The Game Goes On:
An Analysis of Modern Spam Techniques

Ross Thomas, Dmitry Samosseiko, SophosLabs

Virus Bulletin, Montréal, October 2006

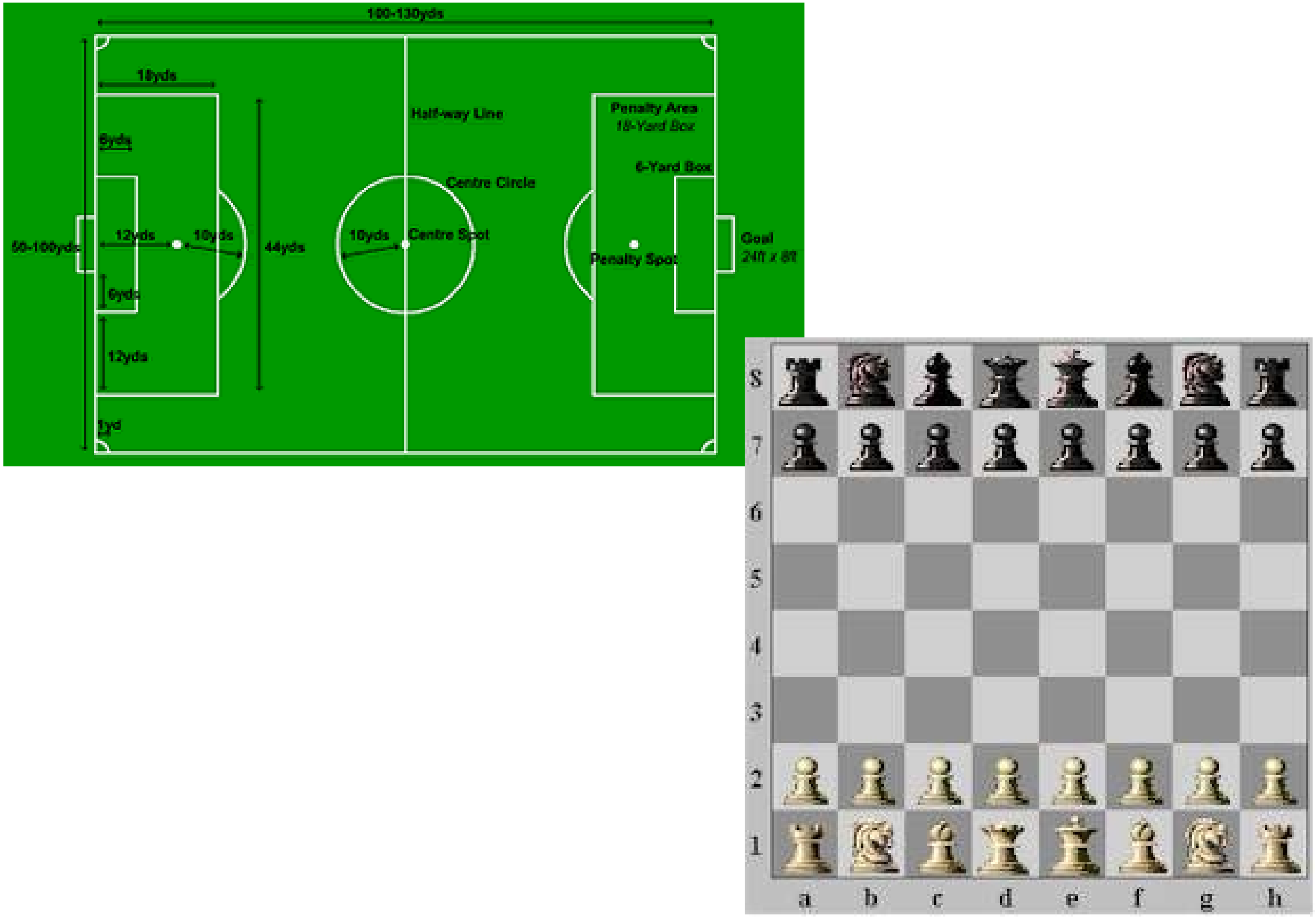
About…

Spam tricks (2006)

vs

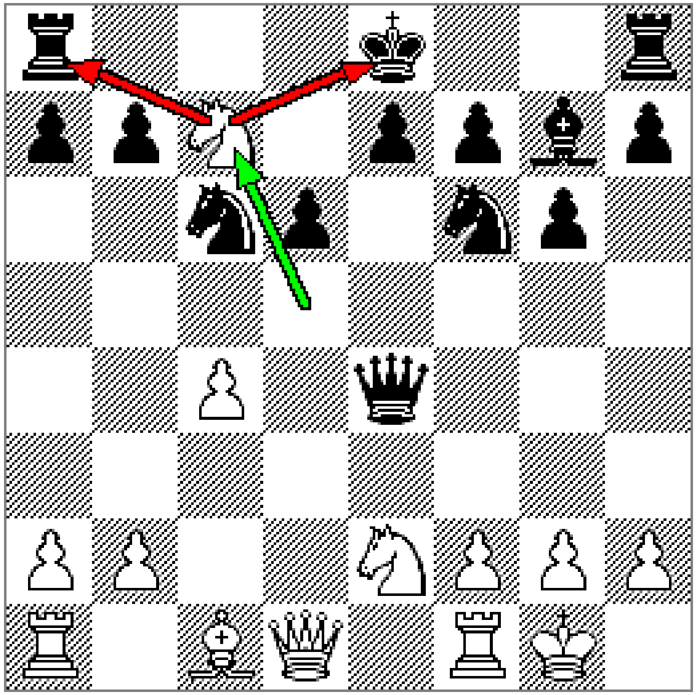
Filters fighting back

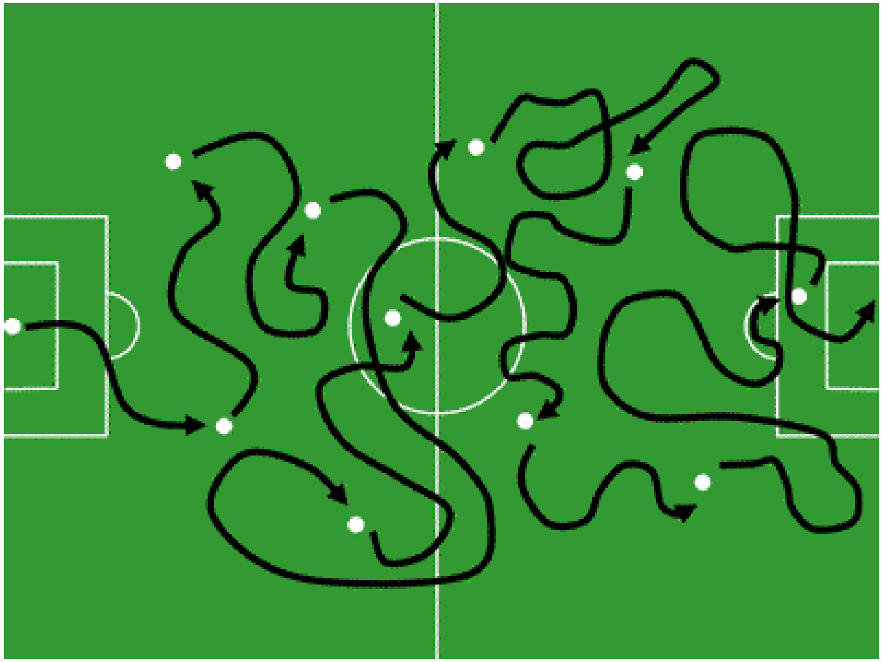
Most games have playing fields…



…and strategies

- Connection-level
- Content analysis





Filter “textbook” strategies

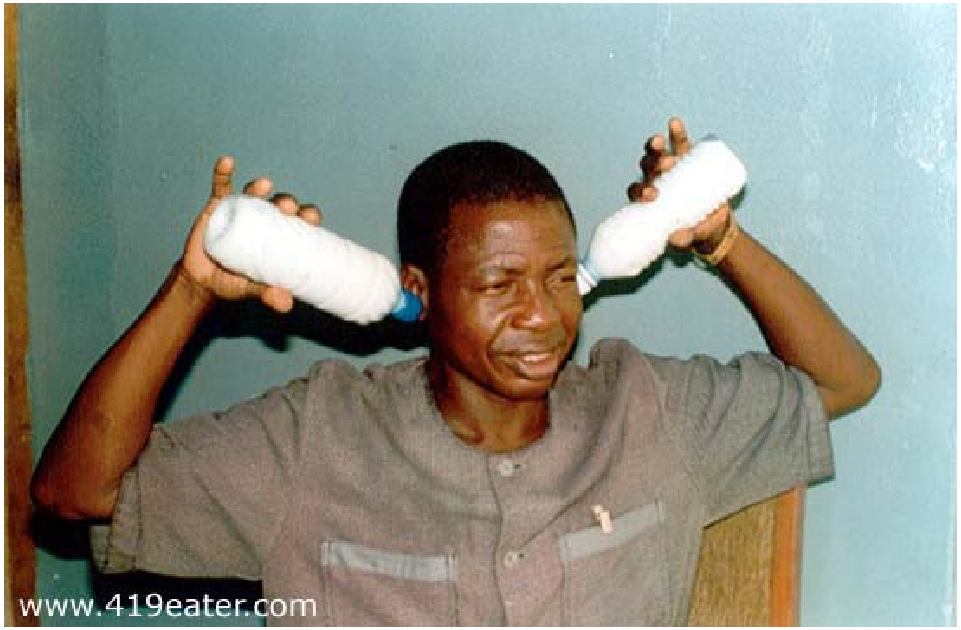
- Connection-level
  - Tracking spam sending networks/hosts (IP/domain blocking)
- Content
  - Checksums
  - Keywords heuristic
  - Call-to-action blocking (URLs, phone number, etc.)
  - Statistical analysis (Bayes, etc)
  - etc.

Classic spam tricks

- Connection-level
  - “Botnets”
  - Open relays
  - Exploited servers, PHP scripts, etc.
  - Exploited web mail systems
- Content
  - Content randomizations
  - URL rotation
  - Obfuscations

Connection

Nigerian scammers

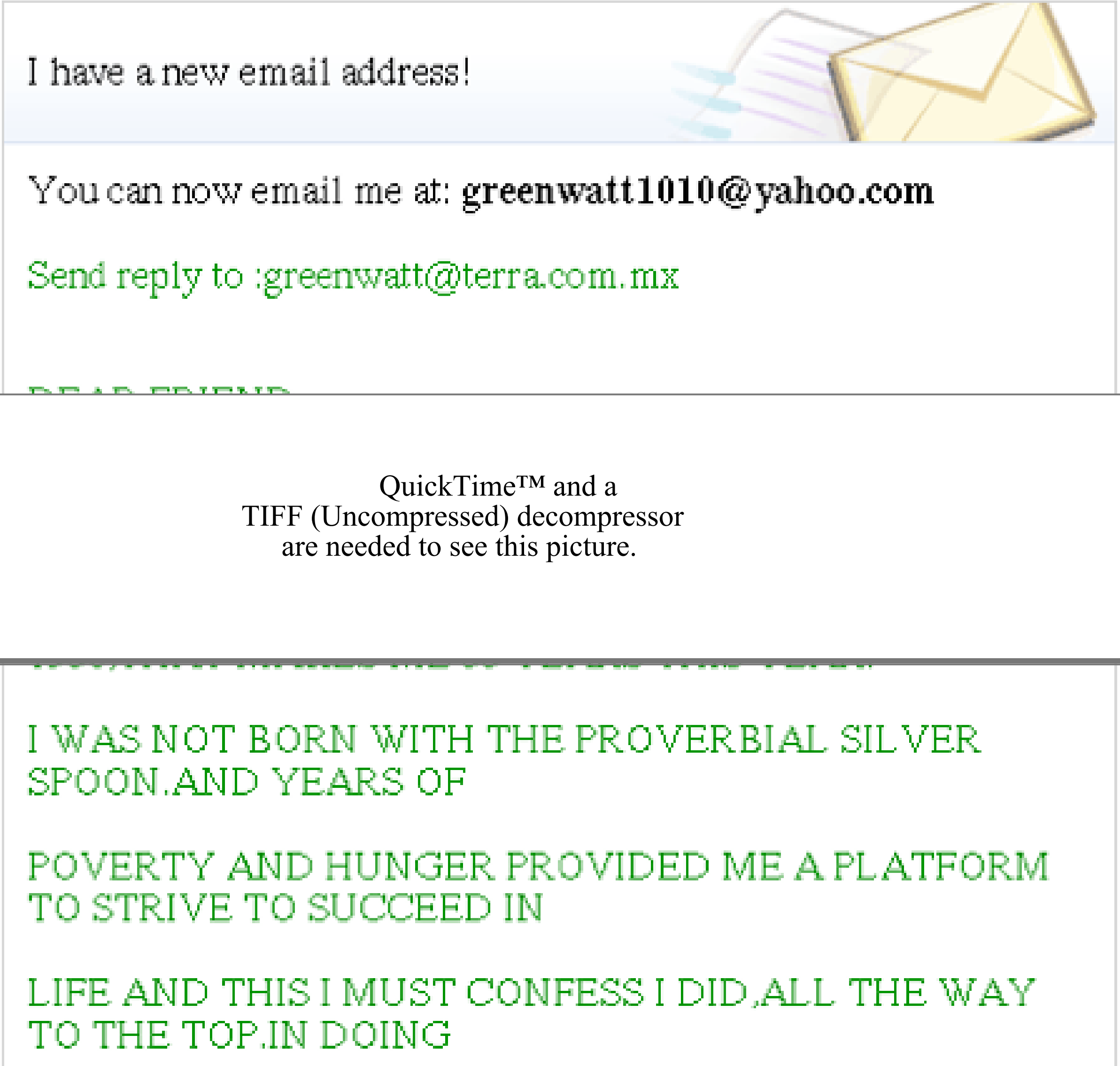


Exploiting web sites

Not limited to “hacking”

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Result



I have a new email address!

You can now email me at: **greenwatt1010@yahoo.com**

Send reply to :greenwatt@terra.com.mx

DEAR FRIEND

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

I WAS NOT BORN WITH THE PROVERBIAL SILVER SPOON.AND YEARS OF

POVERTY AND HUNGER PROVIDED ME A PLATFORM TO STRIVE TO SUCCEED IN

LIFE AND THIS I MUST CONFESS I DID,ALL THE WAY TO THE TOP.IN DOING

Content

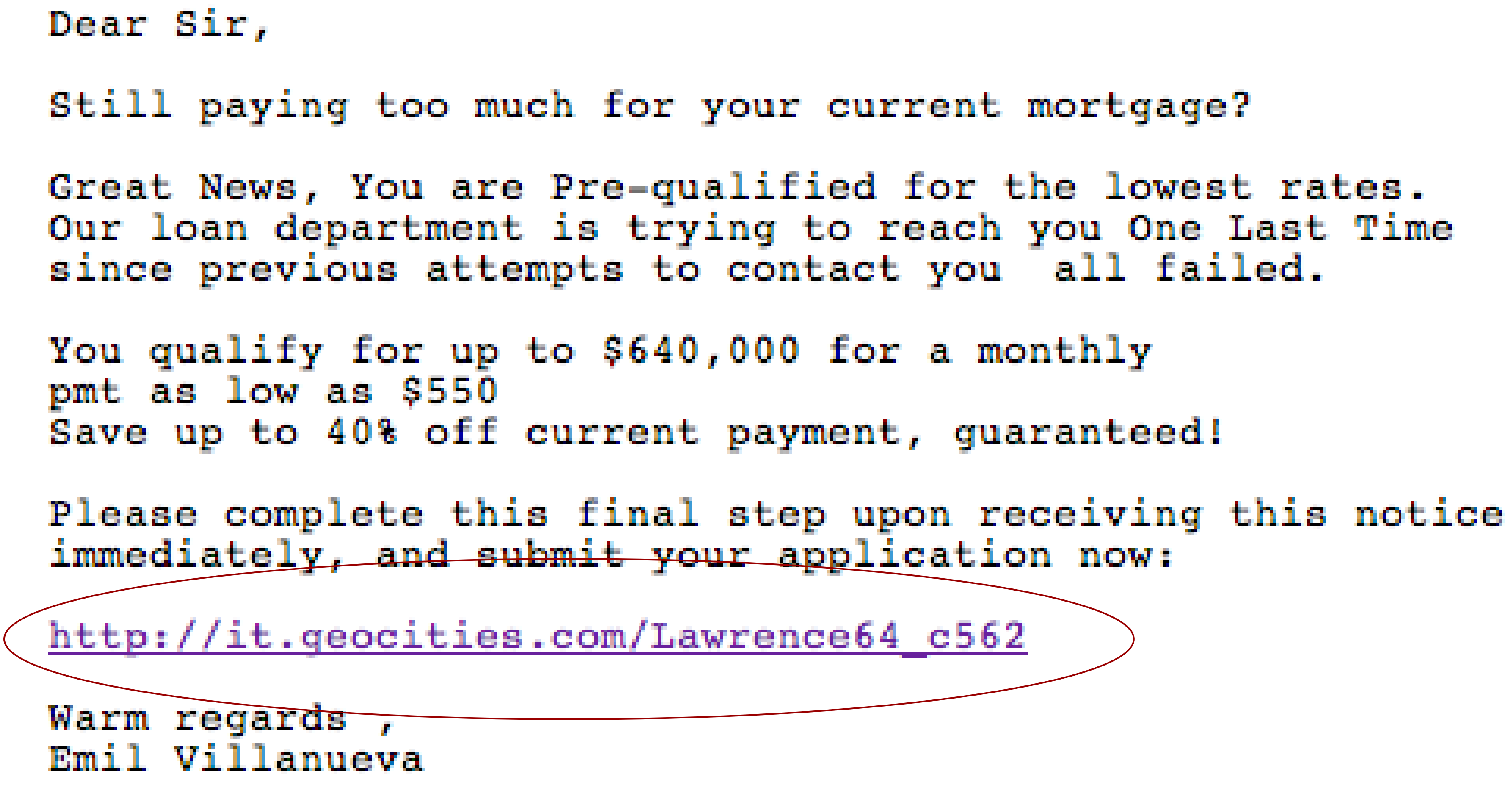
URL blocking

- SophosLabs' own URL list blocks up to 90% of spam
- Public services like SURBL work very well

URL tricks

- Using free web hosting sites as redirectors
- URL shortening services
- Blogs

Geocities abuse example



Dear Sir,

Still paying too much for your current mortgage?

Great News, You are Pre-qualified for the lowest rates.
Our loan department is trying to reach you One Last Time
since previous attempts to contact you all failed.

You qualify for up to $640,000 for a monthly
pmt as low as $550
Save up to 40% off current payment, guaranteed!

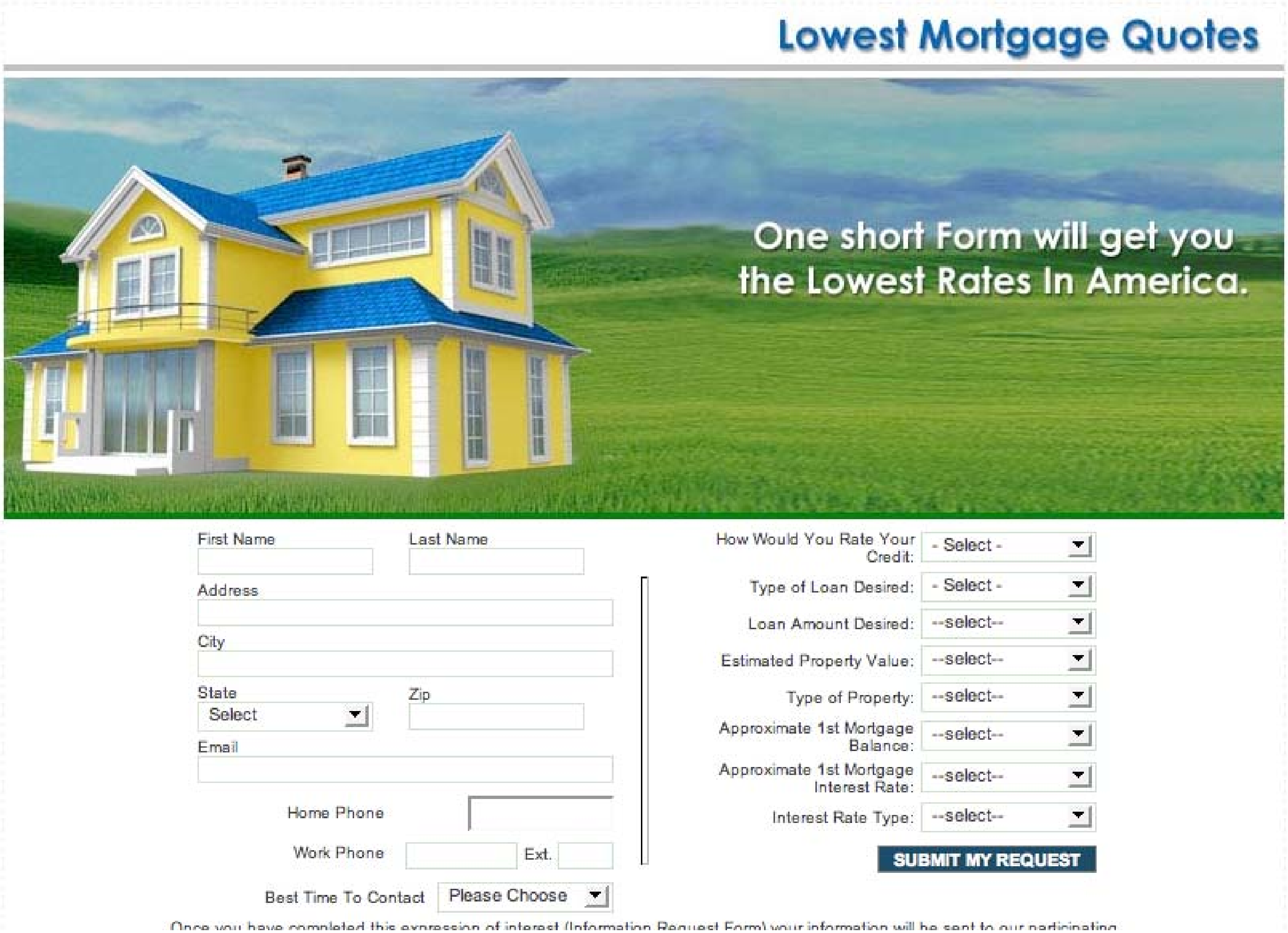
Please complete this final step upon receiving this notice
immediately, and submit your application now:

http://it.geocities.com/Lawrence64_c562

Warm regards ,
Emil Villanueva

```
<SCRIPT language="JavaScript">
function reportSpam()
{
alert('Thank you for your report\nWe will look further into it\n');
}
function continueToSite()
{
window.location.href=" http://www4.coreagousss.com";
}

</SCRIPT>
<body bgcolor="FFFFFF" onLoad=continueToSite()>
```



Lowest Mortgage Quotes

One short Form will get you the Lowest Rates In America.

First Name

Last Name

Address

City

State: Select

Zip

Email

Home Phone

Work Phone Ext.

Best Time To Contact: Please Choose

How Would You Rate Your Credit: - Select -

Type of Loan Desired: - Select -

Loan Amount Desired: --select--

Estimated Property Value: --select--

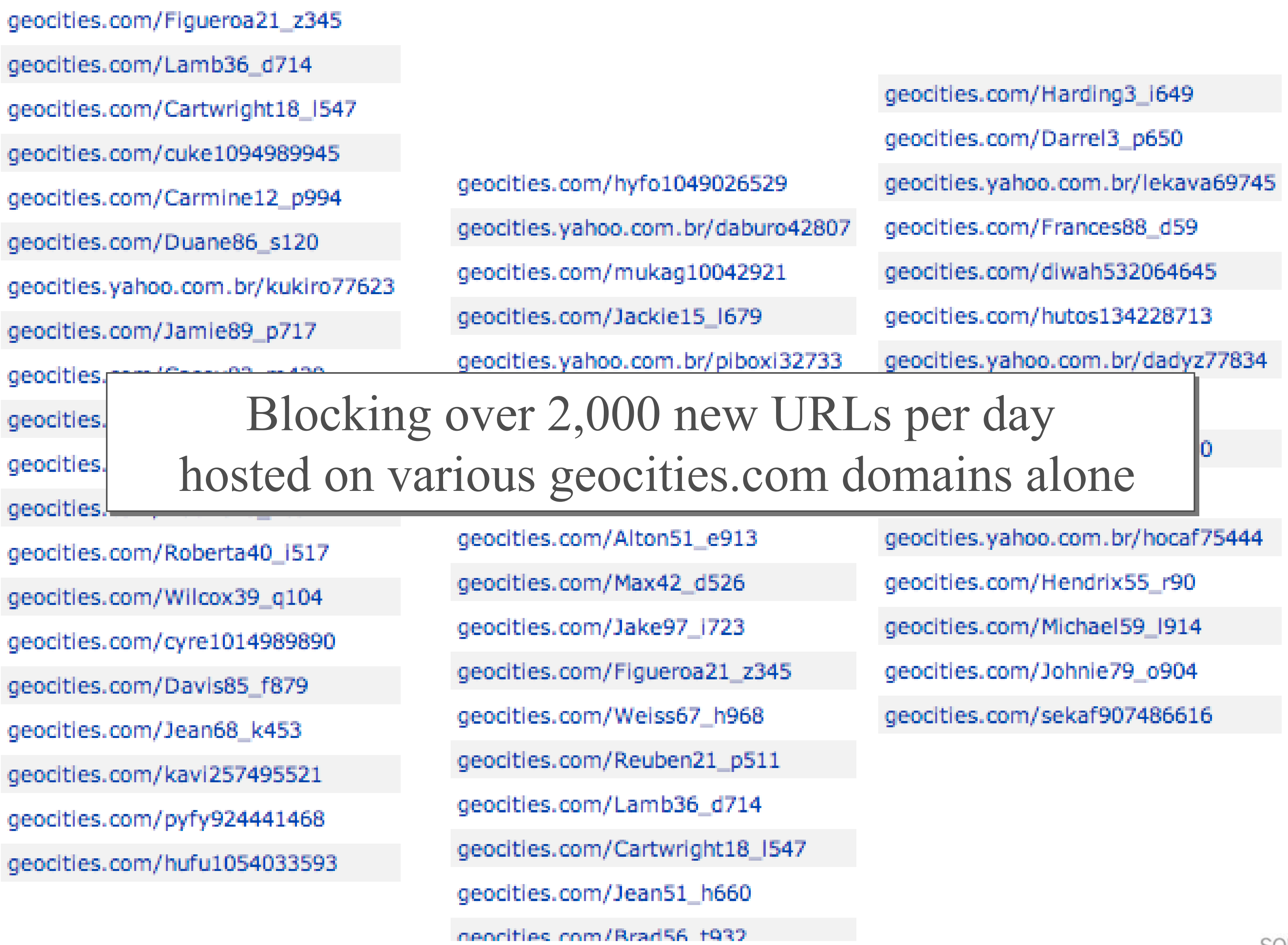
Type of Property: --select--

Approximate 1st Mortgage Balance: --select--

Approximate 1st Mortgage Interest Rate: --select--

Interest Rate Type: --select--

Once you have completed this expression of interest (Information Request Form) your information will be sent to our participating



geocities.com/Figueroa21_z345

geocities.com/Lamb36_d714

geocities.com/Cartwright18_l547

geocities.com/cuke1094989945

geocities.com/Carmine12_p994

geocities.com/Duane86_s120

geocities.yahoo.com.br/kukiro77623

geocities.com/Jamie89_p717

geocities.

geocities.

geocities.

geocities.

geocities.com/Roberta40_l517

geocities.com/Wilcox39_q104

geocities.com/cyre1014989890

geocities.com/Davis85_f879

geocities.com/Jean68_k453

geocities.com/kavi257495521

geocities.com/pyfy924441468

geocities.com/hufu1054033593

geocities.com/hyfo1049026529

geocities.yahoo.com.br/daburo42807

geocities.com/mukag10042921

geocities.com/Jackie15_l679

geocities.yahoo.com.br/piboxi32733

geocities.com/Alton51_e913

geocities.com/Max42_d526

geocities.com/Jake97_l723

geocities.com/Figueroa21_z345

geocities.com/Weiss67_h968

geocities.com/Reuben21_p511

geocities.com/Lamb36_d714

geocities.com/Cartwright18_l547

geocities.com/Jean51_h660

geocities.com/Brad56_t932

geocities.com/Harding3_l649

geocities.com/Darrel3_p650

geocities.yahoo.com.br/lekava69745

geocities.com/Frances88_d59

geocities.com/diwah532064645

geocities.com/hutos134228713

geocities.yahoo.com.br/dadyz77834

0

geocities.yahoo.com.br/hocaf75444

geocities.com/Hendrix55_r90

geocities.com/Michael59_l914

geocities.com/Johnie79_o904

geocities.com/sekaf907486616

Blocking over 2,000 new URLs per day
hosted on various geocities.com domains alone

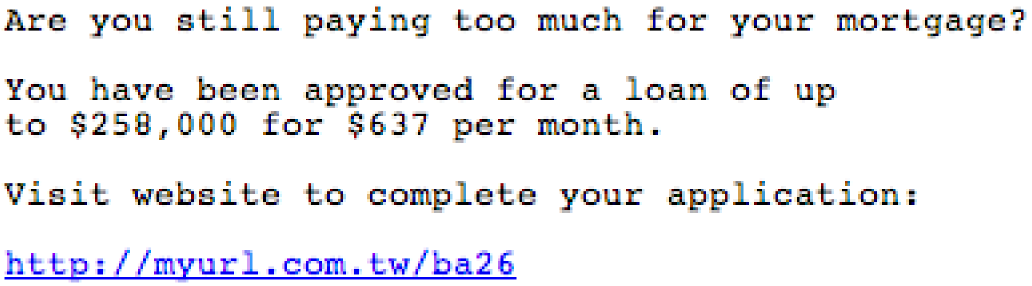
- Not limited to Geocities services, but they are the major target (from 5-15% of all spam)
- Most likely the CAPTCHA tests for Yahoo! IDs have been compromised

Blog abuse

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

URL shortening services

- Up to 20 new URL services discovered every day

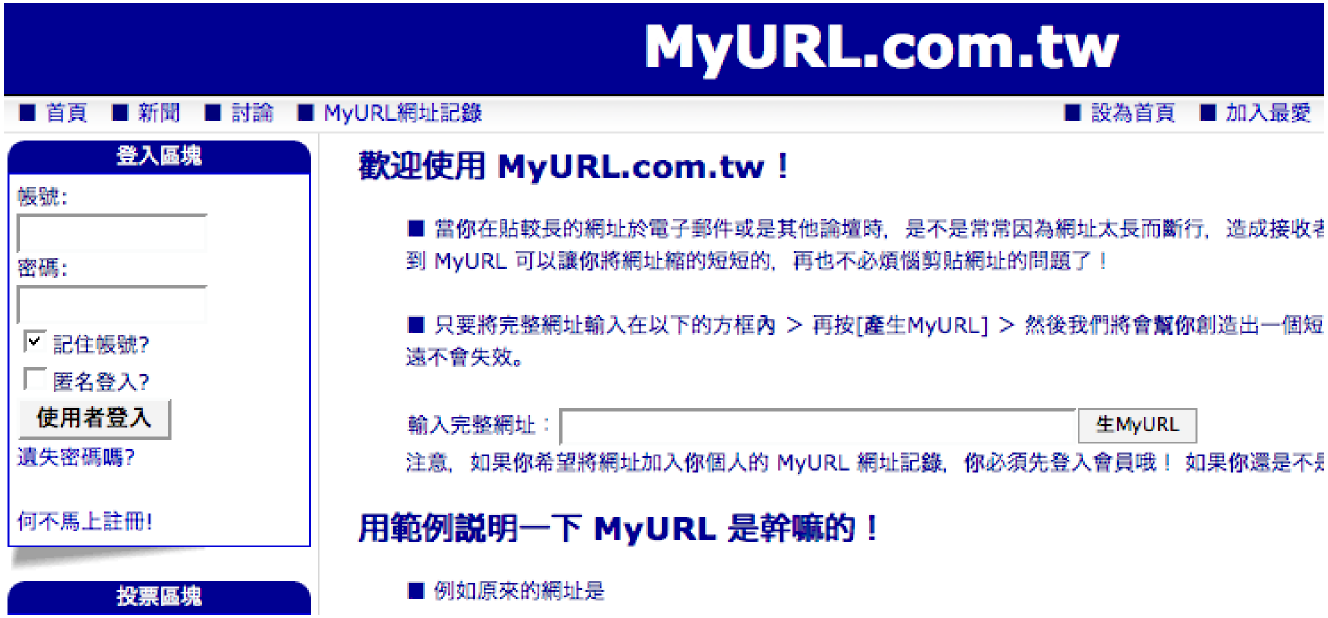


Are you still paying too much for your mortgage?

You have been approved for a loan of up
to $258,000 for $637 per month.

Visit website to complete your application:

http://myurl.com.tw/ba26



MyURL.com.tw

■ 首頁 ■ 新聞 ■ 討論 ■ MyURL網址記錄 ■ 設為首頁 ■ 加入最愛

登入區塊

帳號:

密碼:

☑ 記住帳號?

□ 匿名登入?

使用者登入

遺失密碼嗎?

何不馬上註冊!

投票區塊

歡迎使用 MyURL.com.tw！

■ 當你在貼較長的網址於電子郵件或是其他論壇時，是不是常常因為網址太長而斷行，造成接收
到 MyURL 可以讓你將網址縮的短短的，再也不必煩惱剪貼網址的問題了！

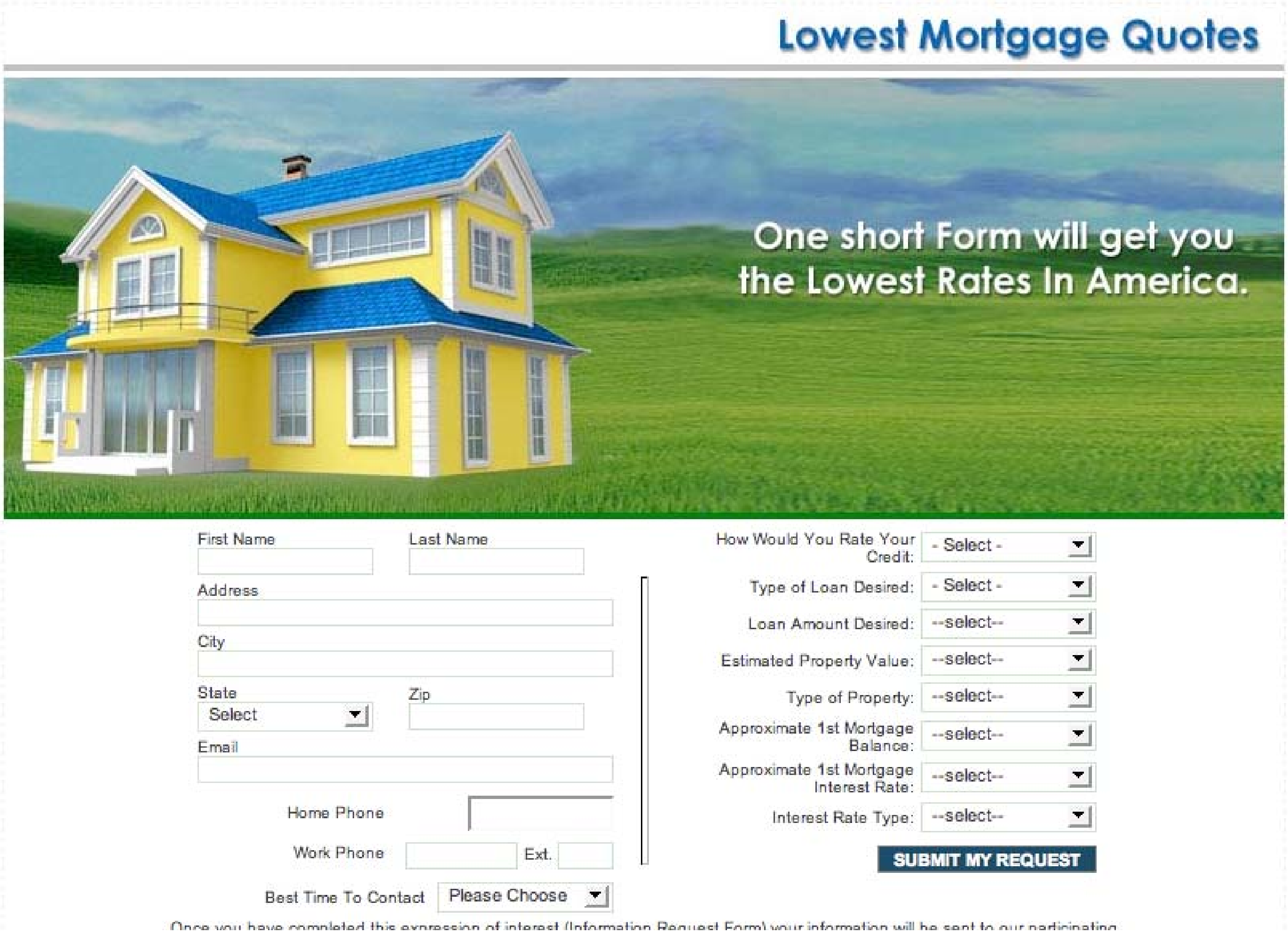
■ 只要將完整網址輸入在以下的方框內 > 再按[產生MyURL] > 然後我們將會幫你創造出一個短
遠不會失效。

輸入完整網址： 生MyURL

注意，如果你希望將網址加入你個人的 MyURL 網址記錄，你必須先登入會員哦！ 如果你還是不

用範例說明一下 MyURL 是幹嘛的！

■ 例如原來的網址是



Lowest Mortgage Quotes

First Name

Last Name

Address

City

State: Select

Zip

Email

Home Phone

Work Phone

Ext.

Best Time To Contact: Please Choose

How Would You Rate Your Credit: - Select -

Type of Loan Desired: - Select -

Loan Amount Desired: --select--

Estimated Property Value: --select--

Type of Property: --select--

Approximate 1st Mortgage Balance: --select--

Approximate 1st Mortgage Interest Rate: --select--

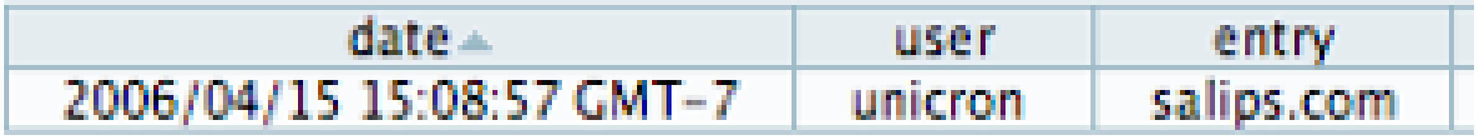
Interest Rate Type: --select--

Once you have completed this expression of interest (Information Request Form) your information will be sent to our participating

Proactive URL blocking

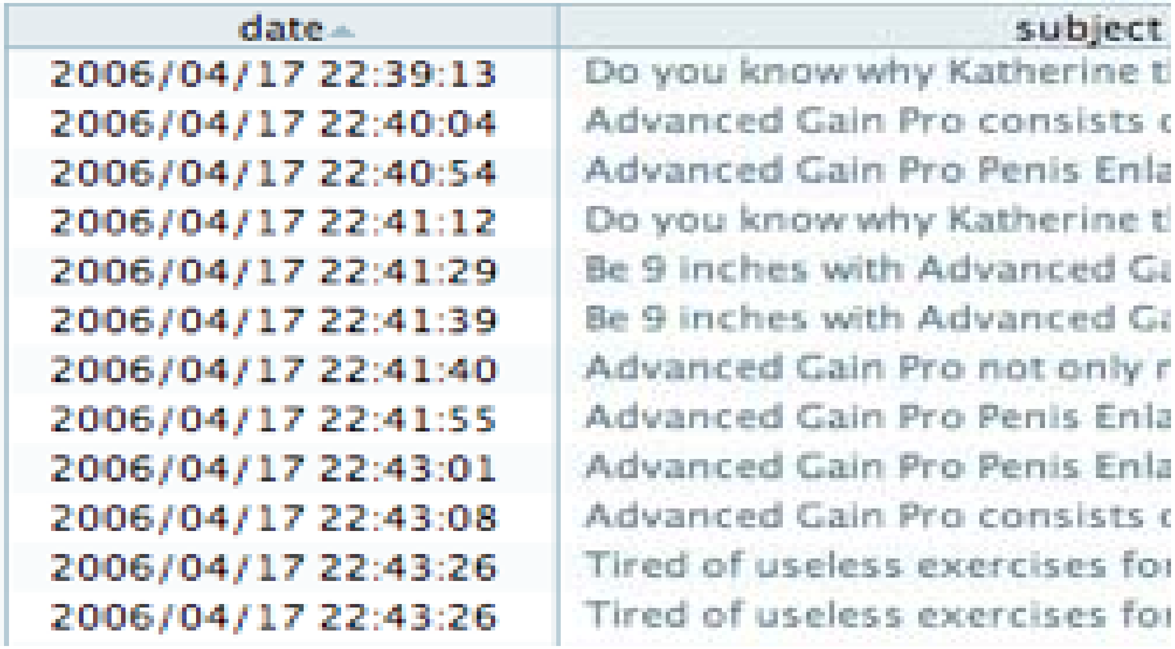
Proactive URL blocking

Blocked:



date ▲	user	entry
2006/04/15 15:08:57 GMT-7	unicron	salips.com

Spammed:



date ▲	subject
2006/04/17 22:39:13	Do you know why Katherine t
2006/04/17 22:40:04	Advanced Gain Pro consists (
2006/04/17 22:40:54	Advanced Gain Pro Penis Enla
2006/04/17 22:41:12	Do you know why Katherine t
2006/04/17 22:41:29	Be 9 inches with Advanced Ga
2006/04/17 22:41:39	Be 9 inches with Advanced Ga
2006/04/17 22:41:40	Advanced Gain Pro not only r
2006/04/17 22:41:55	Advanced Gain Pro Penis Enla
2006/04/17 22:43:01	Advanced Gain Pro Penis Enla
2006/04/17 22:43:08	Advanced Gain Pro consists (
2006/04/17 22:43:26	Tired of useless exercises fo
2006/04/17 22:43:26	Tired of useless exercises fo

And spammers respond…

With “0-minute” domains

fyefga.org

- Registered at 1:28 AM on February 16 2006
- First seen on spam traps at 1:30 AM

The best way to defeat URL blocking is…

…not using URLs at all

instead…

- Phone numbers
- Fax
- VoIP
- IM (ICQ/AIM/…)
- E-mail addresses
- Stock symbols for “pump-n-dump” scams

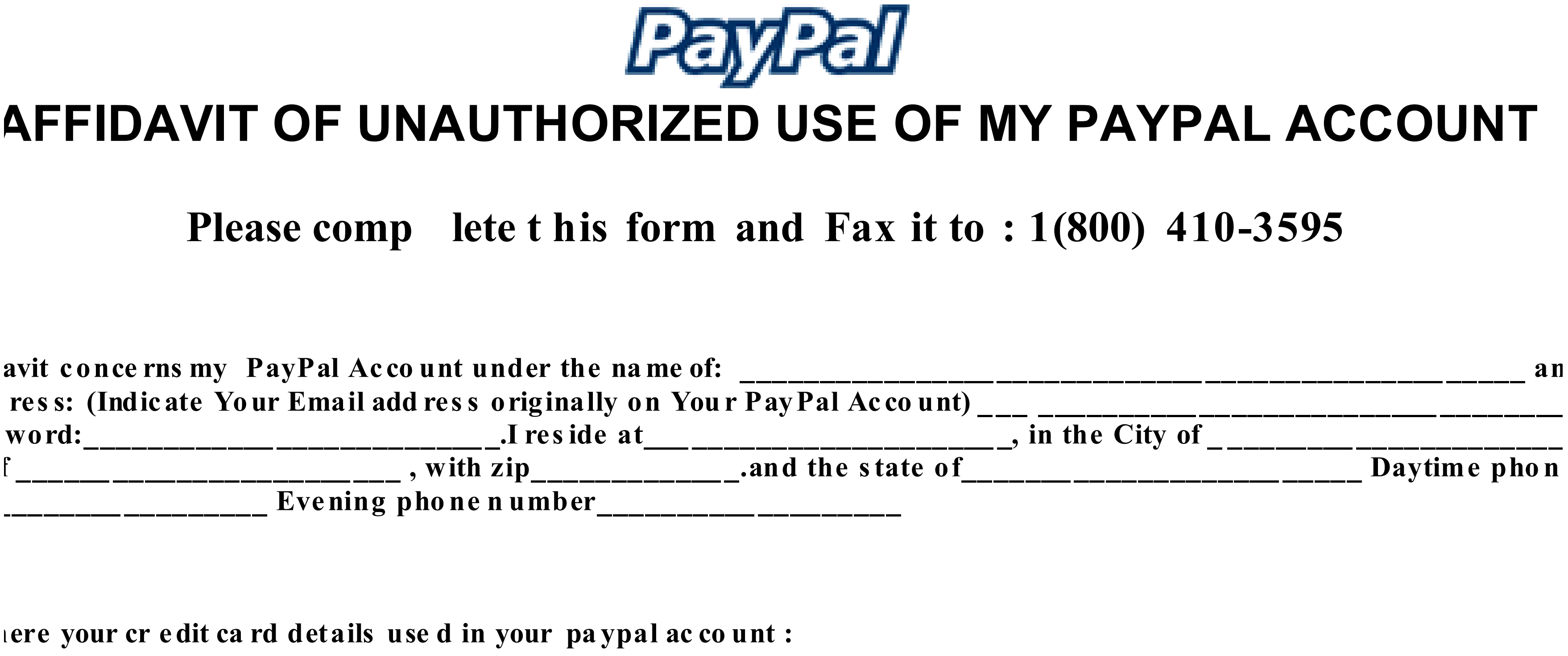
Spam Resume

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Fax + phishing = Phaxing

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Phax form



PayPal

AFFIDAVIT OF UNAUTHORIZED USE OF MY PAYPAL ACCOUNT

Please complete this form and Fax it to : 1(800) 410-3595

avit concerns my PayPal Account under the name of: ____ an
ress: (Indicate Your Email address originally on Your PayPal Account) ___ ______________________________
word:___________________________.I reside at______________________, in the City of ____________________
f _______________________ , with zip_____________.and the state of________________________ Daytime phon
________________ Evening phone number__________________

ıere your credit card details used in your paypal account :

Name from the credit card:____

Number of the credit card:____

Credit card type:__________________

Expiration date:______/_______

Cvv2:_______

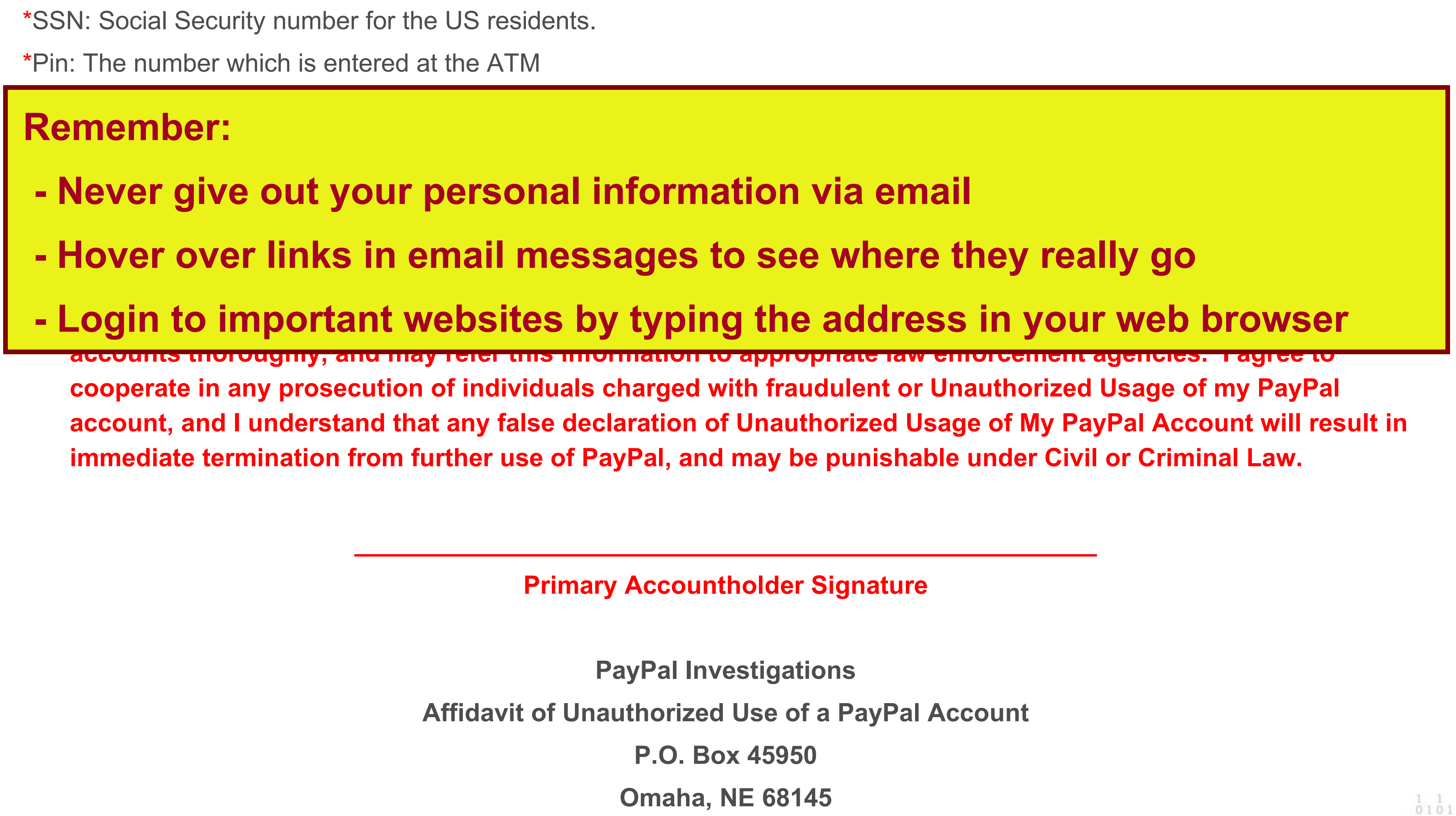
Pin*:______

SSN*:______-_____-_______

Bank name :_________________________________

Bank Routing Number :__________________

Bank Account number :__________________



*SSN: Social Security number for the US residents.

*Pin: The number which is entered at the ATM

Remember:

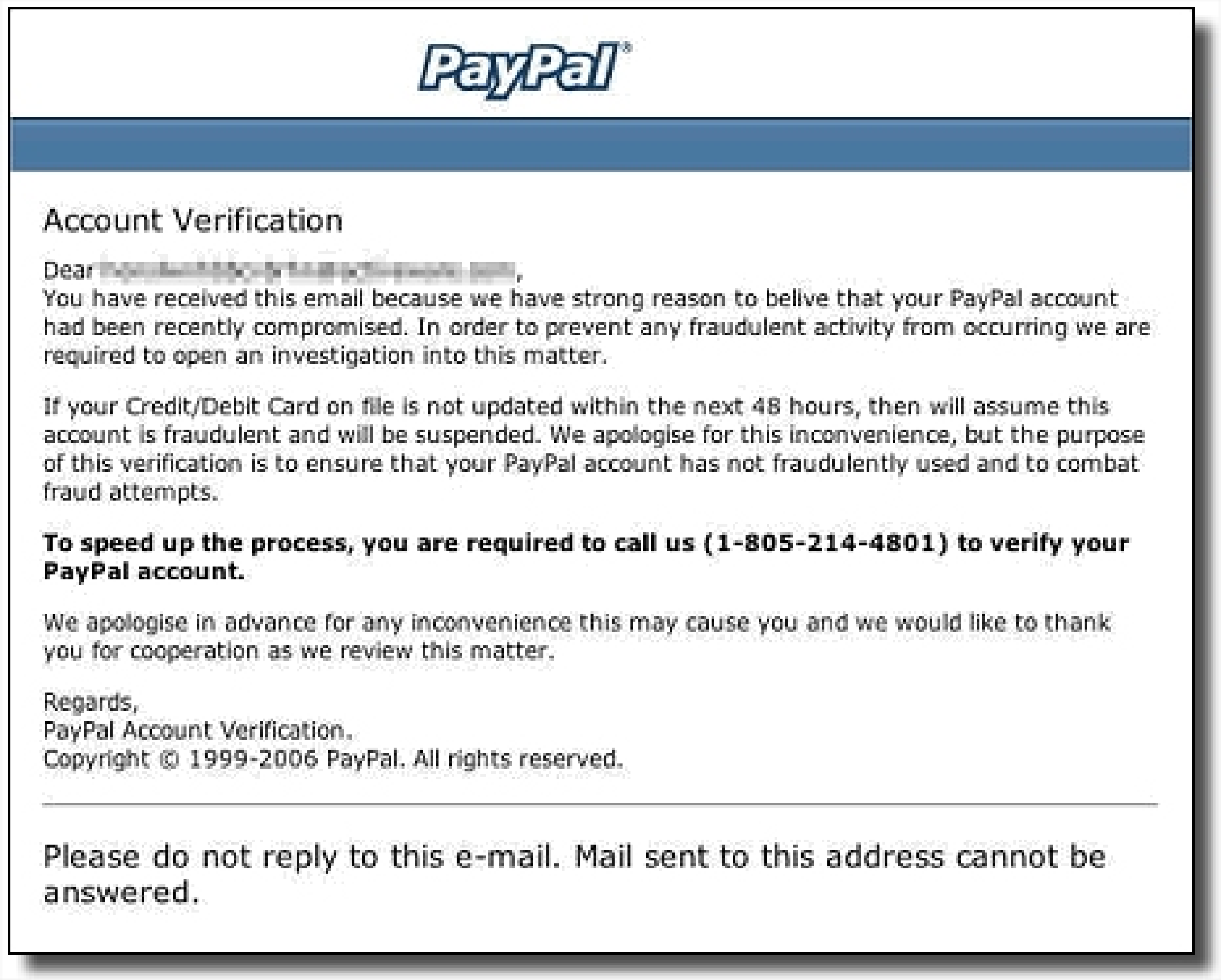
- **Never give out your personal information via email**
- **Hover over links in email messages to see where they really go**
- **Login to important websites by typing the address in your web browser**

accounts thoroughly, and may refer this information to appropriate law enforcement agencies. I agree to cooperate in any prosecution of individuals charged with fraudulent or Unauthorized Usage of my PayPal account, and I understand that any false declaration of Unauthorized Usage of My PayPal Account will result in immediate termination from further use of PayPal, and may be punishable under Civil or Criminal Law.

Primary Accountholder Signature

PayPal Investigations
Affidavit of Unauthorized Use of a PayPal Account
P.O. Box 45950
Omaha, NE 68145

Vishing



PayPal®

Account Verification

Dear [redacted],
You have received this email because we have strong reason to belive that your PayPal account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If your Credit/Debit Card on file is not updated within the next 48 hours, then will assume this account is fraudulent and will be suspended. We apologise for this inconvenience, but the purpose of this verification is to ensure that your PayPal account has not fraudulently used and to combat fraud attempts.

To speed up the process, you are required to call us (1-805-214-4801) to verify your PayPal account.

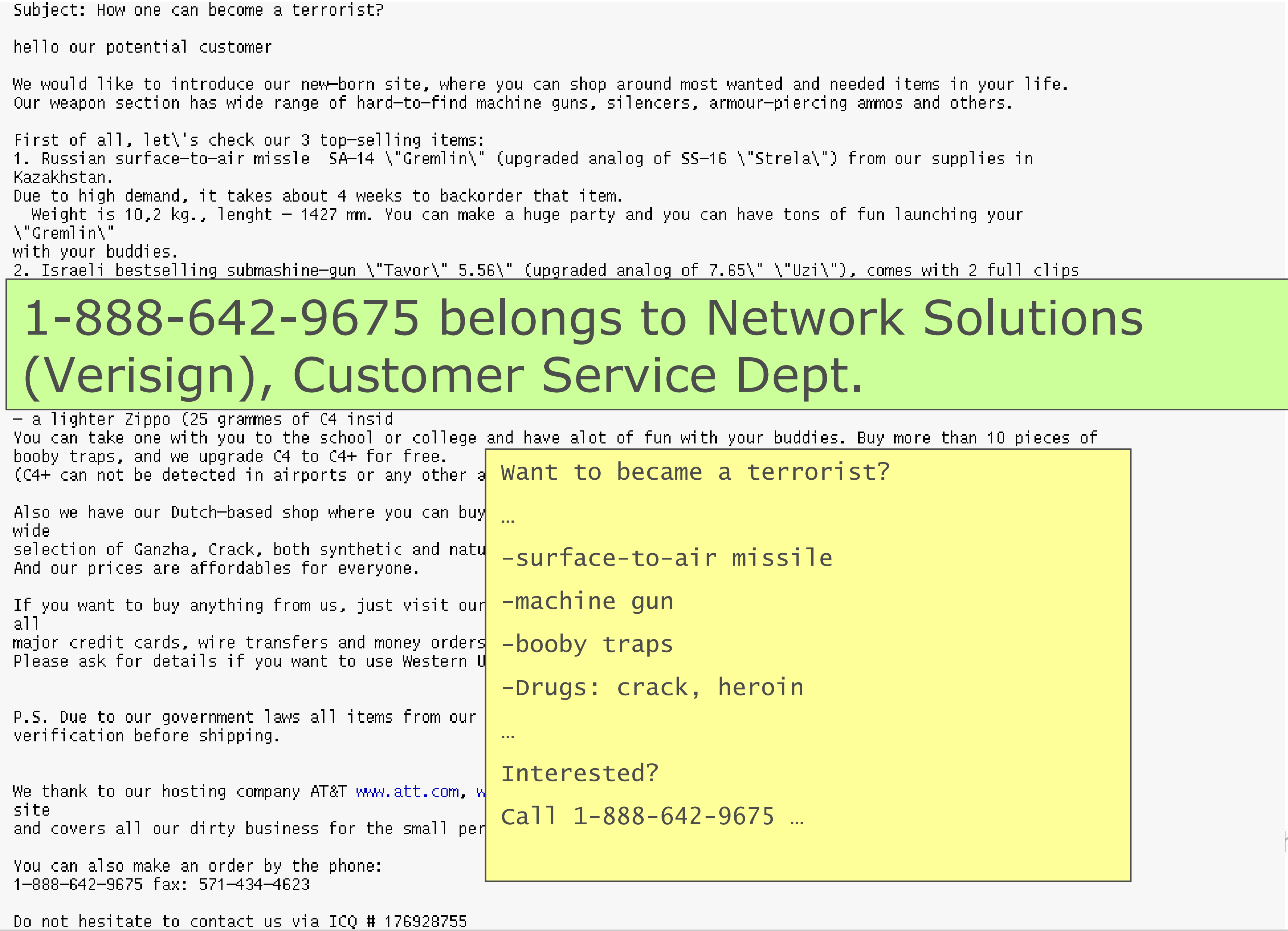
We apologise in advance for any inconvenience this may cause you and we would like to thank you for cooperation as we review this matter.

Regards,
PayPal Account Verification.
Copyright © 1999-2006 PayPal. All rights reserved.

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

Extract and block phone numbers

Beware of “Joe-Jobs”



```
Subject: How one can become a terrorist?

hello our potential customer

We would like to introduce our new-born site, where you can shop around most wanted and needed items in your life.
Our weapon section has wide range of hard-to-find machine guns, silencers, armour-piercing ammos and others.

First of all, let\'s check our 3 top-selling items:
1. Russian surface-to-air missle  SA-14 \"Gremlin\" (upgraded analog of SS-16 \"Strela\") from our supplies in
Kazakhstan.
Due to high demand, it takes about 4 weeks to backorder that item.
  Weight is 10,2 kg., lenght - 1427 mm. You can make a huge party and you can have tons of fun launching your
\"Gremlin\"
with your buddies.
2. Israeli bestselling submashine-gun \"Tavor\" 5.56\" (upgraded analog of 7.65\" \"Uzi\"), comes with 2 full clips
- a lighter Zippo (25 grammes of C4 insid
You can take one with you to the school or college and have alot of fun with your buddies. Buy more than 10 pieces of
booby traps, and we upgrade C4 to C4+ for free.
(C4+ can not be detected in airports or any other a

Also we have our Dutch-based shop where you can buy
wide
selection of Ganzha, Crack, both synthetic and natu
And our prices are affordables for everyone.

If you want to buy anything from us, just visit our
all
major credit cards, wire transfers and money orders
Please ask for details if you want to use Western U


P.S. Due to our government laws all items from our
verification before shipping.


We thank to our hosting company AT&T www.att.com, w
site
and covers all our dirty business for the small per

You can also make an order by the phone:
1-888-642-9675 fax: 571-434-4623

Do not hesitate to contact us via ICQ # 176928755
```

1-888-642-9675 belongs to Network Solutions (Verisign), Customer Service Dept.

Want to became a terrorist?

…

-surface-to-air missile

-machine gun

-booby traps

-Drugs: crack, heroin

…

Interested?

Call 1-888-642-9675 …

Spammers respond

dial: one-eight-hundred-three-fiv-4-31-two-0

1_3*1*4*4+1+4+4*0*0*1

Stock scams with no URLs

```
AGA Resources Inc.
A G A 0
Open: $2.25
Close: $3.00
Up: 33%
```

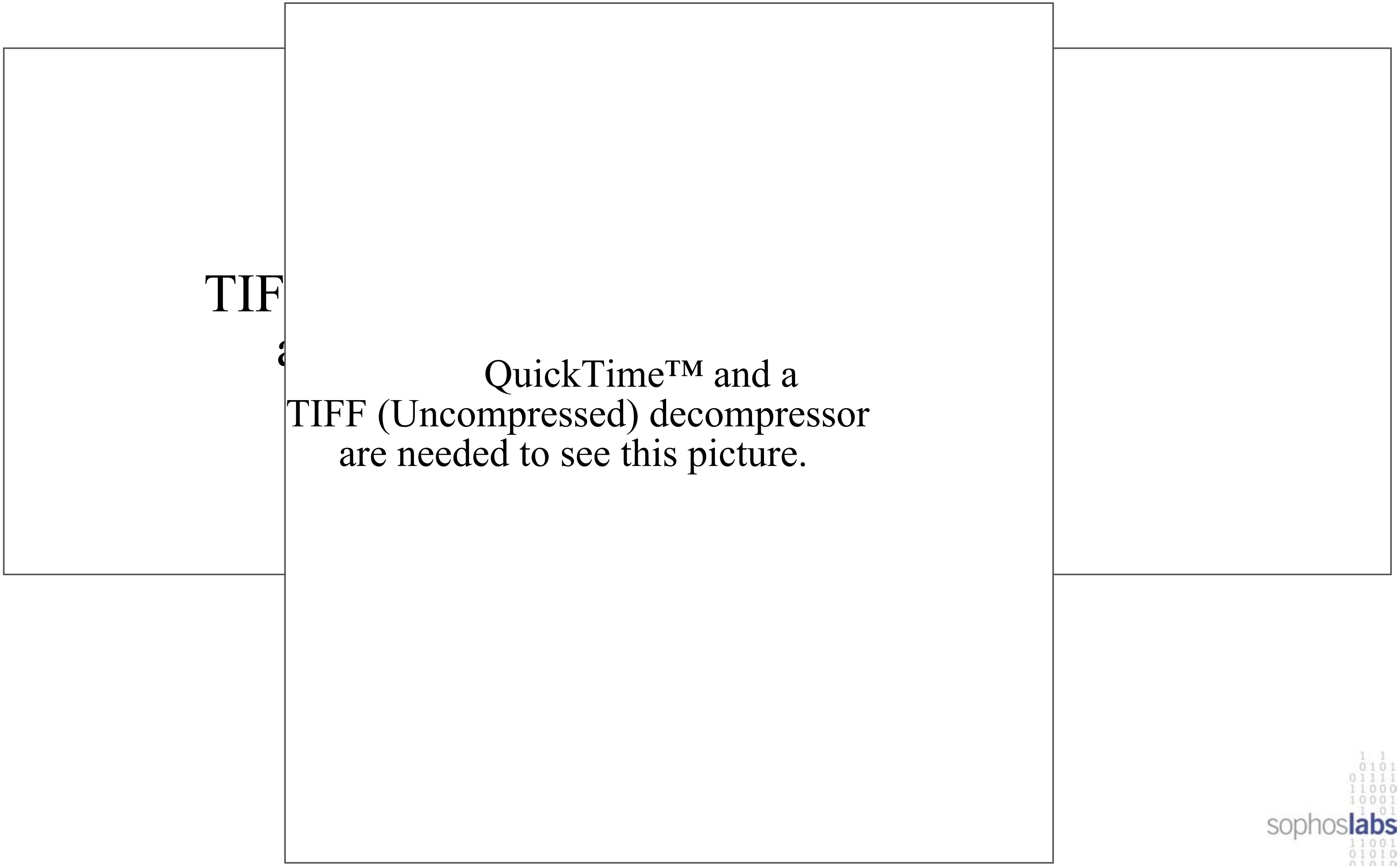
\/iagra
lev`1t*ra
Le\//.itrA
le*v'i-t-ra
\/_1a_gra
\/.alI'u|\/|
v_I@_gra
vaIiuM
v|'agra
c1Alis
\/I@gra
l_ev'|tr-a
vi.Agra
c1ali$
L'e\/-ltra
v.aL.1u`|\/|
\/a|*iu_m

c*ia-ll.s
le\//-itra
l-e\//itr`@
I_ev*lt.ra
vaL.i.um
c-i.ali.s
\/A'|`1_um
ci'AlIs
valiu_|\/|
lev|trA
va|_lum

\/-a_1'iu*|\/|
v'i*agr'A
Ie.vit_ra
\/aLI-u'm
v`A|i_u|\/|
v1agr*a
1ev`1tra
le_v`i't.ra
c'|ali_s
v@1i*u|\/|
c_i*@l|'$
ciAlis
\/a-liu-m
\/Iagra
v@1iu'm
v_i'@gr@
ciAIis

v*|a-gra
ci`ali*S
|evitr_a
vi@g'r@
\/a.Il.um
c|_@.1_is
\/lagrA
1e-v.1tr`@
cI*a*I|_$
v1*Agr'@
val|uM
v@-li*u_|\/|
va1Iu'M
v@li*um

sophoslabs


TIF
a
QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Not as common these days

- Good spam signs -- most filters are now able to detect them
- Not very legible
- Makes spam appear less trustworthy/legitimate
- Switching to some more advanced tricks to disguise content

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Filter’s perspective

□

□

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

□

□

MS Word spam

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Are you smart enough?

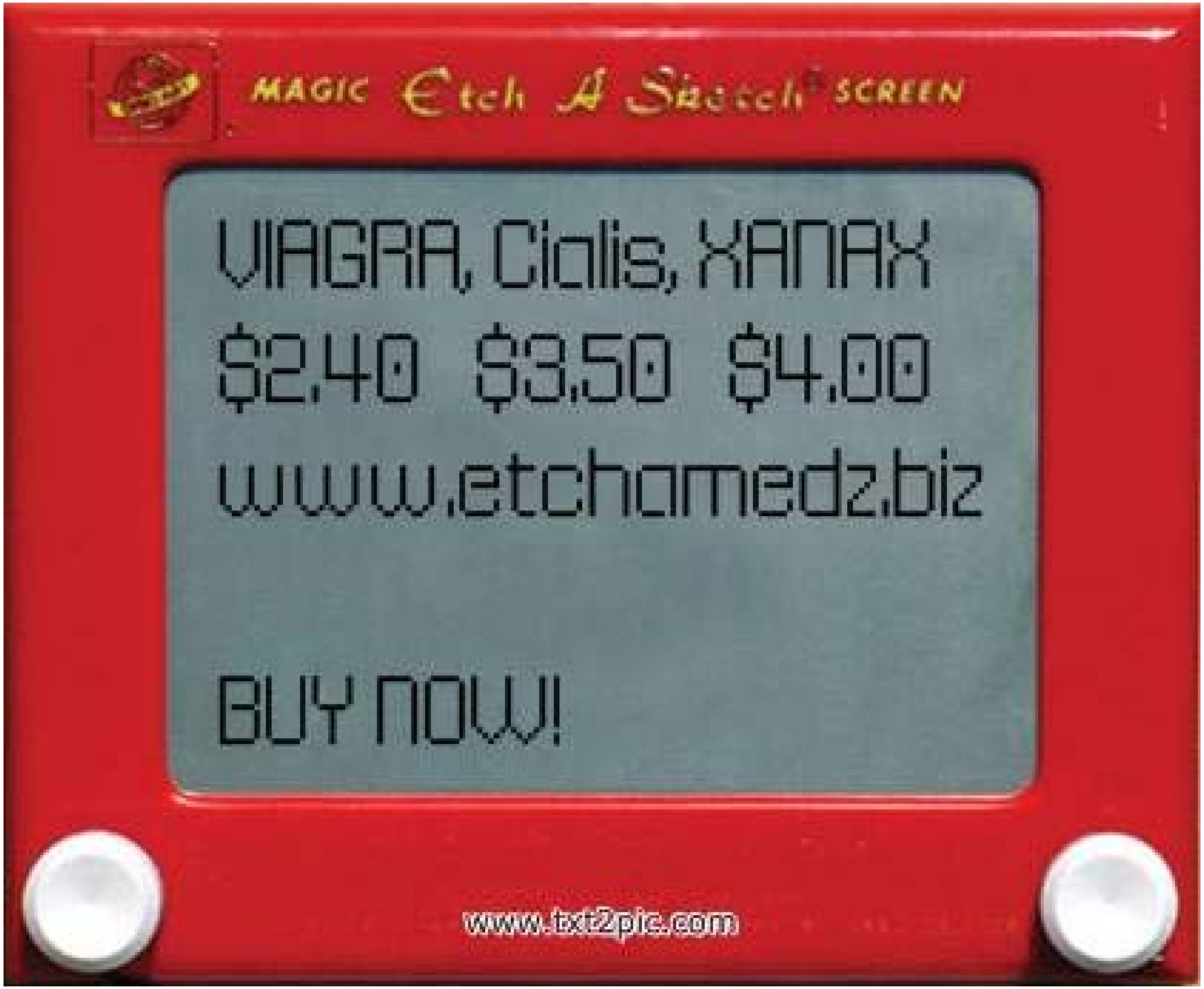
From: "welcome@lf.hebiic.gov.cn”
<welcome@hebiic.gov.cn>
To: undisclosed-recipients: ;
Subject: From far far away

Only Humans with an IQ of at least 120 are allowed to: click here

If you can`t open use this freeware: click here

The best way to defeat text filtering is…

…not using (ASCII) text at all



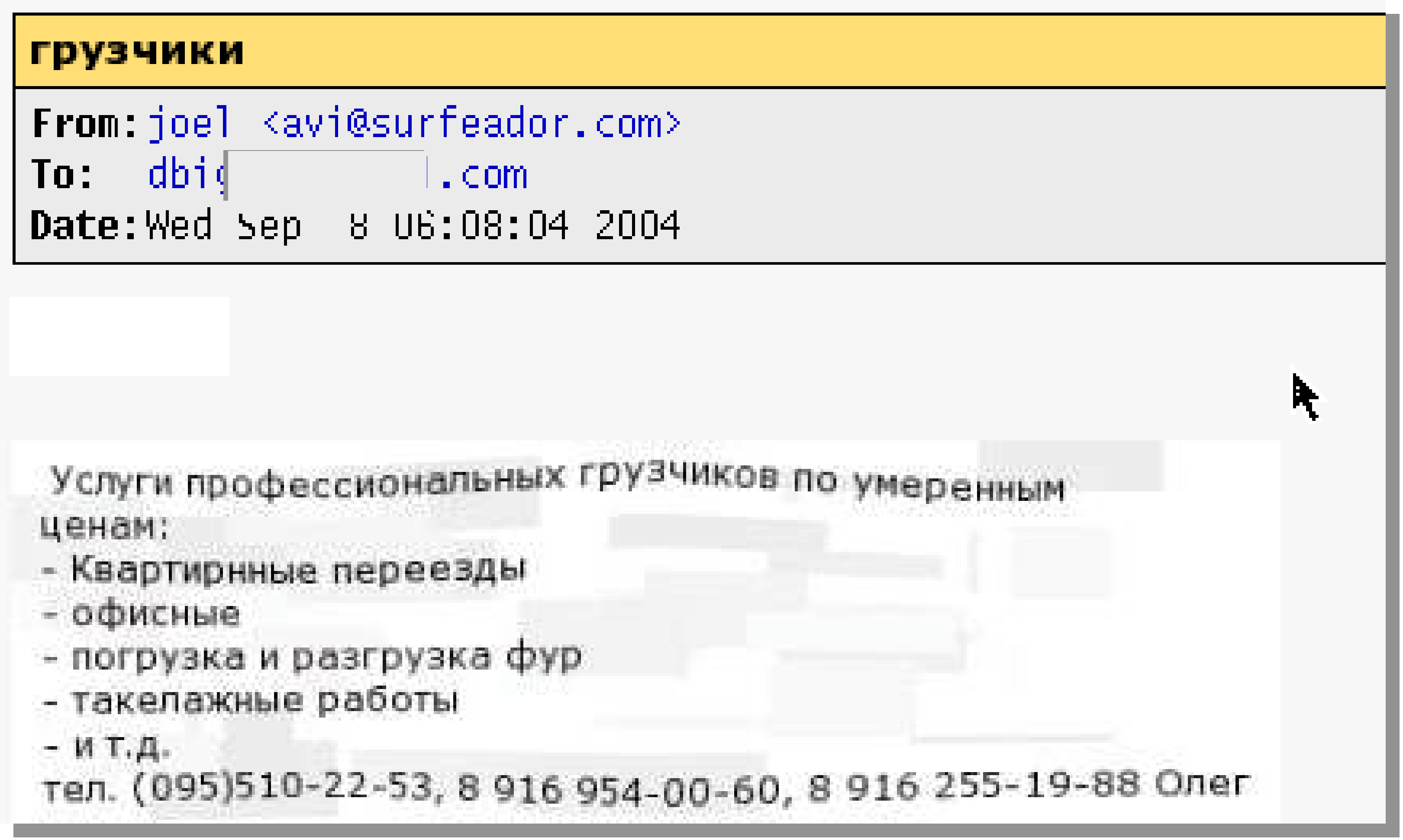
VIAGRA, Cialis, XANAX

$2.40 $3.50 $4.00

www.etchamedz.biz

BUY NOW!

2004



грузчики

From: joel <avi@surfeador.com>
To: dbi[redacted].com
Date: Wed Sep 8 06:08:04 2004

Услуги профессиональных грузчиков по умеренным ценам:
- Квартирнные переезды
- офисные
- погрузка и разгрузка фур
- такелажные работы
- и т.д.

тел. (095)510-22-53, 8 916 954-00-60, 8 916 255-19-88 Олег

2006

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

2006: The era of image spam

Why?

- Attractive
- “Invisible” to most filters
- Bandwidth is no longer a limitation
- Unlimited potential for randomization with little or no impact on legibility

What?

Stock pump-n-dump scams

University “degrees”

Image spam with URLs

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

How: “polka dots”

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

How: “mosaic”

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

How: animation

Buy!
BUY!!!
Buy!
Buy!
BUY!

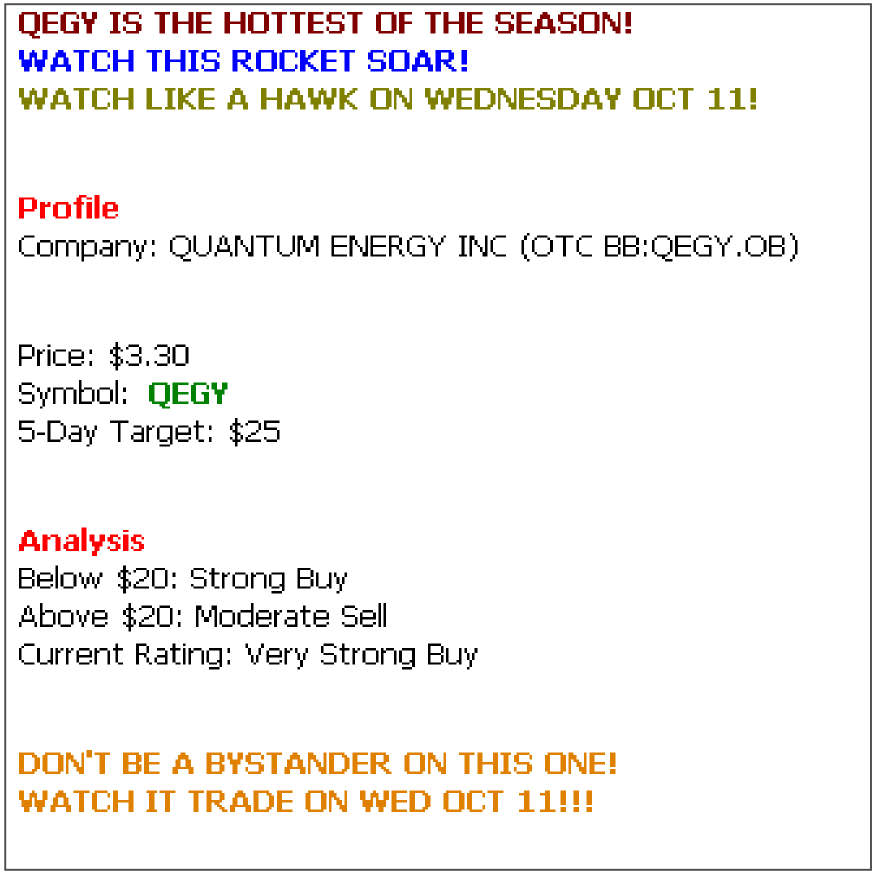
- Not every animated GIF attached to e-mail is spam, apparently…

Anti-(image)-spam techniques

- Connection-level filtering
- Heuristics based on email structure
- Convert to text (Optical Character Recognition)
- Image analysis and “fingerprinting”

Spam vs. legit

30 pixels per byte



QEGY IS THE HOTTEST OF THE SEASON!
WATCH THIS ROCKET SOAR!
WATCH LIKE A HAWK ON WEDNESDAY OCT 11!

Profile
Company: QUANTUM ENERGY INC (OTC BB:QEGY.OB)

Price: $3.30
Symbol: **QEGY**
5-Day Target: $25

Analysis
Below $20: Strong Buy
Above $20: Moderate Sell
Current Rating: Very Strong Buy

DON'T BE A BYSTANDER ON THIS ONE!
WATCH IT TRADE ON WED OCT 11!!!

3 pixels per byte

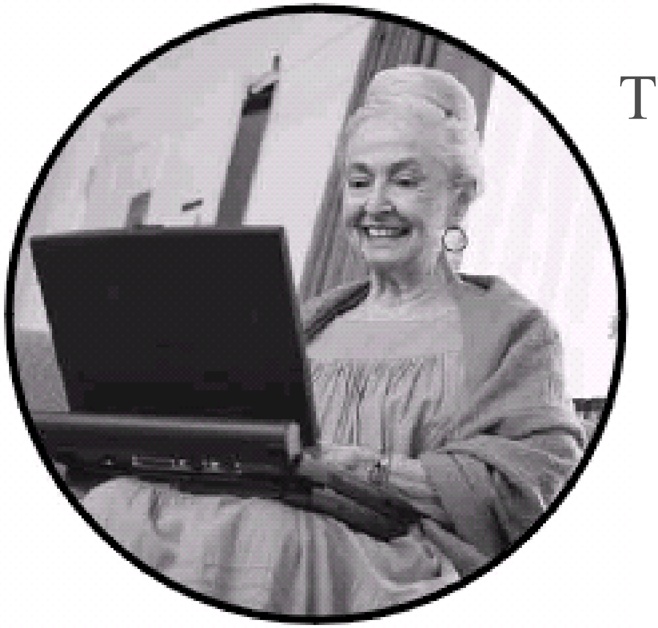
Comparing over 30,000 legit and spam images

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

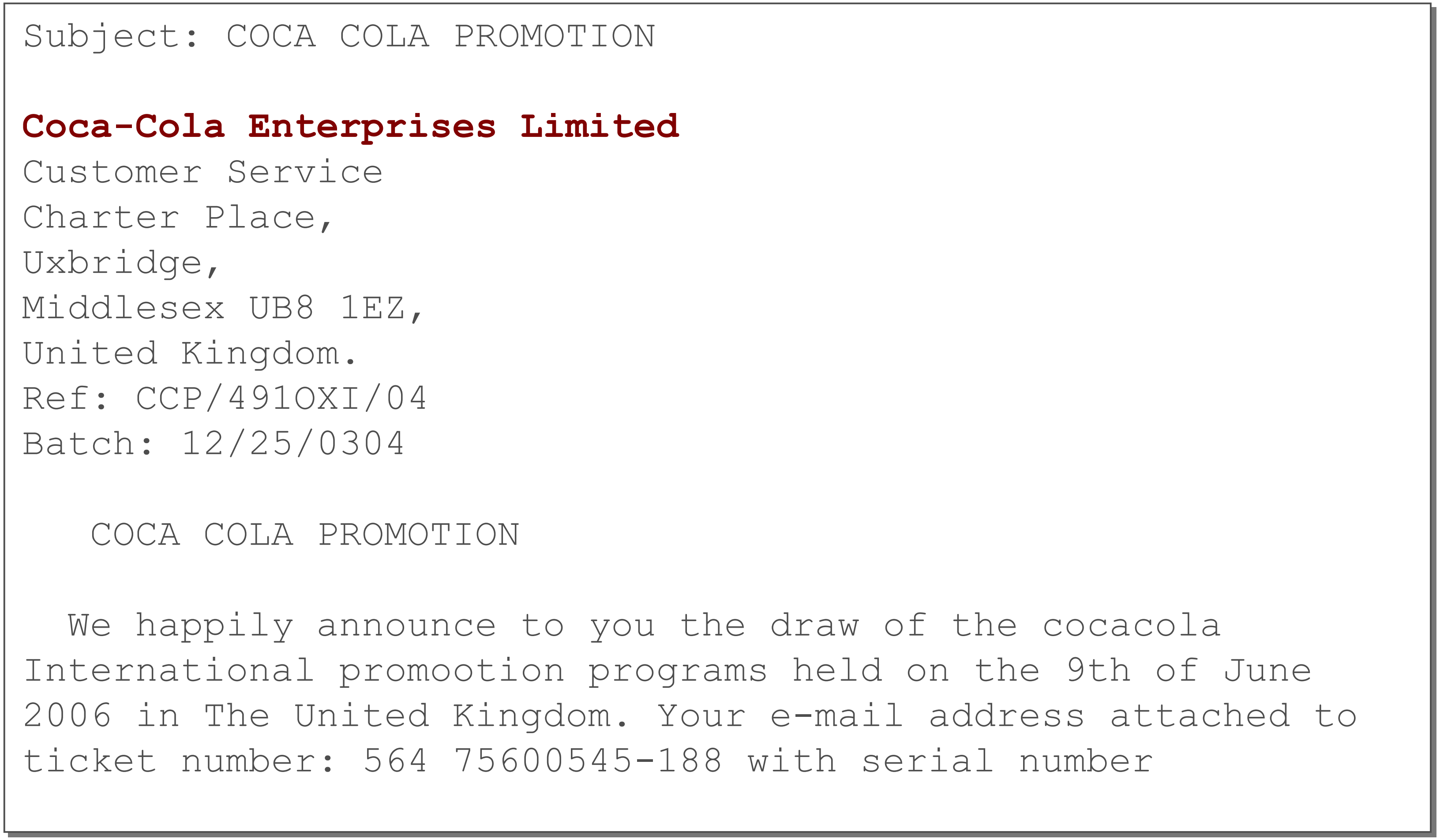
Filtering approaches

- Image metadata within certain bounds:
  - Compression ratio
  - Dimensions
  - Animated or static
- Combined with other information:
  - Sender reputation
  - HTML content
  - MIME structure, headers
- Fuzzy signatures of image metadata specific to a particular spam campaign

Social engineering tricks



The recipient

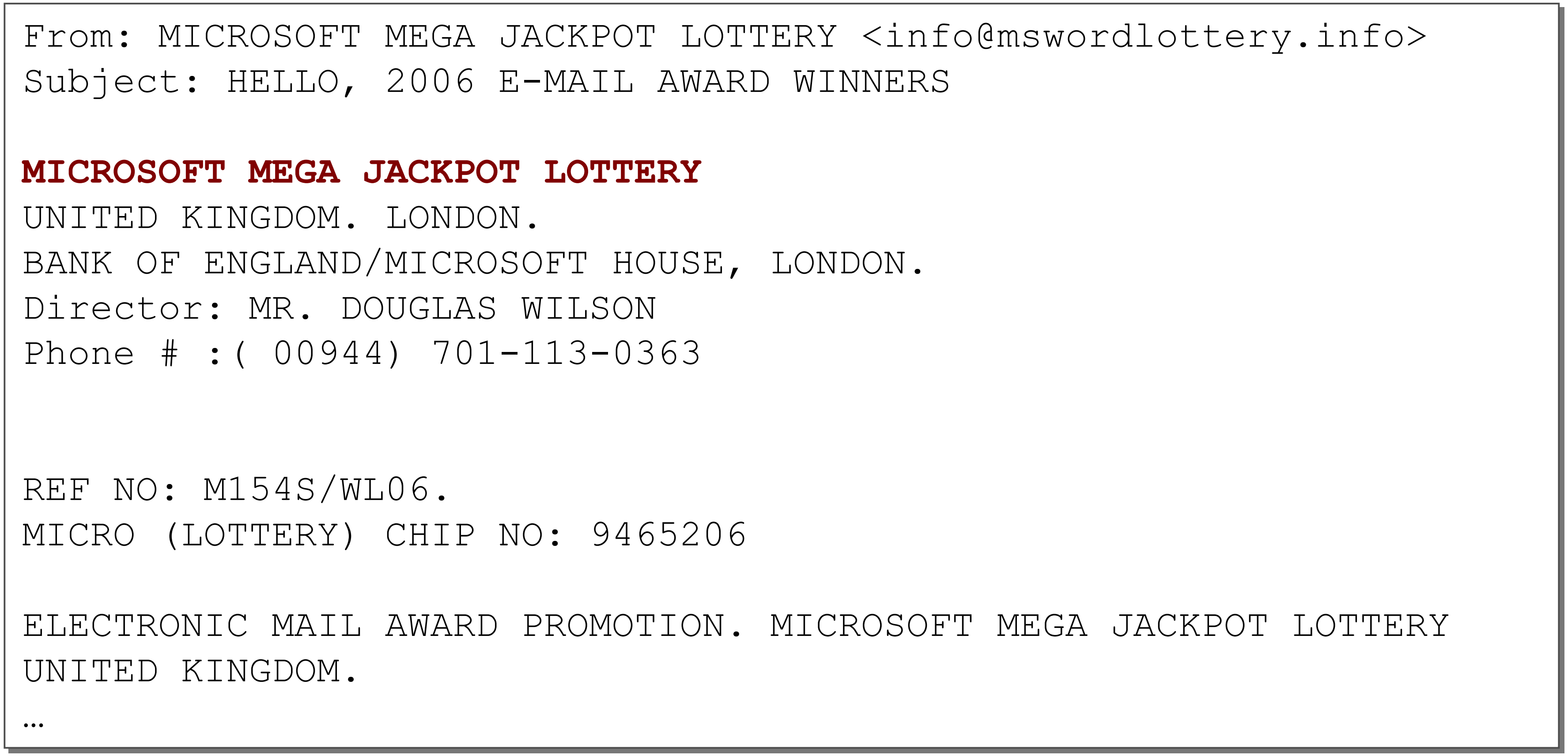


Subject: COCA COLA PROMOTION

Coca-Cola Enterprises Limited
Customer Service
Charter Place,
Uxbridge,
Middlesex UB8 1EZ,
United Kingdom.
Ref: CCP/491OXI/04
Batch: 12/25/0304

COCA COLA PROMOTION

We happily announce to you the draw of the cocacola
International promootion programs held on the 9th of June
2006 in The United Kingdom. Your e-mail address attached to
ticket number: 564 75600545-188 with serial number

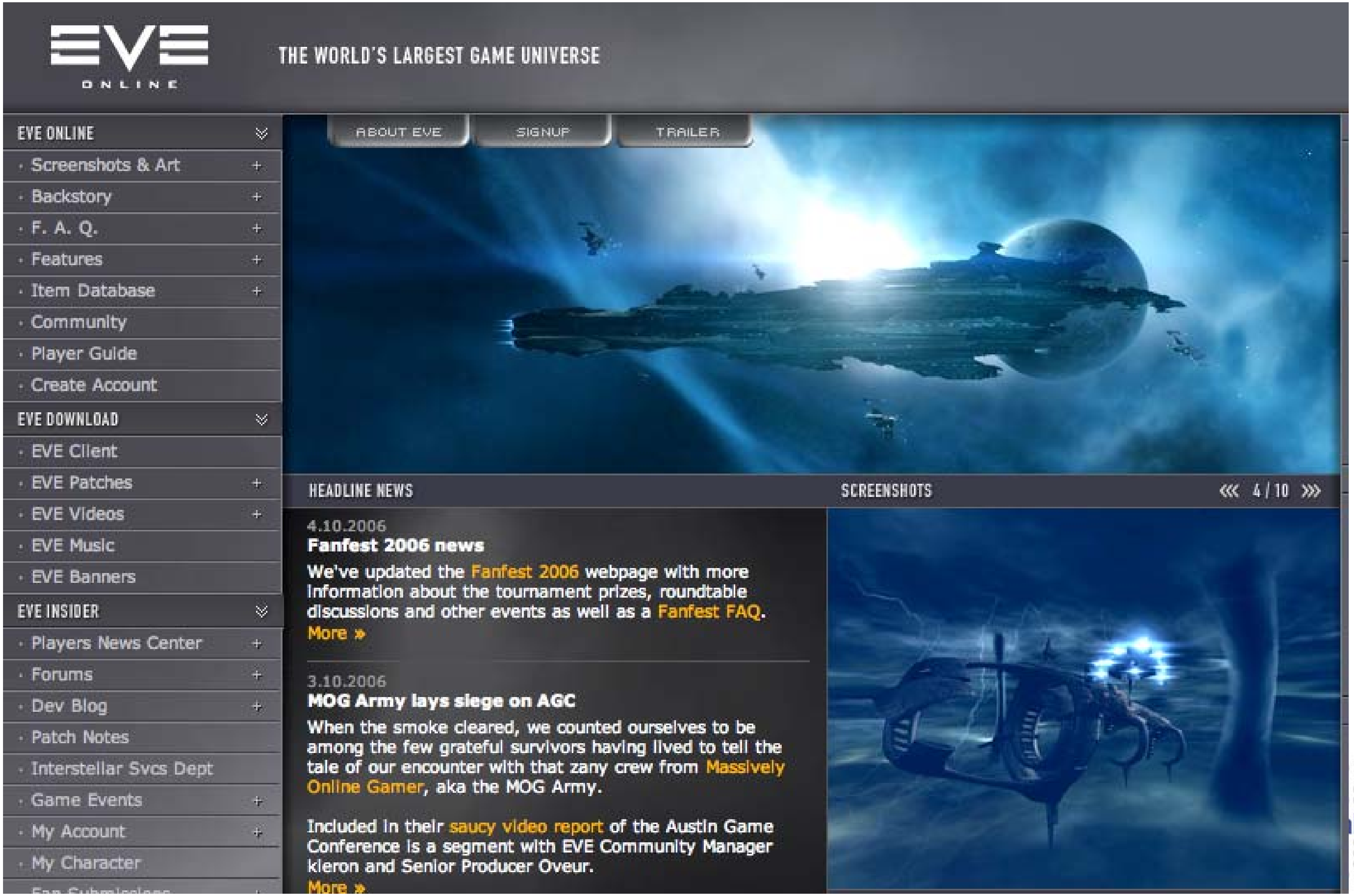


From: MICROSOFT MEGA JACKPOT LOTTERY <info@mswordlottery.info>
Subject: HELLO, 2006 E-MAIL AWARD WINNERS

MICROSOFT MEGA JACKPOT LOTTERY
UNITED KINGDOM. LONDON.
BANK OF ENGLAND/MICROSOFT HOUSE, LONDON.
Director: MR. DOUGLAS WILSON
Phone # :(00944) 701-113-0363

REF NO: M154S/WL06.
MICRO (LOTTERY) CHIP NO: 9465206

ELECTRONIC MAIL AWARD PROMOTION. MICROSOFT MEGA JACKPOT LOTTERY
UNITED KINGDOM.
…



4.10.2006

Fanfest 2006 news

We've updated the Fanfest 2006 webpage with more information about the tournament prizes, roundtable discussions and other events as well as a Fanfest FAQ.

More »

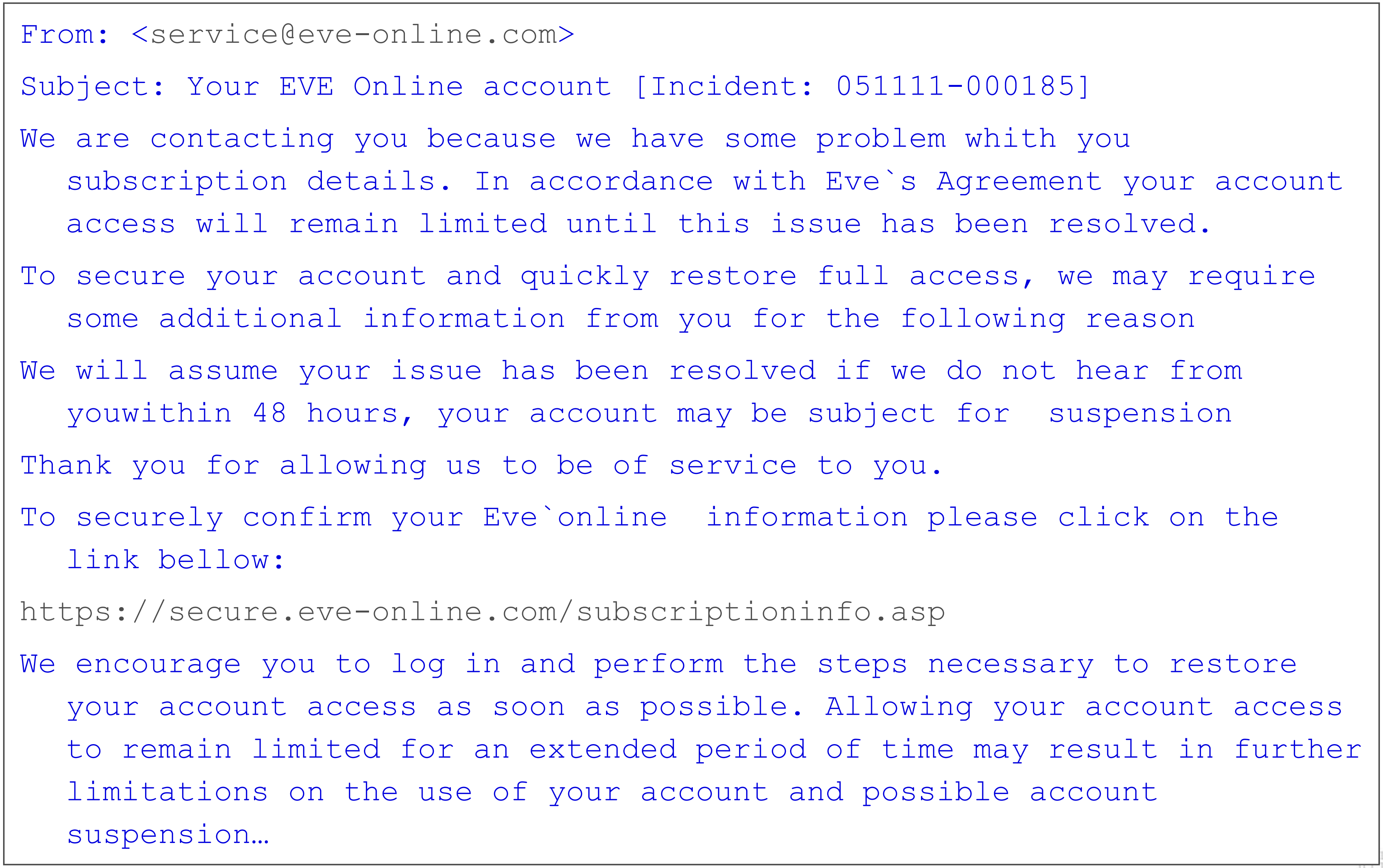
3.10.2006

MOG Army lays siege on AGC

When the smoke cleared, we counted ourselves to be among the few grateful survivors having lived to tell the tale of our encounter with that zany crew from Massively Online Gamer, aka the MOG Army.

Included in their saucy video report of the Austin Game Conference is a segment with EVE Community Manager kieron and Senior Producer Oveur.

More »



From: <service@eve-online.com>

Subject: Your EVE Online account [Incident: 051111-000185]

We are contacting you because we have some problem whith you subscription details. In accordance with Eve`s Agreement your account access will remain limited until this issue has been resolved.

To secure your account and quickly restore full access, we may require some additional information from you for the following reason

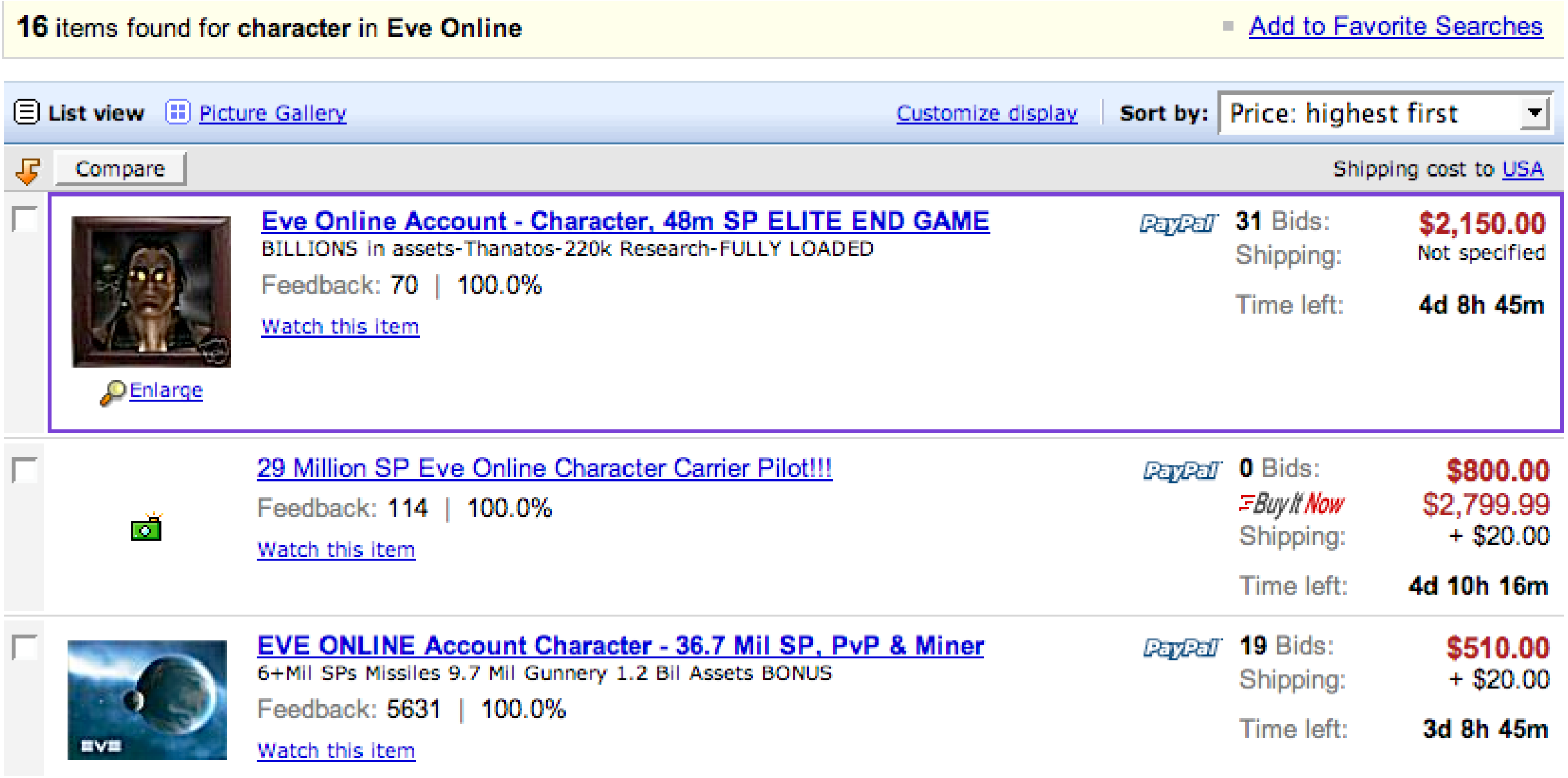
We will assume your issue has been resolved if we do not hear from youwithin 48 hours, your account may be subject for suspension

Thank you for allowing us to be of service to you.

To securely confirm your Eve`online information please click on the link bellow:

https://secure.eve-online.com/subscriptioninfo.asp

We encourage you to log in and perform the steps necessary to restore your account access as soon as possible. Allowing your account access to remain limited for an extended period of time may result in further limitations on the use of your account and possible account suspension…



16 items found for **character** in **Eve Online**

Add to Favorite Searches

Sort by: Price: highest first

Shipping cost to USA

□ **Eve Online Account - Character, 48m SP ELITE END GAME**
BILLIONS in assets-Thanatos-220k Research-FULLY LOADED
Feedback: 70 | 100.0%
Watch this item
PayPal **31** Bids: **$2,150.00**
Shipping: Not specified
Time left: **4d 8h 45m**

□ 29 Million SP Eve Online Character Carrier Pilot!!!
Feedback: 114 | 100.0%
Watch this item
PayPal **0** Bids: **$800.00**
Buy It Now $2,799.99
Shipping: + $20.00
Time left: **4d 10h 16m**

□ **EVE ONLINE Account Character - 36.7 Mil SP, PvP & Miner**
6+Mil SPs Missiles 9.7 Mil Gunnery 1.2 Bil Assets BONUS
Feedback: 5631 | 100.0%
Watch this item
PayPal **19** Bids: **$510.00**
Shipping: + $20.00
Time left: **3d 8h 45m**

ebay®

sophoslabs

More victims

ebay®
YAHOO!®
Microsoft®
PayPal®
Coca-Cola®

Thank you