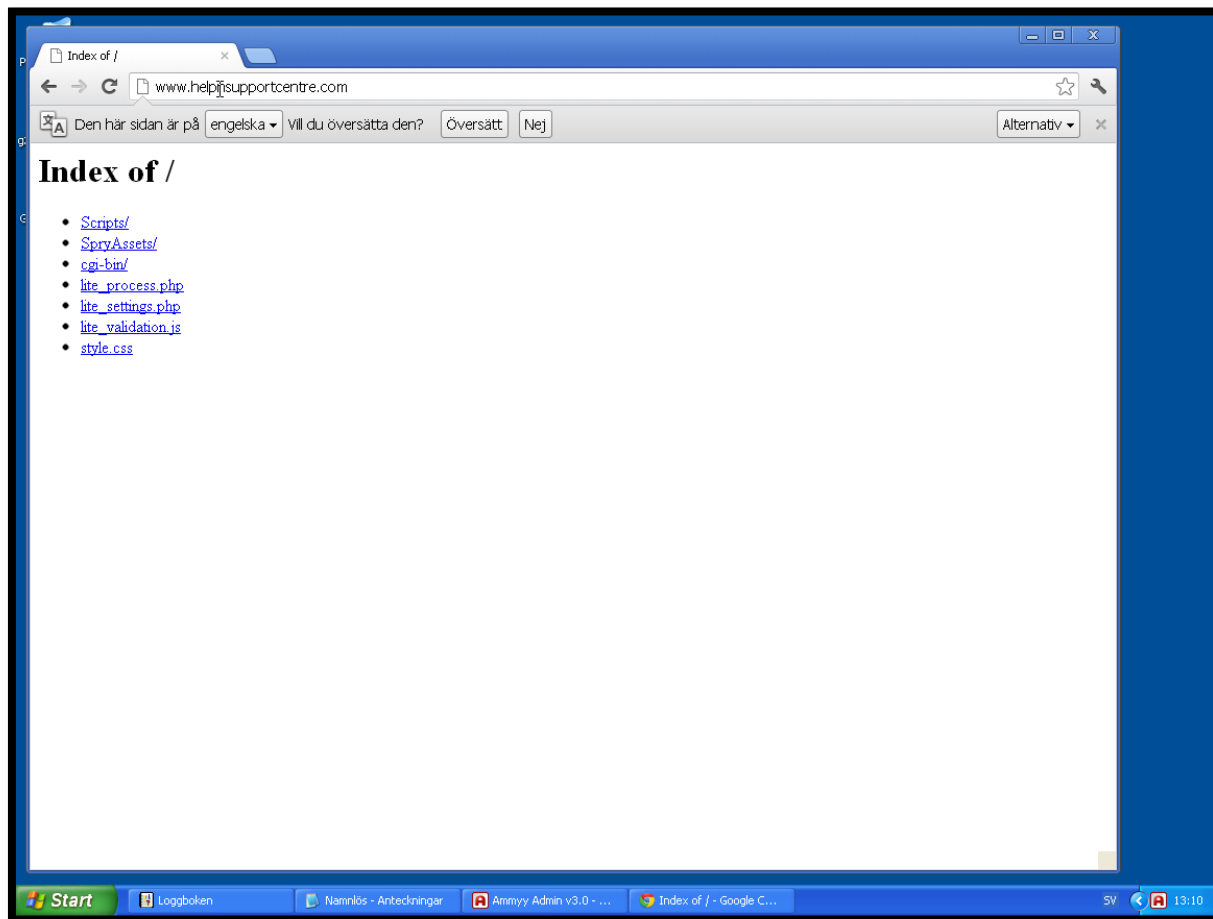
THEIR TRICKS

AND INSTALLED **FAKE** SECURITY PRODUCT

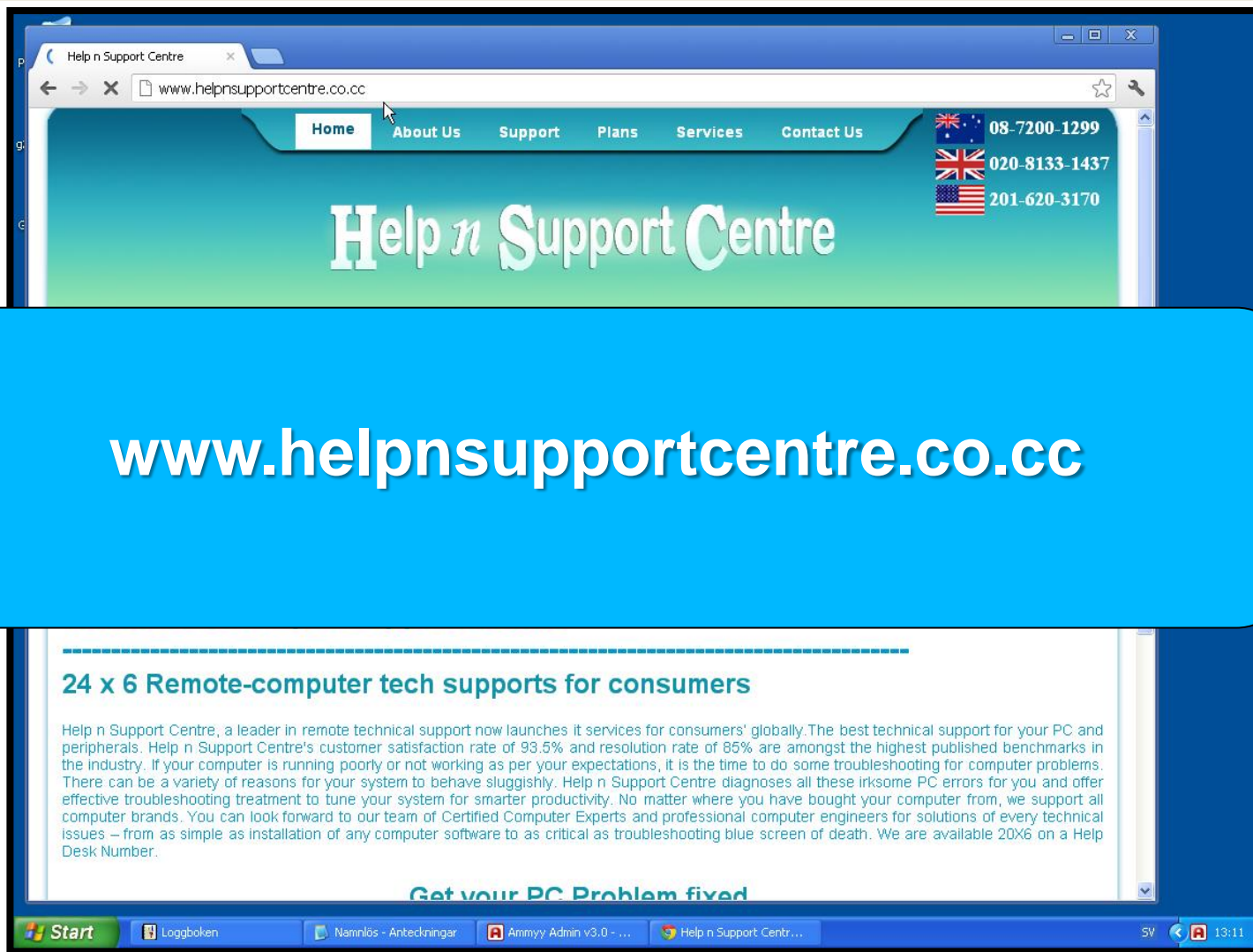


COLLECTING THE DATA

NICE **TYPO** FROM THEIR AGENT



COLLECTING THE DATA



The screenshot shows a web browser window displaying the website www.helpnsupportcentre.co.cc. The browser's address bar shows the URL. The website's navigation menu includes links for Home, About Us, Support, Plans, Services, and Contact Us. The main heading reads "Help n Support Centre". On the right side, there are three phone numbers with corresponding flags: Australia (08-7200-1299), United Kingdom (020-8133-1437), and USA (201-620-3170). Below the navigation, a blue banner contains the URL www.helpnsupportcentre.co.cc. The main content area features a section titled "24 x 6 Remote-computer tech supports for consumers" with a paragraph of text describing the company's services. The Windows taskbar at the bottom shows the Start button and several open applications: Loggboken, Namnlös - Anteckningar, Ammyy Admin v3.0 - ..., and Help n Support Centr... The system tray shows the time as 13:11.

COLLECTING THE DATA

The screenshot shows a web browser window with the following details:

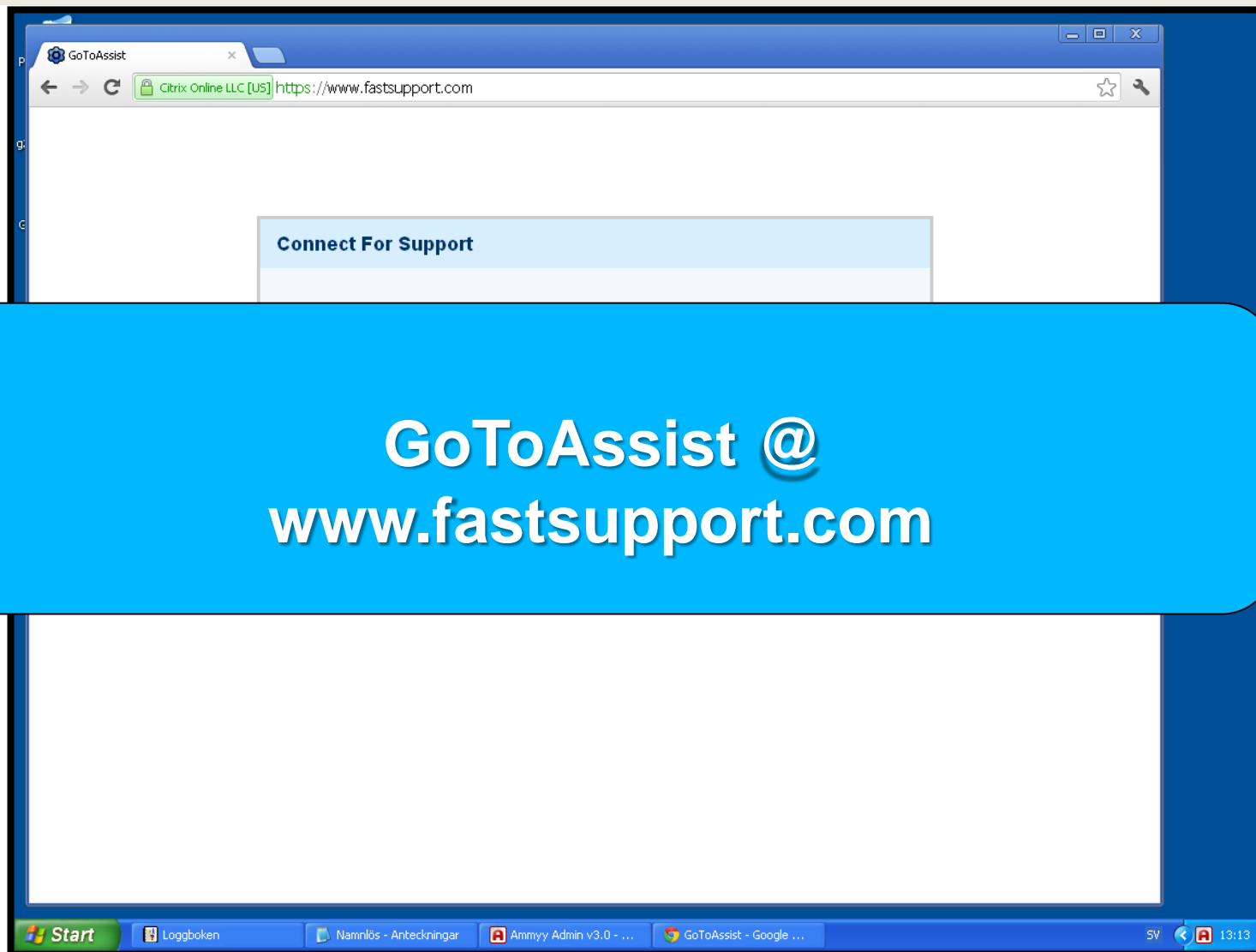
- Browser Tab:** Help n Support Centre
- Address Bar:** www.helpnsupportcentre.co.cc/24mo.html
- Language:** Svenska (Swedish)
- Page Title:** Plans
- Subscription Options:**
 - \$189.00 18 months Subscription
 - \$289.00 24 months Subscription
 - \$389.00 36 months Subscription
- Selected Option:** 24 months Subscription for \$289.00 (highlighted with a mouse cursor)
- Description:**

24 months Plan offers one of the most economical solution of fixing all your computer related issues for 24Months. There are various issues which affect a PC from time to time and hamper one's work. Our plans are designed to take care of all problems be it start up error, slow machines, virus issues, compatibility issues, setup problems and many more. We cover various operating systems and fix all your software and network problems.

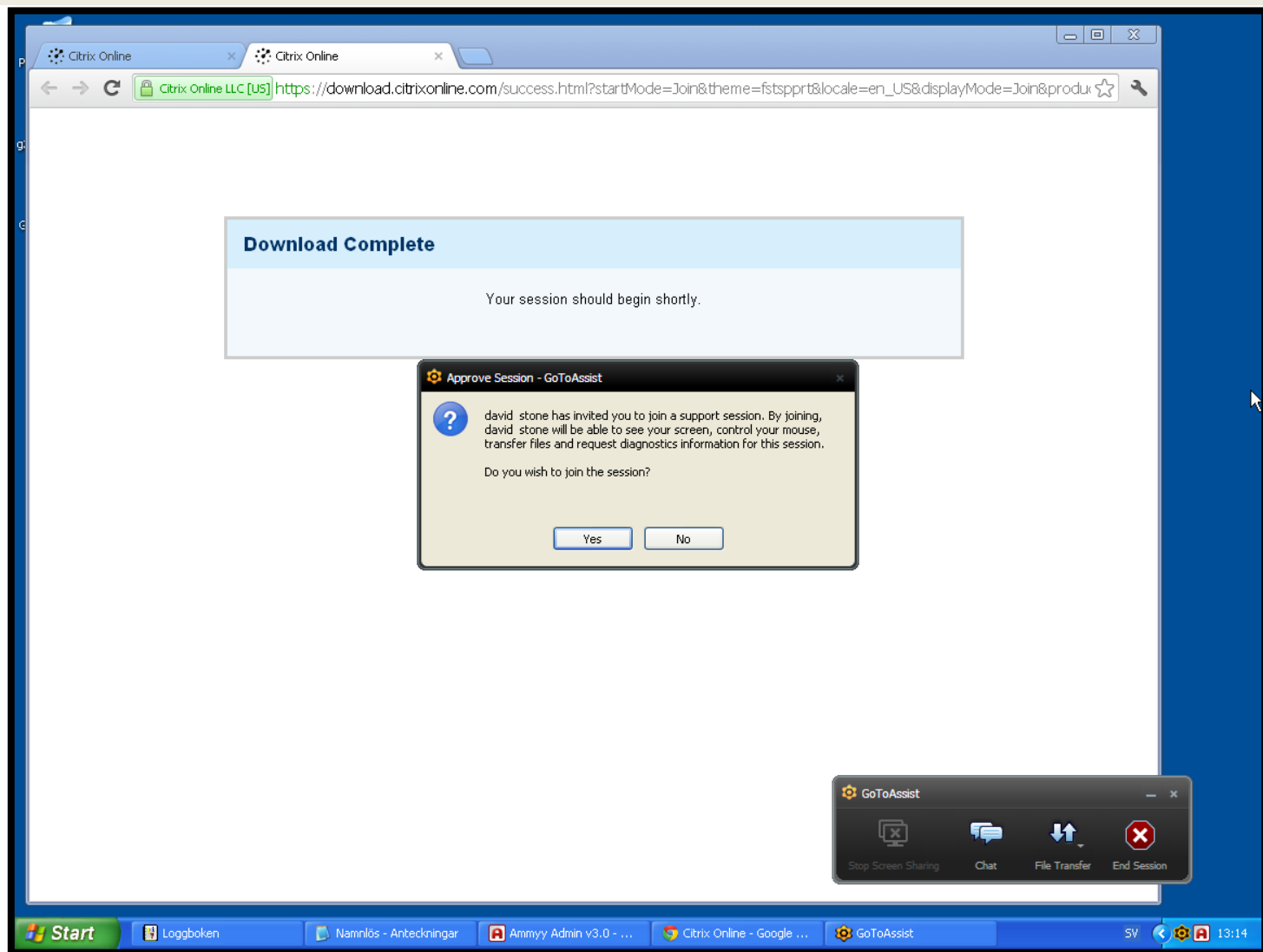
The above plan can be used for a single machine. We will address multiple issues and keep your PC trouble free Half the year.
- Footer:**
 - Terms & Condition | F.A.Q | Privacy Policy
 - Copyright @ Help n Support Centre. - 2011 | Design By: Web Professional Look

The Windows taskbar at the bottom shows the Start button and several open applications: Loggboken, Namnlös - Anteckningar, Ammyy Admin v3.0 - ..., and Help n Support Centr... The system clock shows 13:11 on SV.

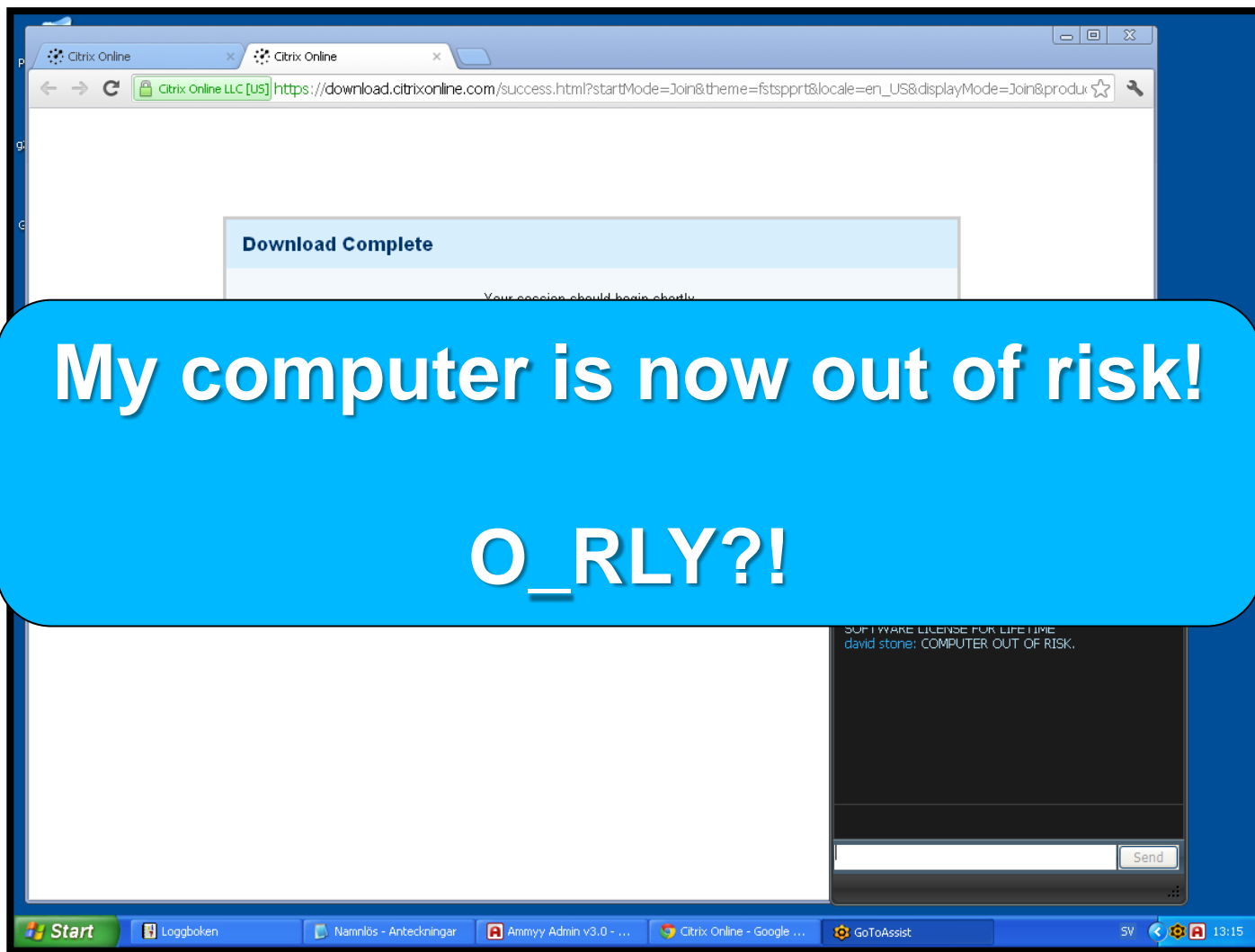
COLLECTING THE DATA



COLLECTING THE DATA



COLLECTING THE DATA

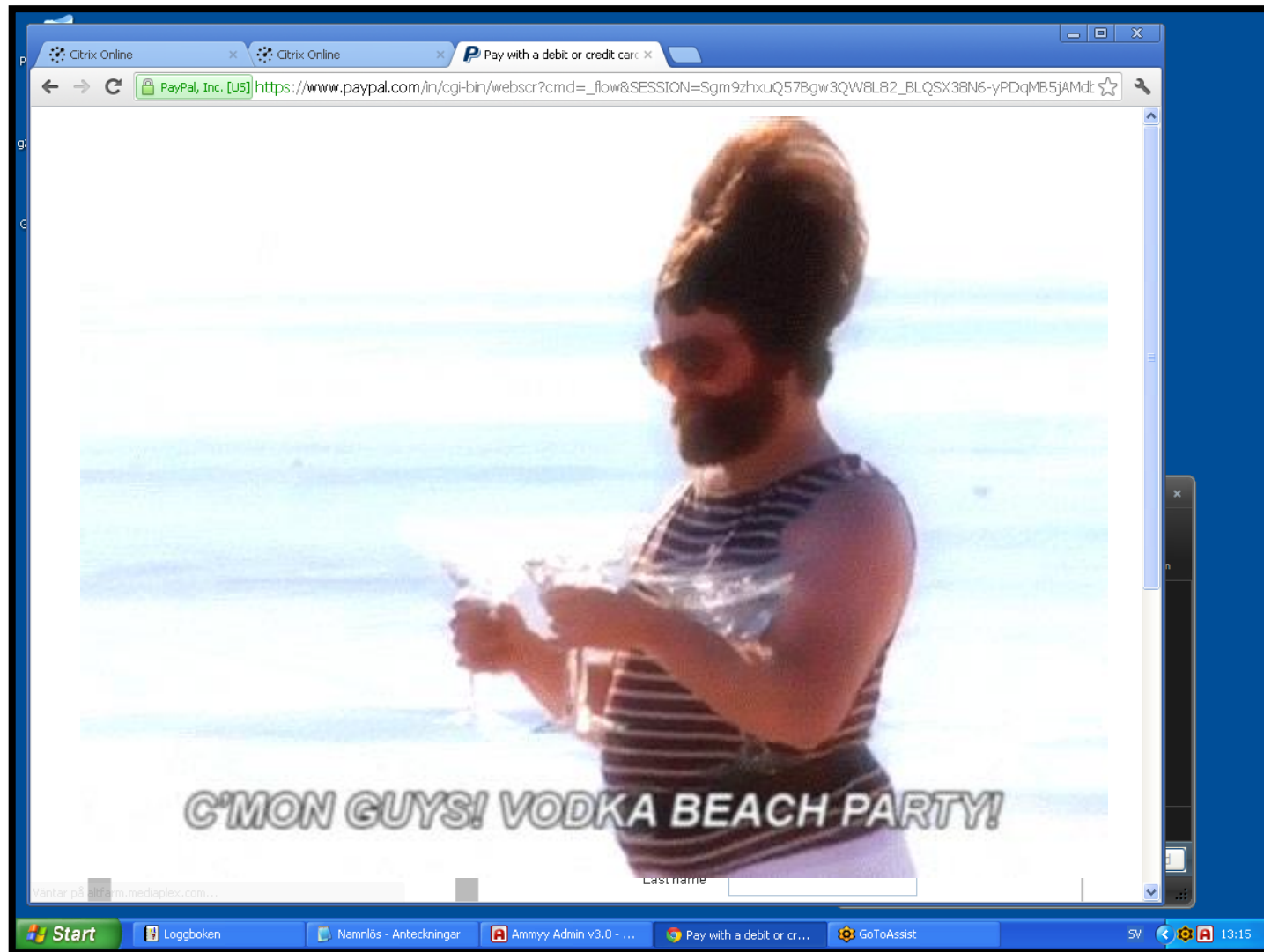


COLLECTING THE DATA

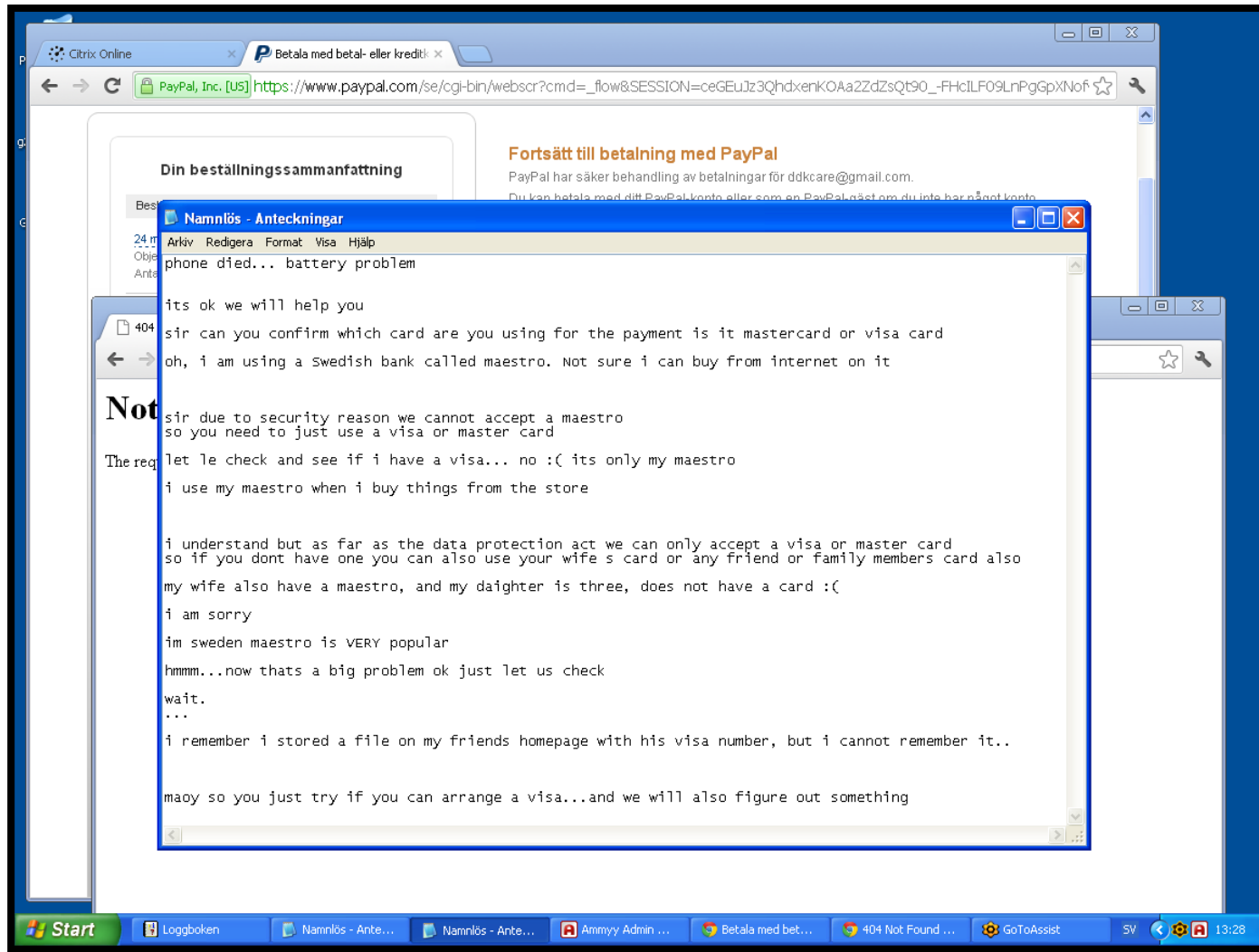
The image shows a screenshot of a web browser window. The address bar displays the URL `www.pctechnocrat.com/secure-plan.html`. Below the address bar, there is a search bar and a language selection dropdown set to 'engelska'. The main content area of the browser shows a login form titled 'Log in' with the text 'Hey, Please log in.' The form contains two input fields: 'Enter User Name' with the text 'pctechnocrat' and 'Enter Password' with masked characters. A blue arrow points to the 'Enter User Name' field. Below the input fields are two buttons: 'Login' and 'Återsta'. The browser's taskbar at the bottom shows several open applications, including 'Loggboken', 'Namnlös - Anteckni...', 'Ammyy Admin v3.0 ...', and 'Welcome to PC Tec...'. The system tray shows the time as 13:34.

Payment Portal
www.pctechnocrat.com

COLLECTING THE DATA



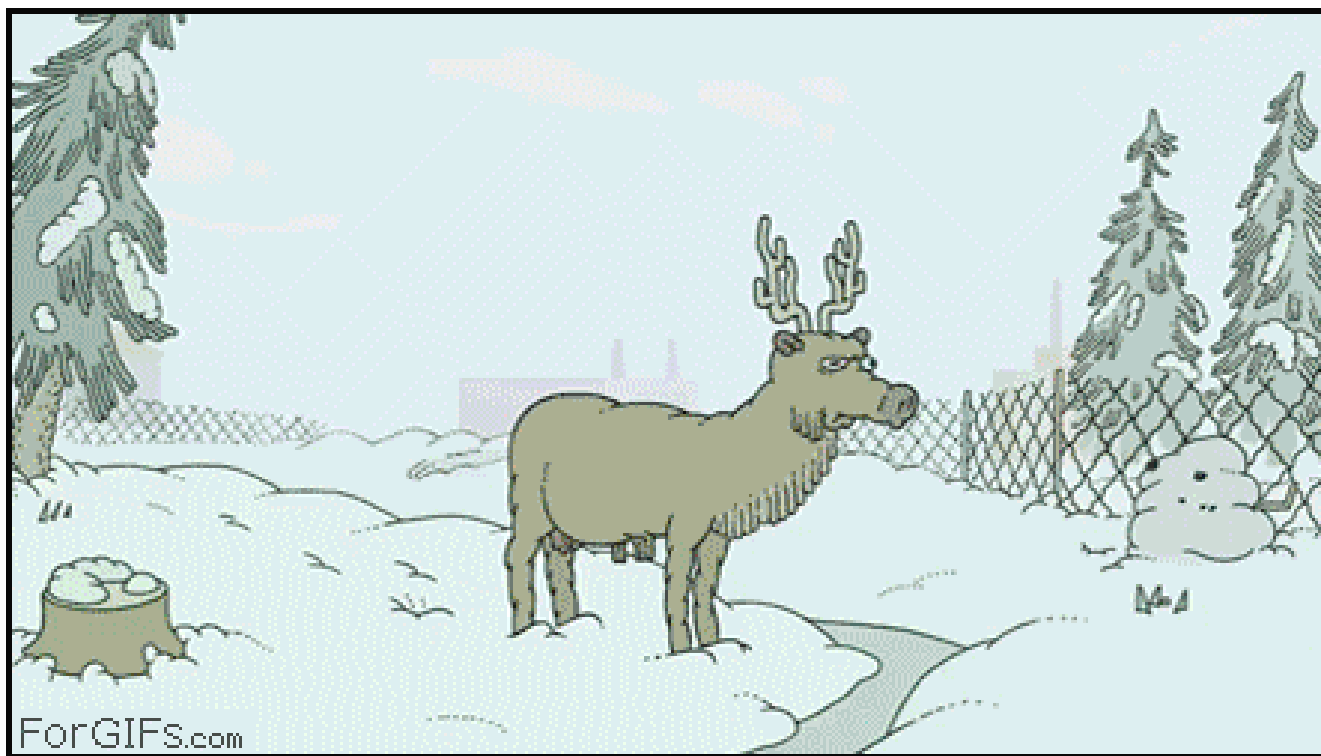
COLLECTING THE DATA



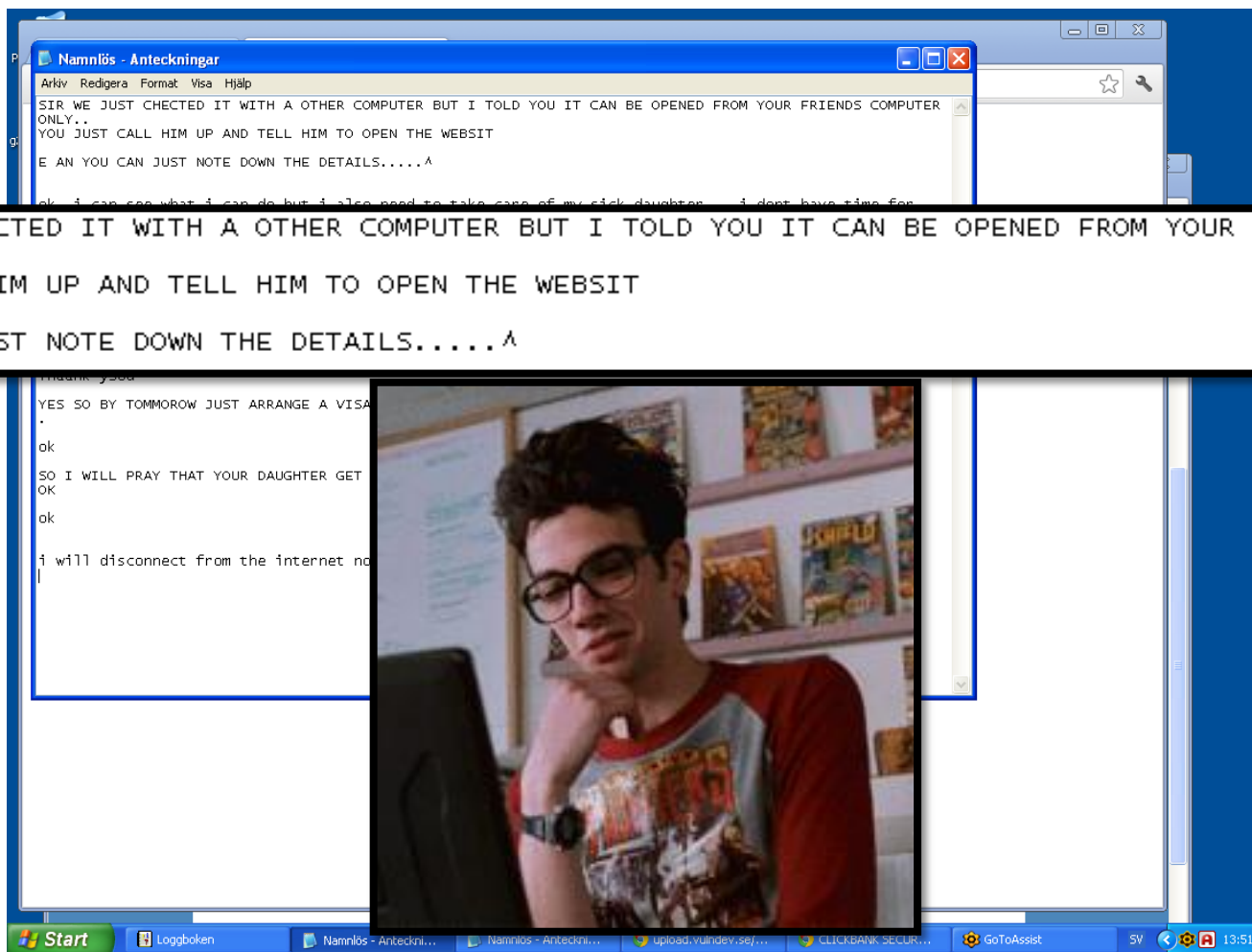
TRICKING THE TRICKSTERS

COLLECTING THE DATA

USED MY **SUPER POWERS** TO TRICK THEM!



COLLECTING THE DATA



COLLECTING THE DATA

101.63.235.197

[01/Aug/2012:13:44:31 +0200]

"GET **/personal/visa_121.txt** HTTP/1.1"

"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1"



COLLECTING THE DATA

== Additional Information From whois://whois.apnic.net ==



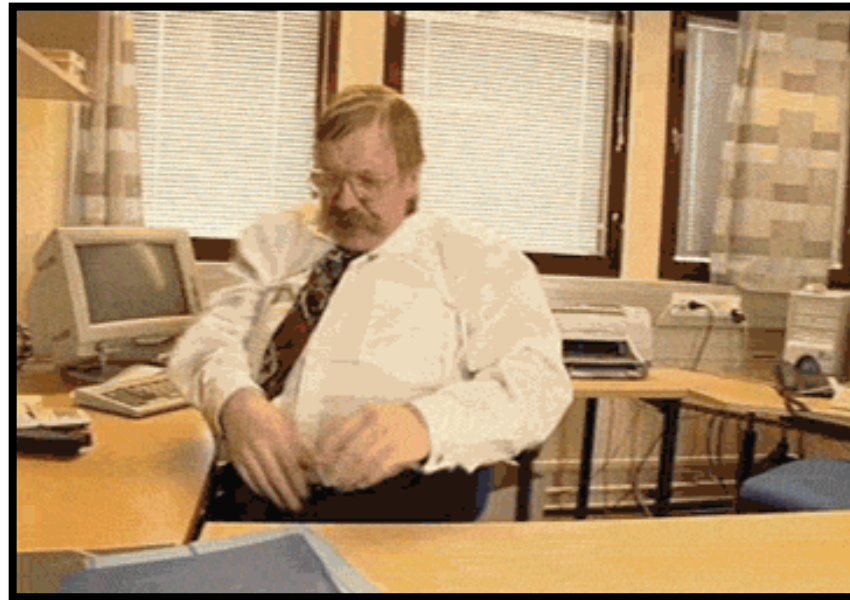
```
inetnum:          101.63.0.0 - 101.63.255.255
netname:          Wireless-HSD
country:          IN
descr:            Wireless-HSD
admin-c:          AH406-AP
tech-c:           AH406-AP
status:           ASSIGNED NON-PORTABLE
changed:          antiabuse.support@relianceada.com 20080619

mnt-by:           MAINT-IN-SN
source:           APNIC
mnt-irt:          IRT-RELIANCE-COMMUNICATIONS-IN

role:             Antiabuse Helpdesk
address:          Reliance Communication Ltd
address:          Antiabuse Helpdesk, 2nd Floor,
address:          International Area , A Block
address:          Dhirubai Ambani Knowledge City,
address:          Thane Belapur Road, Koparkhairane,
address:          Navi Mumbai - 400710
country:          IN
phone:            +91-22-30334141-5
fax-no:           +91-22-30334949
e-mail:           antiabuse.support@relianceada.com
```

COLLECTING THE DATA

HOW DID THEY REACT?!



COLLECTING INFORMATION

COLLECTING THE DATA

Registry Whois Domain Name : helpnsupportcentre.co.cc
Registrar : CO.CC, INC.
Whois Server : co.cc
Referral URL : <http://www.co.cc>
Name Server : NS01.000WEBHOST.COM
Name Server : NS02.000WEBHOST.COM

Updated Date : 28-Jul-2012
Creation Date : 28-Jul-2012
Expiration Date : 28-Jul-2013

Registrant sudipta ganguly

INDIA



Email : sudipta.ganguly@kavishtechsoft.com
Phone :
Instant messenger :

Updated Date : 28-Jul-2012
Creation Date : 28-Jul-2012

COLLECTING THE DATA

Sudipta Ganguly


web Designer at **Kavish** Technosoft Pvt.Ltd

Bardhaman Area, India | Outsourcing/Offshoring

Send Sudipta an InMail



1
connection

 in.linkedin.com/pub/sudipta-ganguly/3b/378/9a

Experience

web Designer

Kavish Technosoft Pvt.Ltd 

Privately Held; 501-1000 employees; Outsourcing/Offshoring industry

Currently holds this position

Contact Sudipta for:

- career opportunities
- new ventures
- expertise requests
- reference requests
- consulting offers
- job inquiries
- business deals
- getting back in touch

COLLECTING THE DATA

Domain Name: PCTECHNOCRAT.COM

Registrant:



Kavish Technosoft
Rohit Kayan (rohit.kayan@gmail.com)

2nd floor, Rays IT Park, EN-9
Sector 5, Salt Lake city,
Kolkata
West Bengal, 700091
IN
Tel. +91.9831067070

Creation Date: 05-Oct-2010

Expiration Date: 05-Oct-2013

Domain servers in listed order:

- 1.nseasy.com
- 2.nseasy.com


Administrative Contact:

Kavish Technosoft
Rohit Kayan (rohit.kayan@gmail.com)

2nd floor, Rays IT Park, EN-9
Sector 5, Salt Lake city,
Kolkata
West Bengal, 700091
IN
Tel. +91.9831067070

COLLECTING THE DATA

```
121         <script language="javascript">
122 <!--//
123 /*This Script allows people to enter by using a form that asks for a
124 UserID and Password*/
125 function pasuser(form) {
126 if (form.id.value=="pctechnocrat") {
127 if (form.pass.value=="kavish") {
128 location="plans & products.html"
129 } else {
130 alert("Invalid Password")
131 }
132 } else { alert("Invalid UserID")
133 }
134 }
135 //-->
136 </script>
137
```



SUMMARY

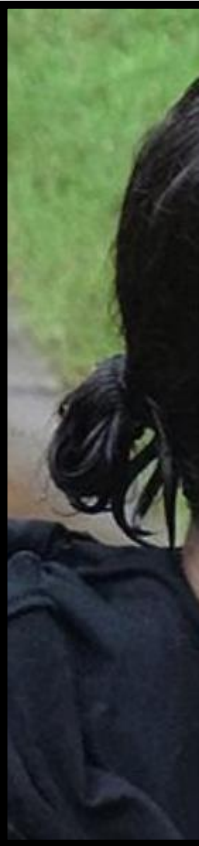
- **PayPal Accounts**
 - ddkcare@gmail.com

MORE INFORMATION WAS SHARED WITH
LAW ENFORCEMENT

- Rohit Kayan
- **Company**
 - Kavish Technosoft

CONCLUSION

CONCLUSION



CONCLUSION



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Protecting America's Consumers

Home News Competition Consumer Protection Economics General Counsel Actions Congressional Policy International
About Public Affairs Public Events Speeches Webcasts Reporter Resources Noticias en Español

For Release: 10/03/2012

FTC Halts Massive Tech Support Scams

Tens of Thousands of Consumers Allegedly Tricked Into Paying for Removal of Bogus Viruses and Non-Existent Spyware, and Allowing Scammers to Remotely Access their Computers

The Federal Trade Commission has launched a major international crackdown on tech support scams in which telemarketers masquerade as major computer companies, con consumers into believing that their computers are riddled with viruses, spyware and other malware, and then charge hundreds of dollars to remotely access and "fix" the consumers' computers.

At the request of the FTC, a U.S. District Court Judge has *ordered* a halt to six alleged tech support scams pending further hearings, and has frozen their assets.

"The FTC has been aggressive – and successful – in its pursuit of tech support scams," said FTC Chairman Jon Leibowitz. "And the tech support scam artists we are talking about today have taken scareware to a whole other level of virtual mayhem."

E-mail this News Release
If you send this link to someone else, the FTC will not collect any personal information about you or the recipient.

Related Items:

Watch Press Conference

Federal Trade Commission, Plaintiff, v. Pecon Software Ltd., also doing business as Pecon Services LLC, Pecon Services, Inc.; Pecon Infotech Ltd.; Pecon Software UK Ltd.; Mahesh Kumar Shah, also known as MK Shah; Prateek Shah; Sujoy Roy; Zulfiquar Ali; and Vikas Kumar Gupta, Defendants
(United States District Court for the Southern District of New York)
Case No. 12 CIV 7186
FTC File No. 1223118

Federal Trade Commission, Plaintiff, v. PCare247 Inc.; PC Care247 Solutions Private Limited; Connexions Infotech Inc.; Connexions IT Services Private Limited, also doing business as Connexions InfoTech Services Pvt. Ltd.; Vikas Agrawal, also known as Vikas Agarwal; Navin Pasari; Anuj Agrawal; Sanjay Agarwalla; and Parmeshwar Agrawal, Defendants
(United States District Court for the Southern District of New York)
Case No. 12 CIV 7189
FTC File No. 1223243

Federal Trade Commission, Plaintiff, v. Zeal IT Solutions Pvt Ltd. and Kishore Ghosh,

Chairman Jon Leibowitz announces a major international crackdown on tech support scams at a press conference Oct. 3 2012 at the Federal Trade Commission in Washington, DC.

KASPERSKY Lab

THANK YOU

David Jacoby

Senior Security Researcher, Kaspersky Lab

