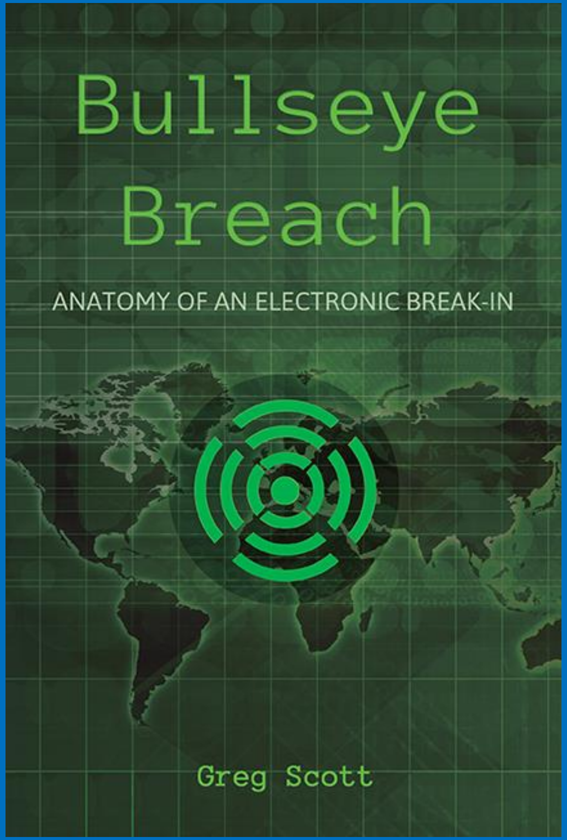
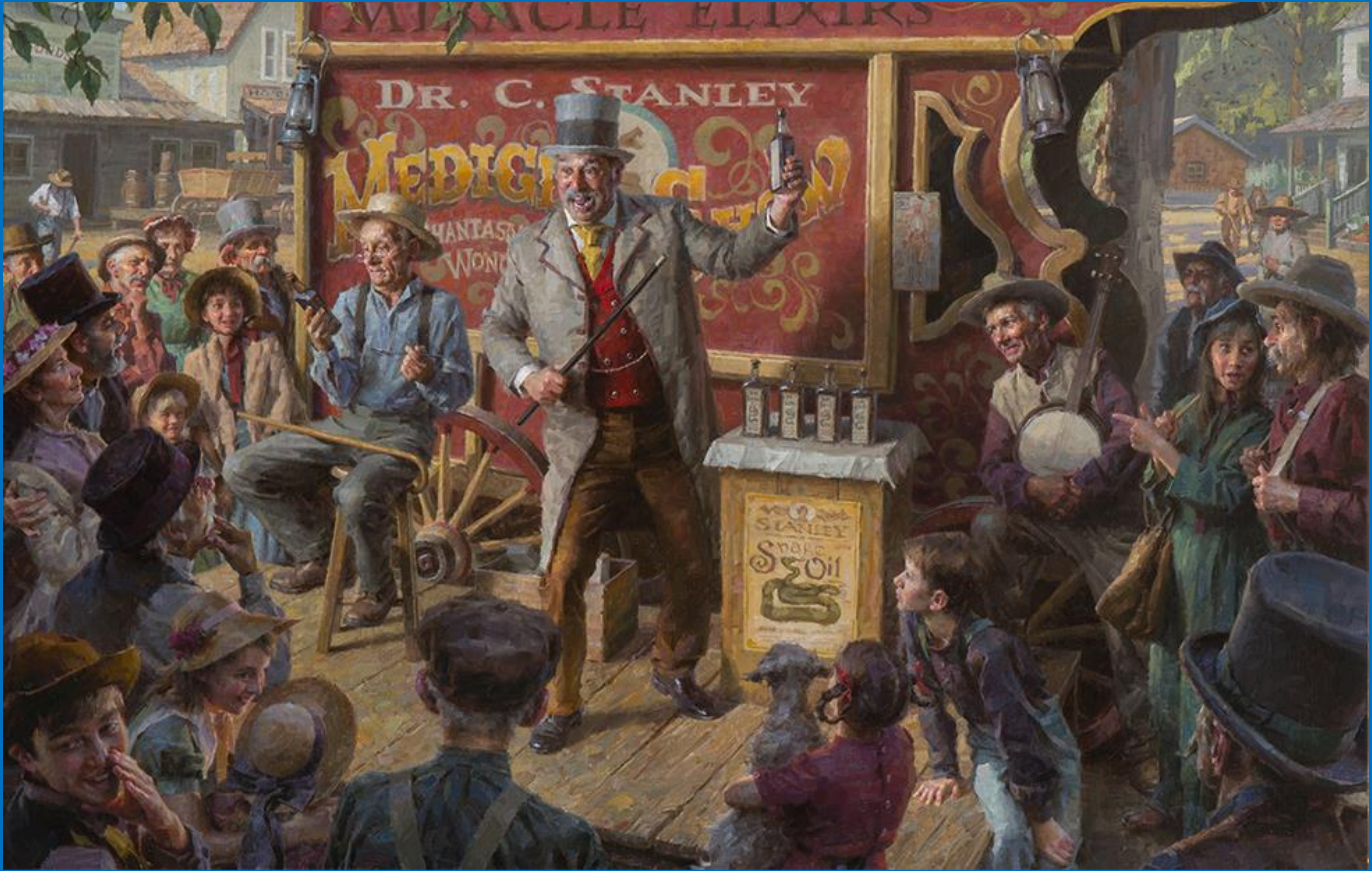
A few common Internet attacks



Greg Scott



Different century

Same snake oil

Image from http://www.morganweistling.com/images/2015/WEISTLING_FINAL_REVISE_FOR_ADS_SNAKE_OIL_SALESMAN.jpg

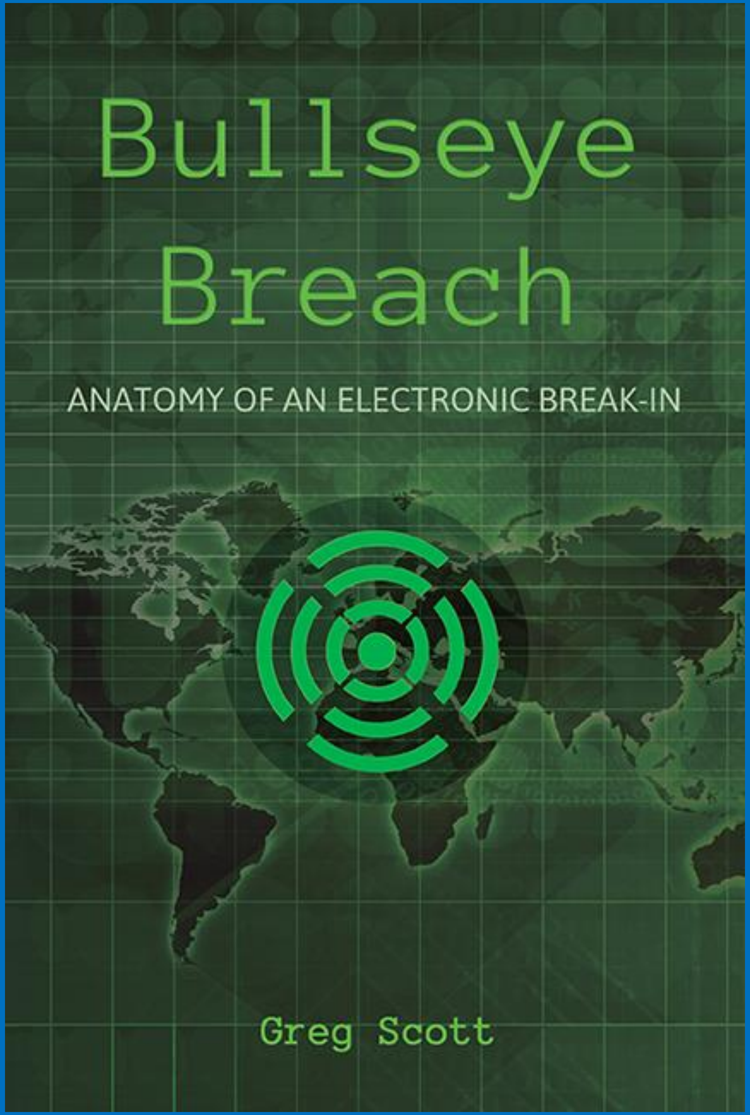
Only now we call it “social engineering.”

A great definition:

- Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information.
    - See https://en.wikipedia.org/wiki/Social_engineering_(security)

- By far the number one threat to our privacy.
- Social engineering nailed the IT Department in my *Bullseye Breach* fictional world.
- And it nailed several organizations in the real world.

Social engineering tactics helped steal millions of credit cards in my fictional world.



It’s behind nearly all the sensational data breaches in the real world.

How does 21st century social engineering work?

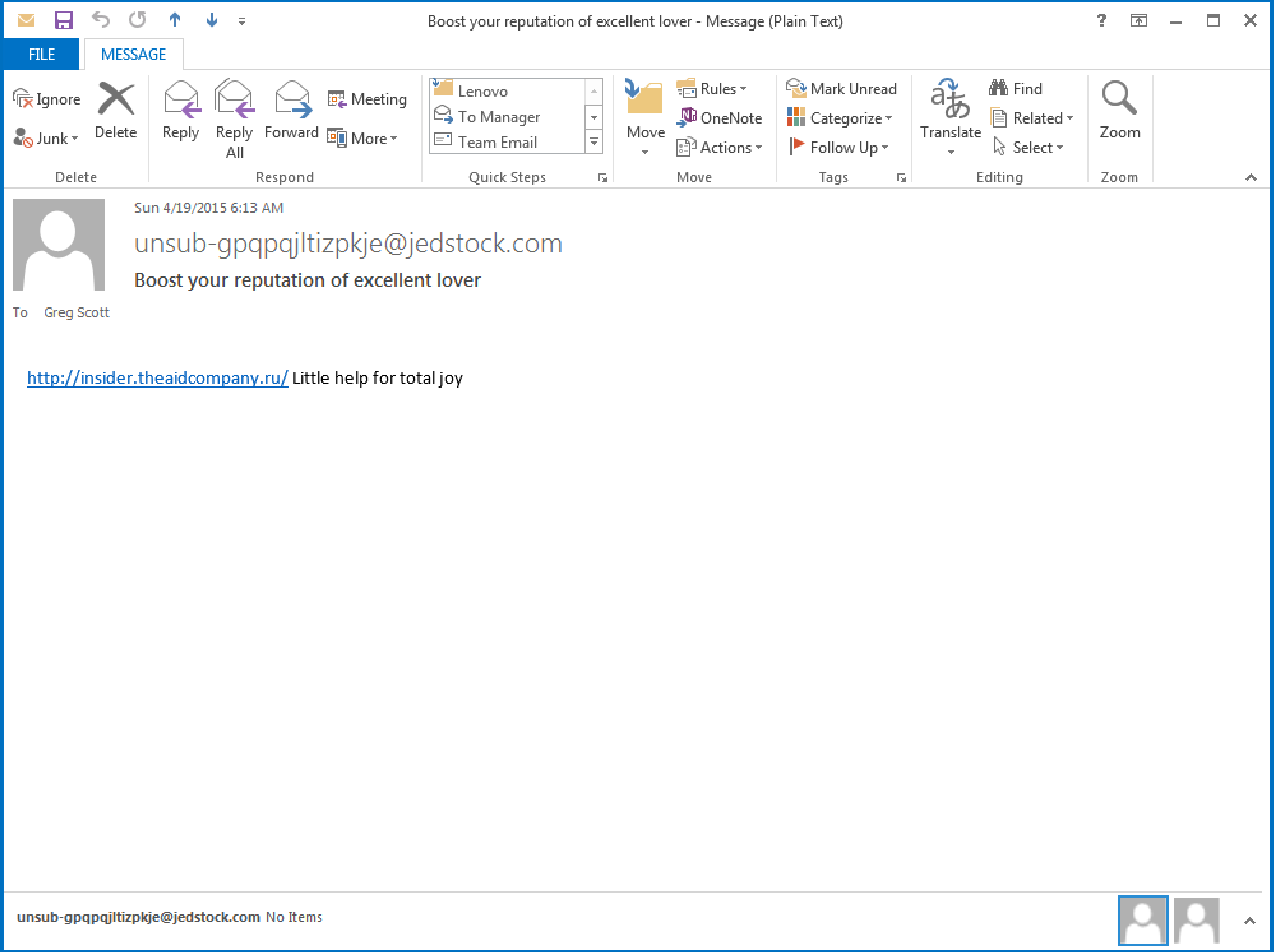
Hi Amy,
This is Joe, from IT...I'm working from home today...

Phishing attack

- In a typical large scale phishing attack, an evil intruder named Trudy sends a mass email to potential victims with the hope that victims will open a malware attachment or access the wrong website.

- In a spear phishing attack, Trudy does homework on potential victim Alice and tailors her email to Alice's unique tastes.
  - If Alice is a victim of the US Government Office of Personnel Management data breach, Trudy might tailor her email to mimic the "click here" OPM email.
  - Alice thinks the email directs her to an OPM website to set up her free credit monitoring
  - But Alice really goes to Trudy's evil website designed to steal Alice's banking info.

A typical “phishy” spam email



Sun 4/19/2015 6:13 AM

unsub-gpqpqjltizpkje@jedstock.com

Boost your reputation of excellent lover

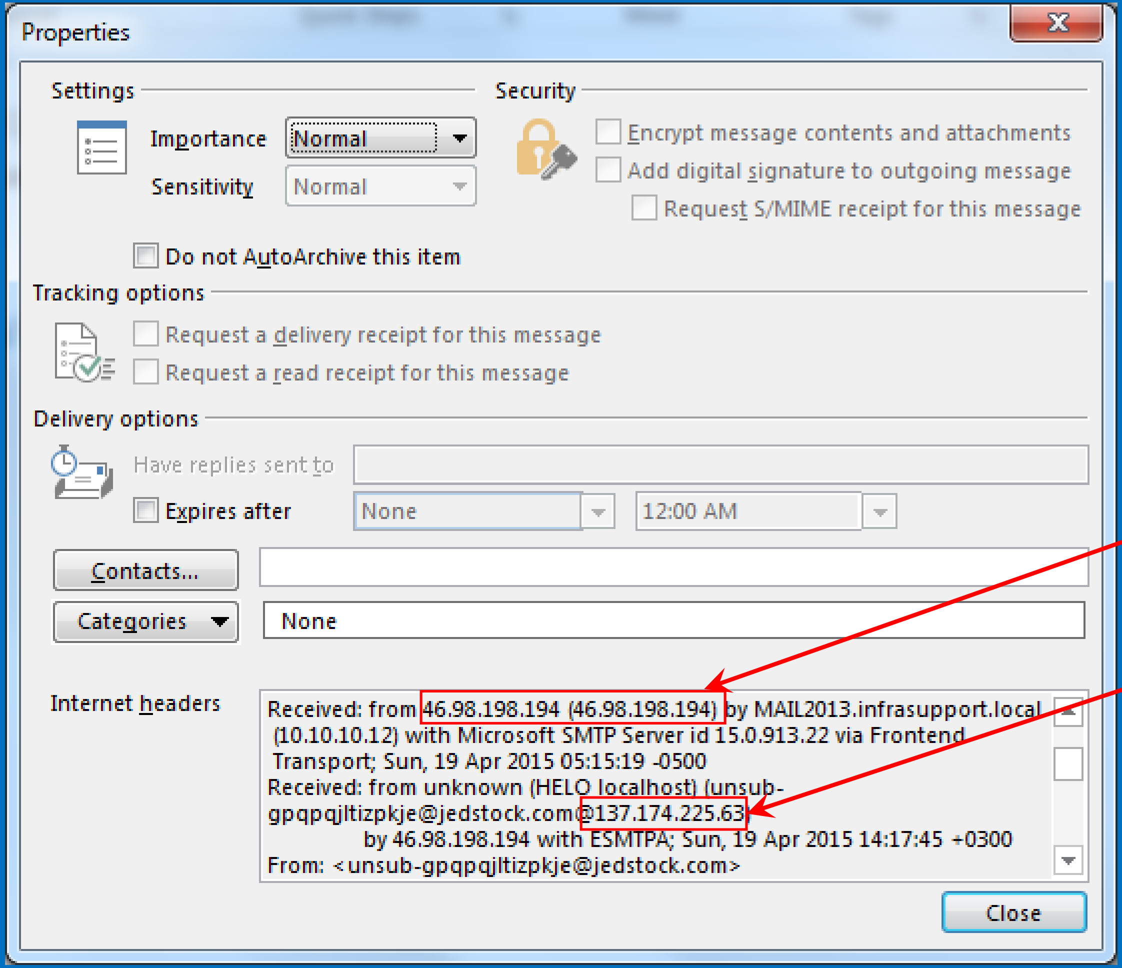
To Greg Scott

http://insider.theaidcompany.ru/ Little help for total joy

unsub-gpqpqjltizpkje@jedstock.com No Items

- This one is easy to spot from its clumsy content.
- But how would you find out where it really came from?

Click File...Properties



Importance: Normal

Sensitivity: Normal

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request S/MIME receipt for this message

□ Do not AutoArchive this item

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Have replies sent to

□ Expires after: None 12:00 AM

Categories: None

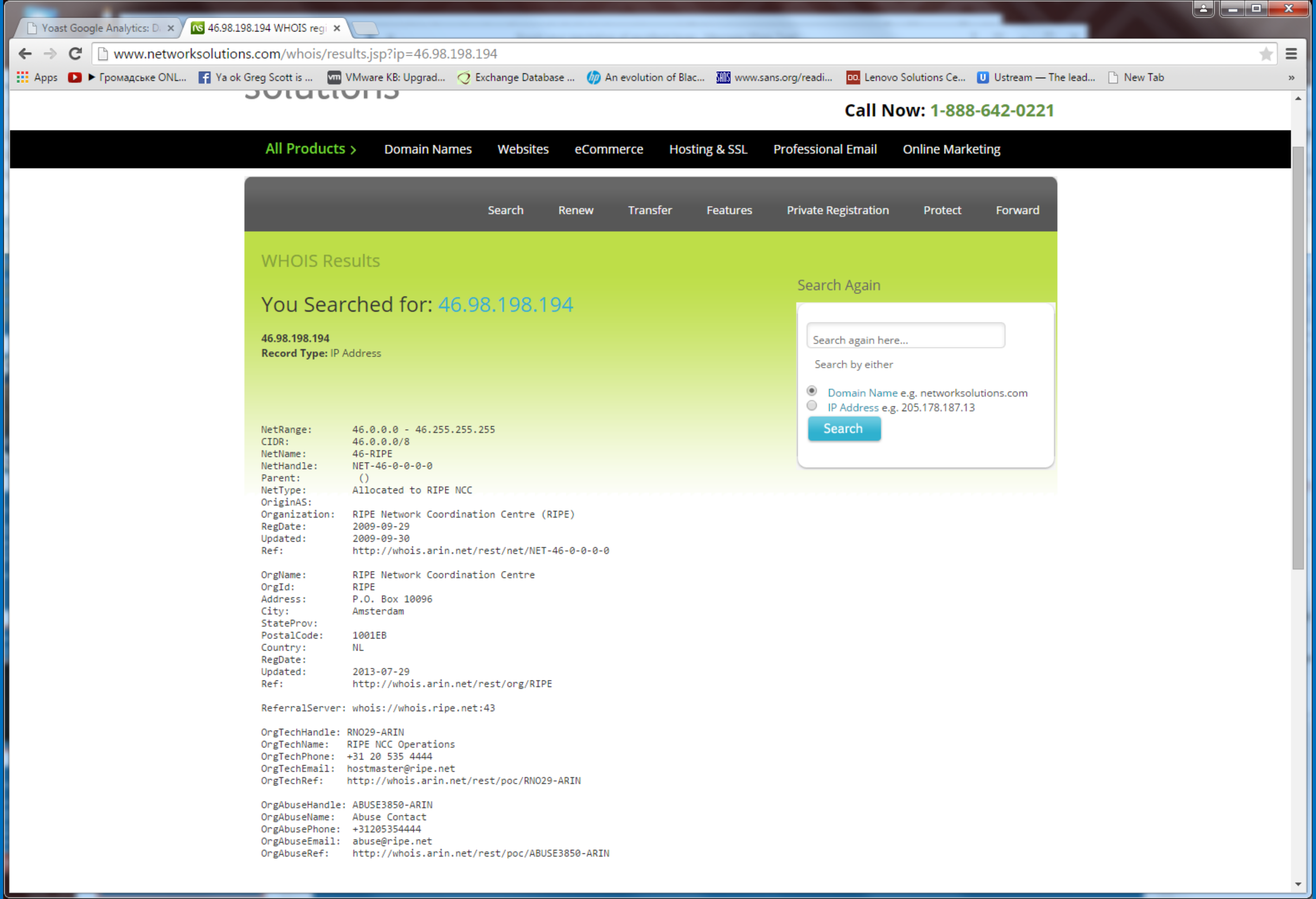
Internet headers:

```
Received: from 46.98.198.194 (46.98.198.194) by MAIL2013.infrasupport.local
 (10.10.10.12) with Microsoft SMTP Server id 15.0.913.22 via Frontend
 Transport; Sun, 19 Apr 2015 05:15:19 -0500
Received: from unknown (HELO localhost) (unsub-
gpqpqjltizpkje@jedstock.com@137.174.225.63)
          by 46.98.198.194 with ESMTPA; Sun, 19 Apr 2015 14:17:45 +0300
From: <unsub-gpqpqjltizpkje@jedstock.com>
```

Look at the email header

Where did it really come from?

Use a whois lookup to find out who owns the sending IP Address



Call Now: 1-888-642-0221

WHOIS Results

You Searched for: 46.98.198.194

46.98.198.194
Record Type: IP Address

```
NetRange:       46.0.0.0 - 46.255.255.255
CIDR:           46.0.0.0/8
NetName:        46-RIPE
NetHandle:      NET-46-0-0-0-0
Parent:          ()
NetType:        Allocated to RIPE NCC
OriginAS:
Organization:   RIPE Network Coordination Centre (RIPE)
RegDate:        2009-09-29
Updated:        2009-09-30
Ref:            http://whois.arin.net/rest/net/NET-46-0-0-0-0

OrgName:        RIPE Network Coordination Centre
OrgId:          RIPE
Address:        P.O. Box 10096
City:           Amsterdam
StateProv:
PostalCode:     1001EB
Country:        NL
RegDate:
Updated:        2013-07-29
Ref:            http://whois.arin.net/rest/org/RIPE

ReferralServer: whois://whois.ripe.net:43

OrgTechHandle: RNO29-ARIN
OrgTechName:   RIPE NCC Operations
OrgTechPhone:  +31 20 535 4444
OrgTechEmail:  hostmaster@ripe.net
OrgTechRef:    http://whois.arin.net/rest/poc/RNO29-ARIN

OrgAbuseHandle: ABUSE3850-ARIN
OrgAbuseName:   Abuse Contact
OrgAbusePhone:  +31205354444
OrgAbuseEmail:  abuse@ripe.net
OrgAbuseRef:    http://whois.arin.net/rest/poc/ABUSE3850-ARIN
```

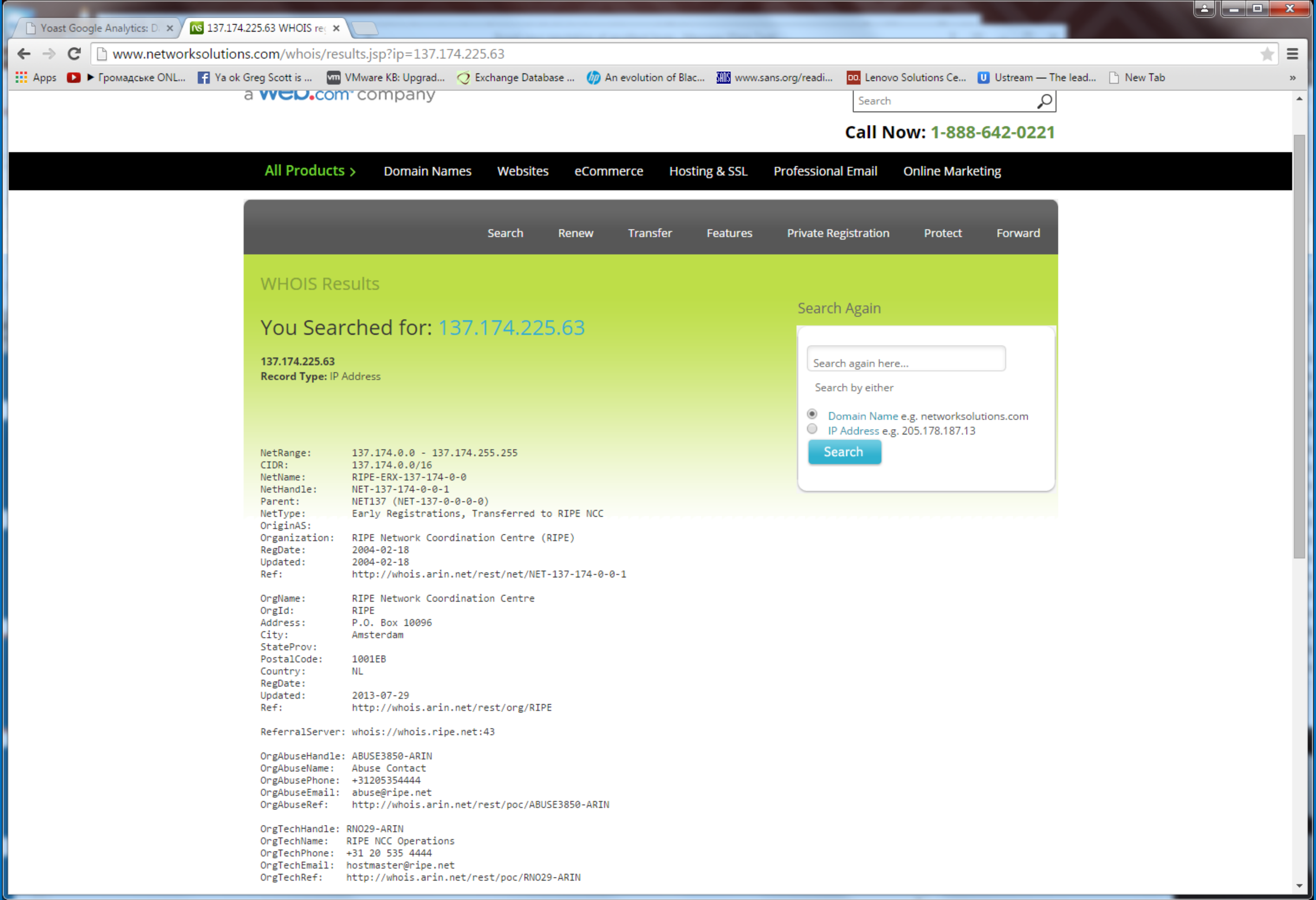
Search Again

Search again here...

Search by either

● Domain Name e.g. networksolutions.com
○ IP Address e.g. 205.178.187.13

Search



WHOIS Results

You Searched for: 137.174.225.63

137.174.225.63
Record Type: IP Address

Search Again

Search again here...

Search by either

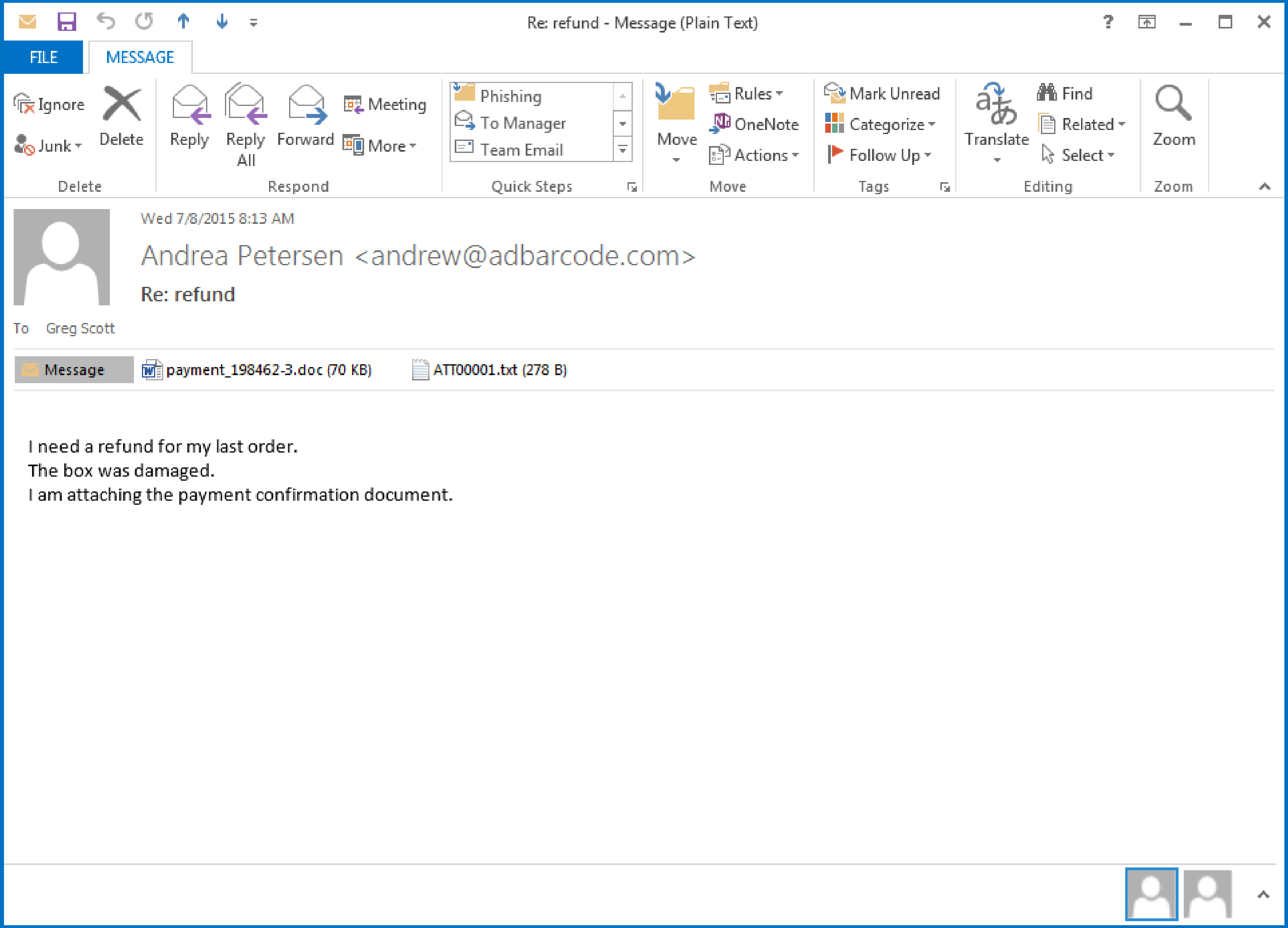
● Domain Name e.g. networksolutions.com
○ IP Address e.g. 205.178.187.13

Search

```
NetRange:       137.174.0.0 - 137.174.255.255
CIDR:           137.174.0.0/16
NetName:        RIPE-ERX-137-174-0-0
NetHandle:      NET-137-174-0-0-1
Parent:         NET137 (NET-137-0-0-0-0)
NetType:        Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:   RIPE Network Coordination Centre (RIPE)
RegDate:        2004-02-18
Updated:        2004-02-18
Ref:            http://whois.arin.net/rest/net/NET-137-174-0-0-1

OrgName:        RIPE Network Coordination Centre
OrgId:          RIPE
Address:        P.O. Box 10096
City:           Amsterdam
StateProv:
PostalCode:     1001EB
Country:        NL
RegDate:
Updated:        2013-07-29
Ref:            http://whois.arin.net/rest/org/RIPE

ReferralServer: whois://whois.ripe.net:43

OrgAbuseHandle: ABUSE3850-ARIN
OrgAbuseName:   Abuse Contact
OrgAbusePhone:  +31205354444
OrgAbuseEmail:  abuse@ripe.net
OrgAbuseRef:    http://whois.arin.net/rest/poc/ABUSE3850-ARIN

OrgTechHandle: RNO29-ARIN
OrgTechName:   RIPE NCC Operations
OrgTechPhone:  +31 20 535 4444
OrgTechEmail:  hostmaster@ripe.net
OrgTechRef:    http://whois.arin.net/rest/poc/RNO29-ARIN
```

This one started in the Netherlands and routed through Ukraine.

They're not always obvious to spot from content



Wed 7/8/2015 8:13 AM

Andrea Petersen <andrew@adbarcode.com>

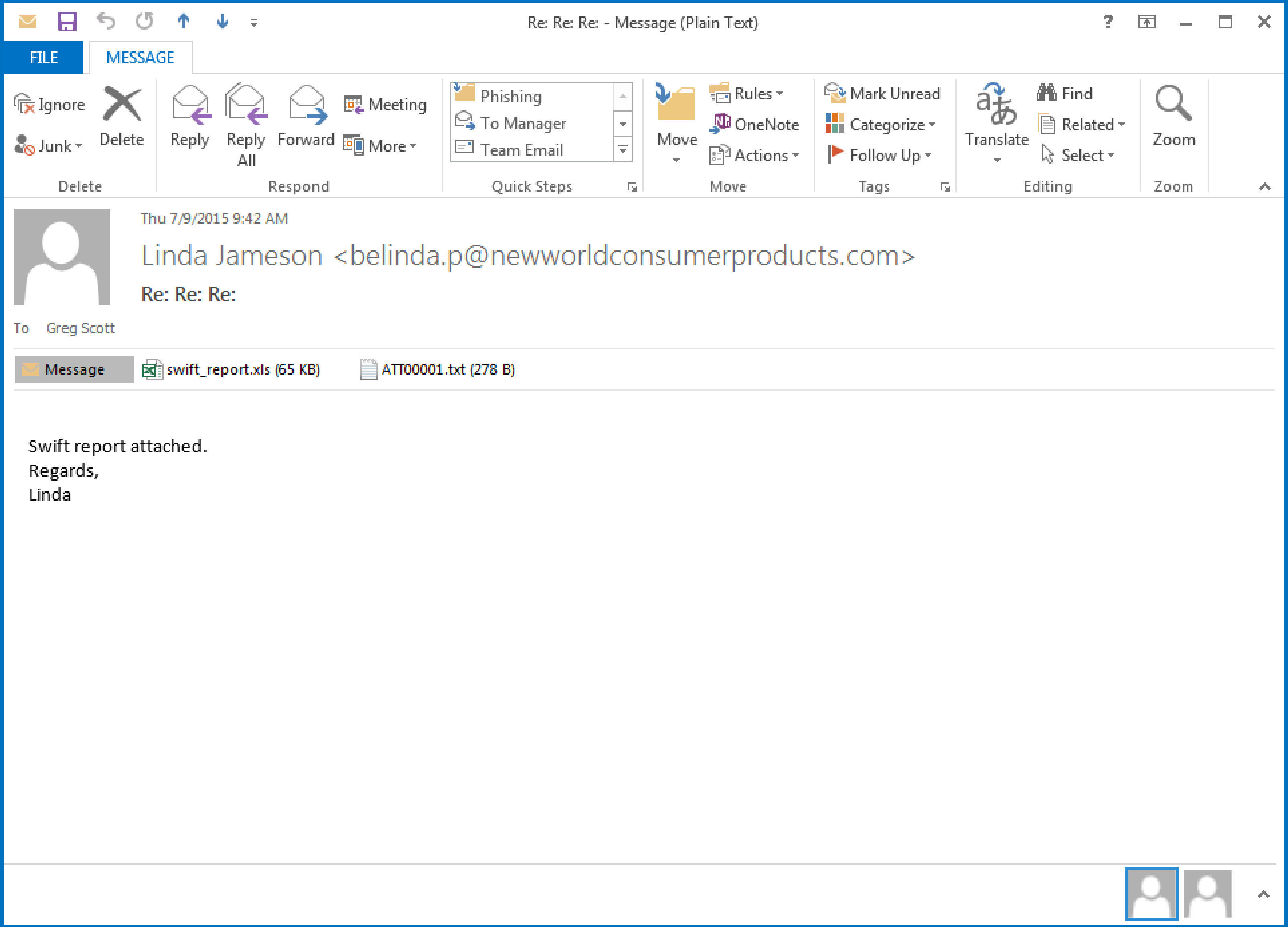
Re: refund

To Greg Scott

payment_198462-3.doc (70 KB) ATT00001.txt (278 B)

I need a refund for my last order.
The box was damaged.
I am attaching the payment confirmation document.

Here's another one aimed at the financial industry



Thu 7/9/2015 9:42 AM

Linda Jameson <belinda.p@newworldconsumerproducts.com>

Re: Re: Re:

To Greg Scott

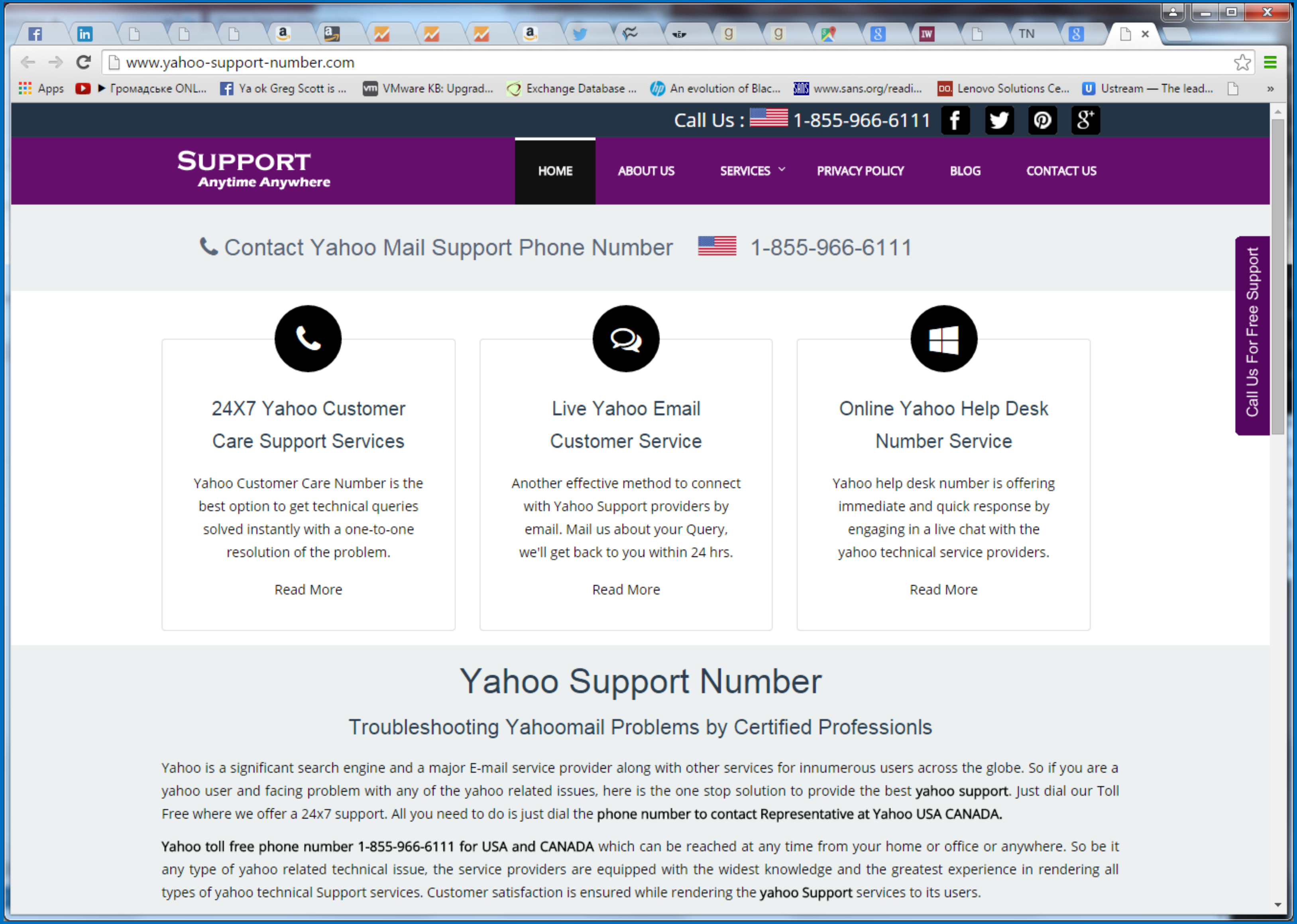
Message | swift_report.xls (65 KB) | ATT00001.txt (278 B)

Swift report attached.
Regards,
Linda

Watering hole attack

- Alice operates a website that everyone in Bob’s industry uses.
- Alice’s website has a zero day vulnerability. Or maybe Alice uses sloppy security practices.
  - Zero day – a software bug bad guys exploit that good guys haven’t found out about yet.
- Trudy exploits the vulnerability in Alice’s website and embeds an evil program.
- Bob accesses Alice’s website. Trudy’s content silently invades Bob’s computer.
- Trudy now owns Bob.

Fake tech support websites



Call Us : 1-855-966-6111

Contact Yahoo Mail Support Phone Number 1-855-966-6111

24X7 Yahoo Customer Care Support Services

Yahoo Customer Care Number is the best option to get technical queries solved instantly with a one-to-one resolution of the problem.

Live Yahoo Email Customer Service

Another effective method to connect with Yahoo Support providers by email. Mail us about your Query, we'll get back to you within 24 hrs.

Online Yahoo Help Desk Number Service

Yahoo help desk number is offering immediate and quick response by engaging in a live chat with the yahoo technical service providers.

Yahoo Support Number

Troubleshooting Yahoomail Problems by Certified Professionls

Yahoo is a significant search engine and a major E-mail service provider along with other services for innumerous users across the globe. So if you are a yahoo user and facing problem with any of the yahoo related issues, here is the one stop solution to provide the best **yahoo support**. Just dial our Toll Free where we offer a 24x7 support. All you need to do is just dial the **phone number to contact Representative at Yahoo USA CANADA.**

Yahoo toll free phone number 1-855-966-6111 for USA and CANADA which can be reached at any time from your home or office or anywhere. So be it any type of yahoo related technical issue, the service providers are equipped with the widest knowledge and the greatest experience in rendering all types of yahoo technical Support services. Customer satisfaction is ensured while rendering the **yahoo Support** services to its users.

Post a question in a Yahoo support forum.

The reply sends you to a website with a toll free phone number.

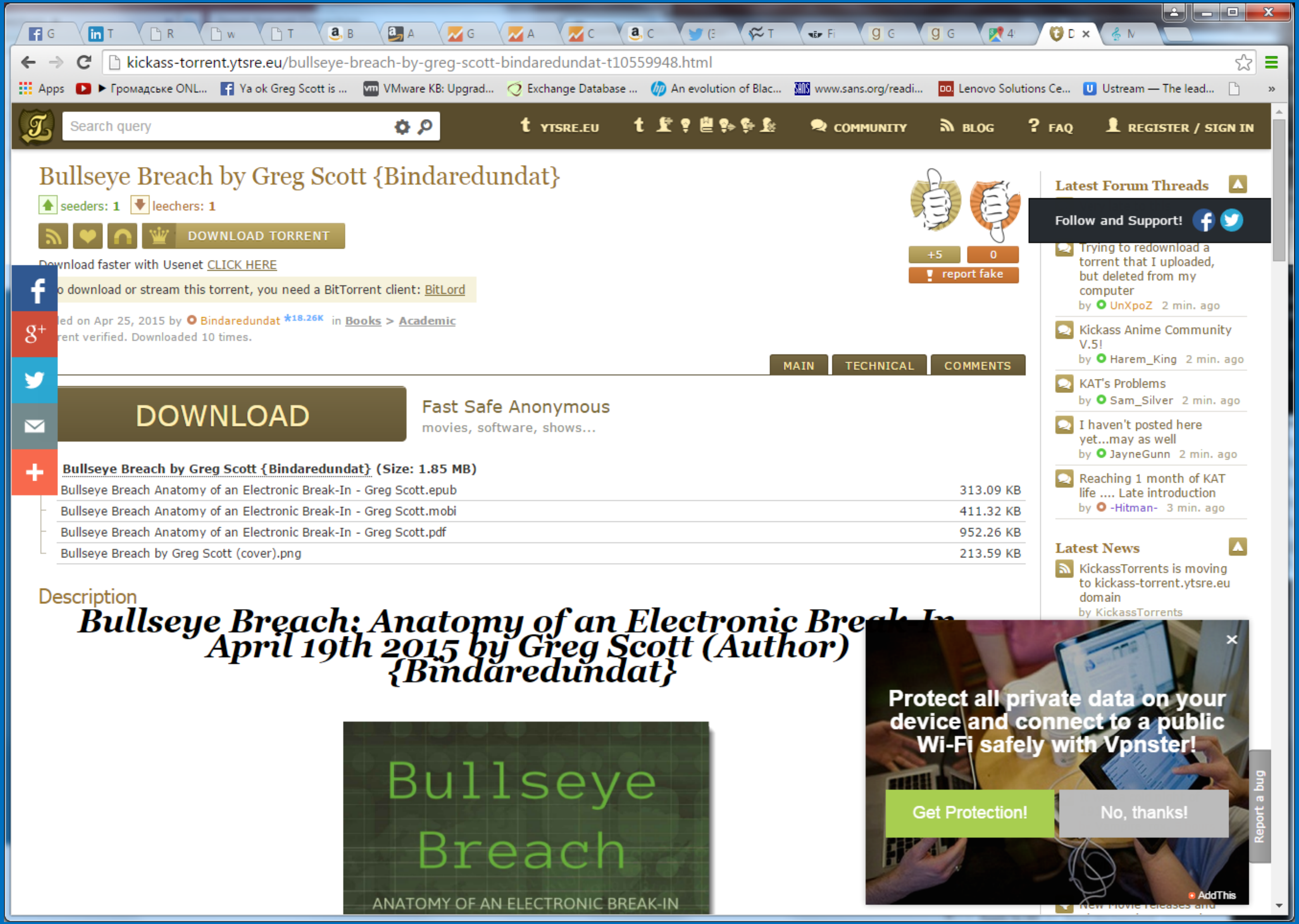
Call the number.

Grant permission for some bozo on the other side of the world to connect to your computer.

Give them your credit card number.

Now they own you.

Appeals to greed



kickass-torrent.ytsre.eu/bullseye-breach-by-greg-scott-bindaredundat-t10559948.html

Bullseye Breach by Greg Scott {Bindaredundat}

seeders: 1 leechers: 1

Download faster with Usenet CLICK HERE

o download or stream this torrent, you need a BitTorrent client: BitLord

led on Apr 25, 2015 by Bindaredundat *18.26K in Books > Academic
rent verified. Downloaded 10 times.

Fast Safe Anonymous
movies, software, shows...

Bullseye Breach by Greg Scott {Bindaredundat} (Size: 1.85 MB)

Bullseye Breach Anatomy of an Electronic Break-In - Greg Scott.epub	313.09 KB
Bullseye Breach Anatomy of an Electronic Break-In - Greg Scott.mobi	411.32 KB
Bullseye Breach Anatomy of an Electronic Break-In - Greg Scott.pdf	952.26 KB
Bullseye Breach by Greg Scott (cover).png	213.59 KB

Description

Bullseye Breach: Anatomy of an Electronic Break-In
April 19th 2015 by Greg Scott (Author)
{Bindaredundat}

Bullseye Breach
ANATOMY OF AN ELECTRONIC BREAK-IN

Latest Forum Threads

Trying to redownload a torrent that I uploaded, but deleted from my computer
by UnXpoZ 2 min. ago

Kickass Anime Community V.5!
by Harem_King 2 min. ago

KAT's Problems
by Sam_Silver 2 min. ago

I haven't posted here yet...may as well
by JayneGunn 2 min. ago

Reaching 1 month of KAT life .... Late introduction
by -Hitman- 3 min. ago

Latest News

KickassTorrents is moving to kickass-torrent.ytsre.eu domain
by KickassTorrents

Protect all private data on your device and connect to a public Wi-Fi safely with Vpnster!

Access this sleazy website that promises a free download of my book, *Bullseye Breach*.

Endure popup after popup promising all kinds of free junk.

Sooner or later, you'll see a popup claiming you have a virus. Or your flash player is out of date.

Go ahead – click on the link!

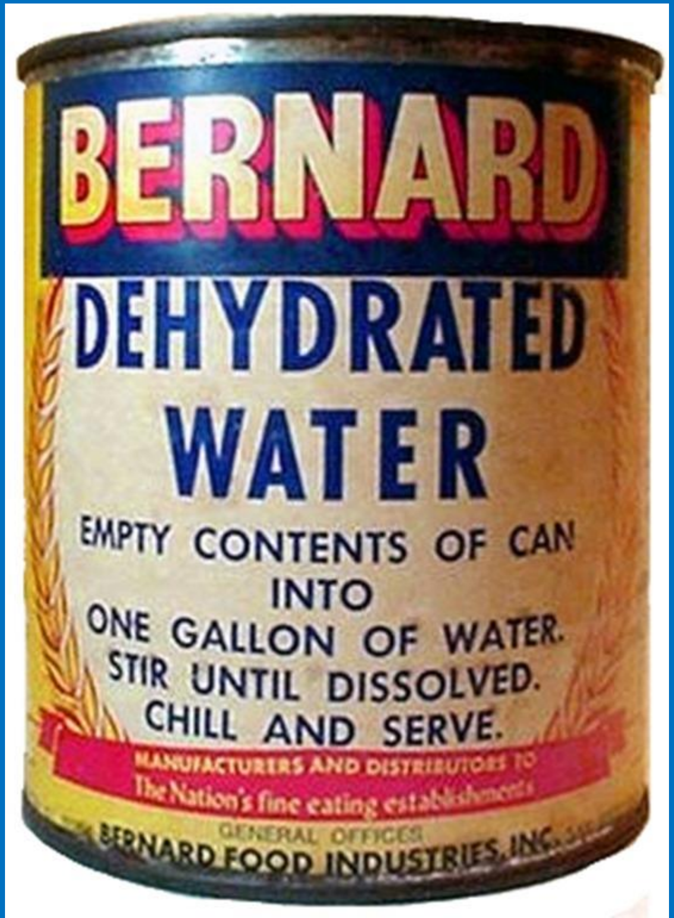
Use this device to identify your most powerful security weapon.

Instructions:

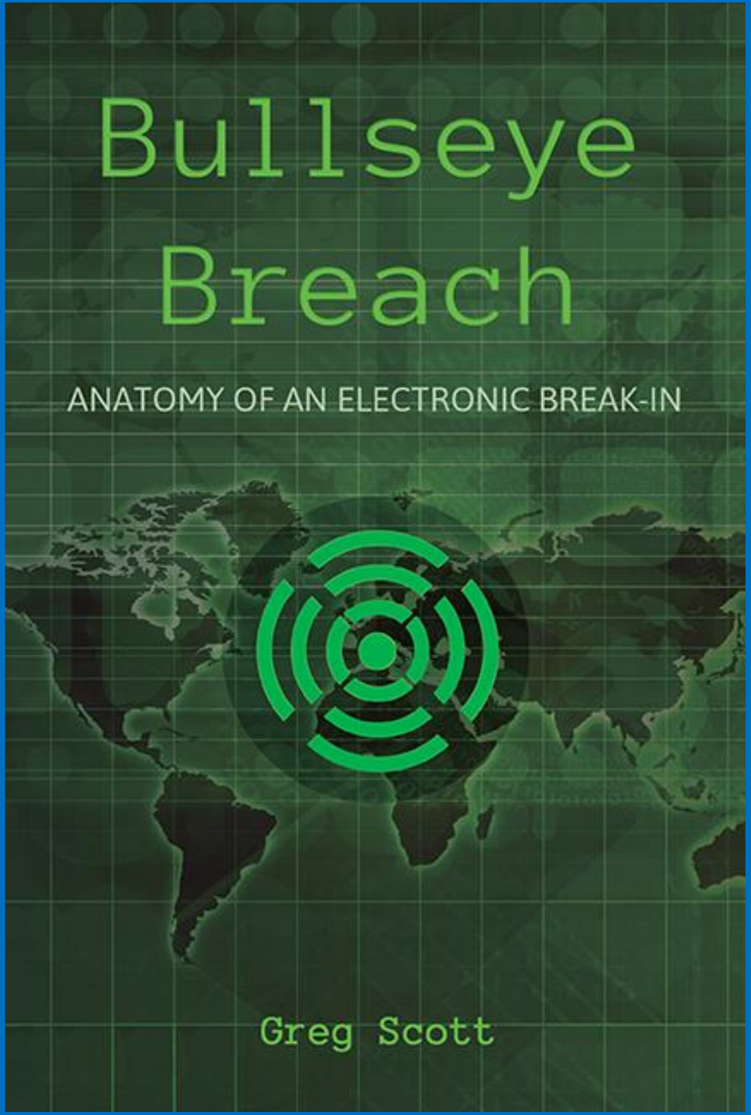
- Hold this device in front of you.
- Look inside.
- Gaze upon the most important weapon in your security arsenal.

- Exercise this weapon frequently.
- Keep it updated.
- Guard it jealously.
- Use it wisely.

Con games are alive and well today and live on the Internet



Buy your copy today!



Greg Scott – gregscott@infrasupport.com
Twitter: DGregScott
1 (651) 260-1051

Warning: Don't start reading until a Friday because you won't be able to put it down.

This gives you the weekend to recover from jet-lag after reading all night.

http://www.bullseyebreach.com