PHISHING
NOTANDINN VEIDDUR

Kristján Valur Jónsson

CERT-IS Netöryggissveit

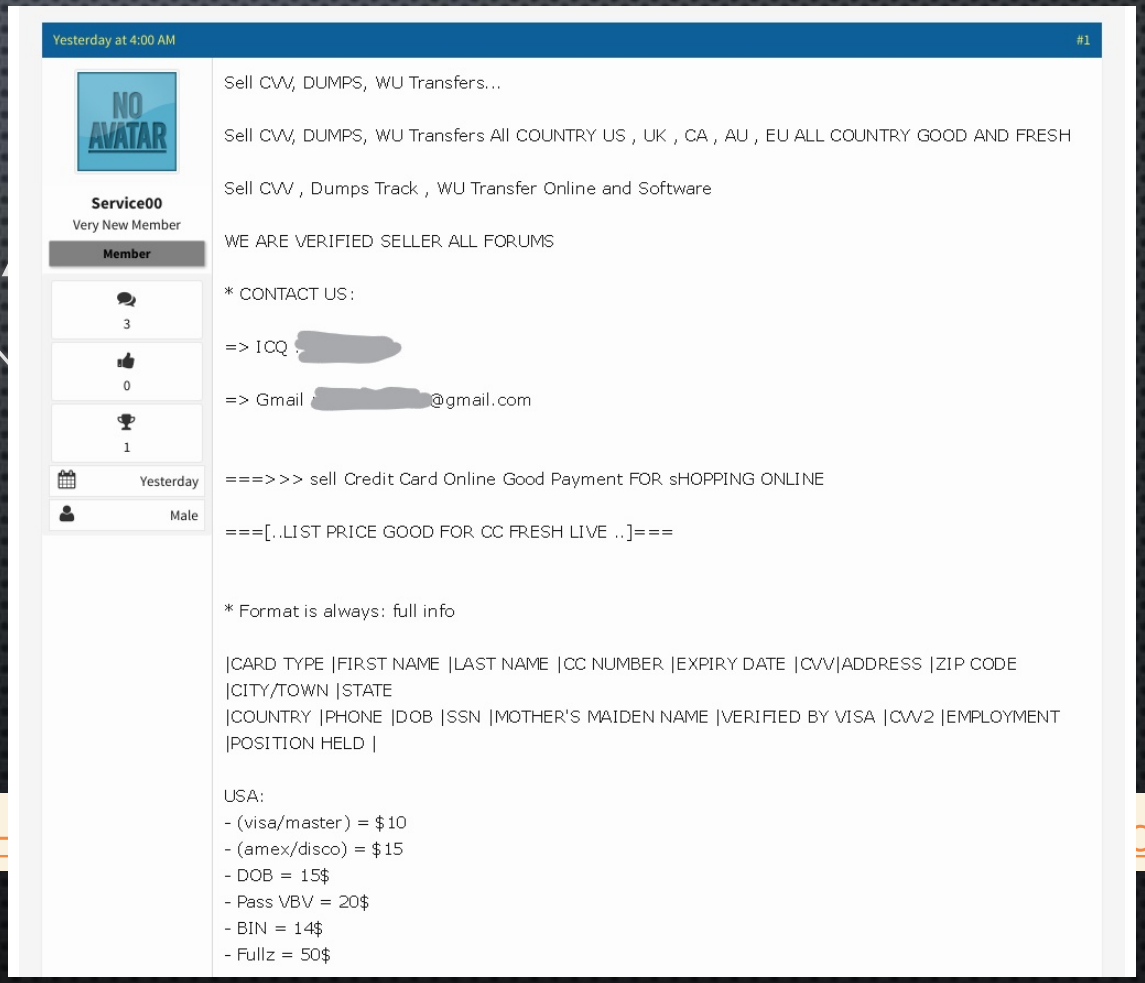
- Hvað eru netveiðar?
- Af hverju er verið að veiða?
- Hvernig er beitunni komið til mín?
- Af hverju bít ég á önguLinn?
- Hvað get ég gert til að varast að vera veiddur?

Hvað eru vefveiðar (phishing)?

Safn aðferða þar sem brögðum er beitt til að komast yfir upplýsingar notandans sem hafa virði af einhverju tagi fyrir árásaraðilann

AF HVERJU?

- **NOTENDAUPPLÝSINGAR ERU VERÐMÆ**
  - NOTENDANÖFN/TÖLVUPÓSTFÖN
  - LYKILORÐ
  - BANKAUPPLÝSINGAR
  - KORTAUPPLÝSINGAR



https://www.infosecurity-
ahoo/

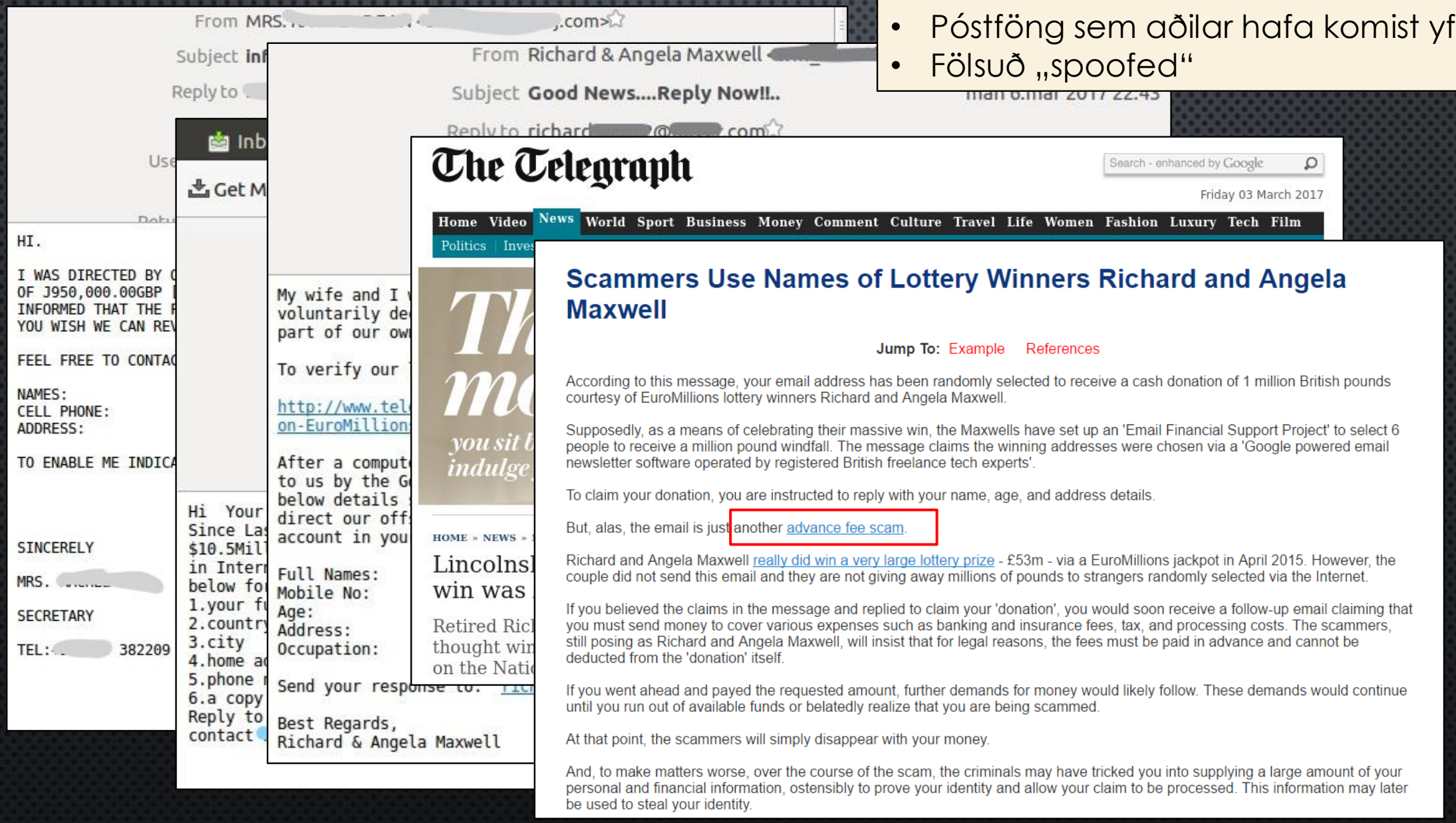
KASTIÐ - ÖNGULLINN OG BEITAN

Beitunni komið út

- Algengast: Tölvupóstur
  - Fjölpóstur – "spam"
  - Beinskeyttara – spearphishing, Whaling
- Brögð til að auka líkur á árangri – "social engineering"
  - Tilbúið neyðarástand
  - Von um endurgreiðslu eða gróða
  - Staðfesta upplýsingar - oft viljandi rangar

Sendandi:

- Póstföng sem aðilar hafa komist yfir
- Fölsuð „spoofed“



From MRS. .com>

Subject inf

Reply to

HI.

I WAS DIRECTED BY
OF J950,000.00GBP
INFORMED THAT THE
YOU WISH WE CAN REV

FEEL FREE TO CONTAC

NAMES:
CELL PHONE:
ADDRESS:

TO ENABLE ME INDICA

SINCERELY

MRS.

SECRETARY

TEL: 382209

From Richard & Angela Maxwell

Subject Good News....Reply Now!!..

Reply to richard @ .com

My wife and I
voluntarily de
part of our ow

To verify our

http://www.tel
on-EuroMillion

After a comput
to us by the G
below details
direct our off
account in you

Full Names:
Mobile No:
Age:
Address:
Occupation:

Send your response to:

Best Regards,
Richard & Angela Maxwell

Inb

Get M

Hi Your
Since La
$10.5Mil
in Inter
below fo
1.your f
2.country
3.city
4.home a
5.phone
6.a copy
Reply to
contact

The Telegraph

Search - enhanced by Google

Friday 03 March 2017

Home Video News World Sport Business Money Comment Culture Travel Life Women Fashion Luxury Tech Film

Politics Inves

HOME » NEWS »

Lincolns
win was

Retired Ric
thought wi
on the Nati

Scammers Use Names of Lottery Winners Richard and Angela Maxwell

Jump To: Example References

According to this message, your email address has been randomly selected to receive a cash donation of 1 million British pounds courtesy of EuroMillions lottery winners Richard and Angela Maxwell.

Supposedly, as a means of celebrating their massive win, the Maxwells have set up an 'Email Financial Support Project' to select 6 people to receive a million pound windfall. The message claims the winning addresses were chosen via a 'Google powered email newsletter software operated by registered British freelance tech experts'.

To claim your donation, you are instructed to reply with your name, age, and address details.

But, alas, the email is just another advance fee scam.

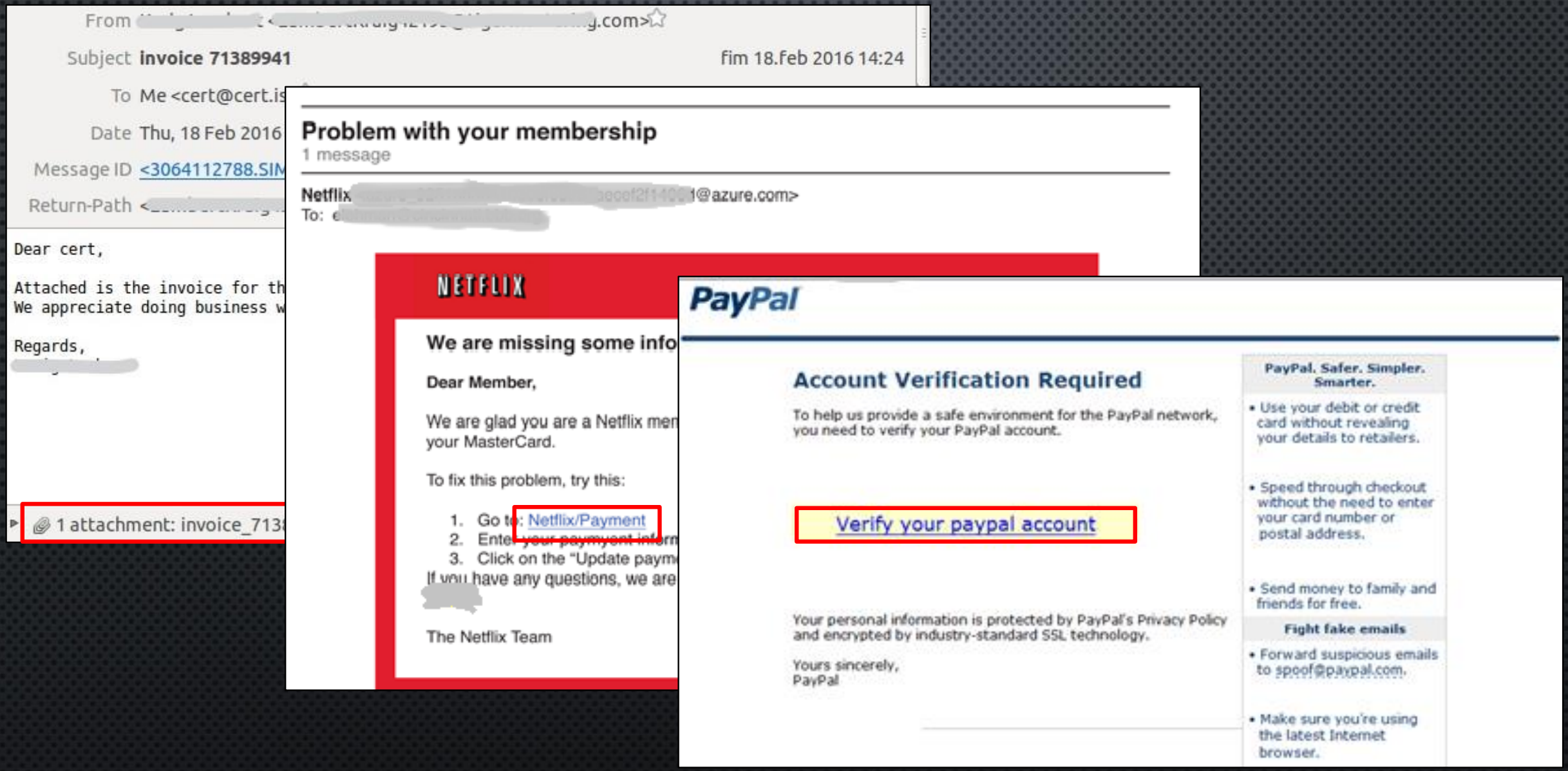
Richard and Angela Maxwell really did win a very large lottery prize - £53m - via a EuroMillions jackpot in April 2015. However, the couple did not send this email and they are not giving away millions of pounds to strangers randomly selected via the Internet.

If you believed the claims in the message and replied to claim your 'donation', you would soon receive a follow-up email claiming that you must send money to cover various expenses such as banking and insurance fees, tax, and processing costs. The scammers, still posing as Richard and Angela Maxwell, will insist that for legal reasons, the fees must be paid in advance and cannot be deducted from the 'donation' itself.

If you went ahead and payed the requested amount, further demands for money would likely follow. These demands would continue until you run out of available funds or belatedly realize that you are being scammed.

At that point, the scammers will simply disappear with your money.

And, to make matters worse, over the course of the scam, the criminals may have tricked you into supplying a large amount of your personal and financial information, ostensibly to prove your identity and allow your claim to be processed. This information may later be used to steal your identity.


From
Subject invoice 71389941
fim 18.feb 2016 14:24
To Me <cert@cert.is
Date Thu, 18 Feb 2016
Message ID <3064112788.SIM
Return-Path
Dear cert,
Attached is the invoice for th
We appreciate doing business w
Regards,
1 attachment: invoice_713
Problem with your membership
1 message
Netflix
To:
NETFLIX
We are missing some info
Dear Member,
We are glad you are a Netflix mem
your MasterCard.
To fix this problem, try this:
1. Go to: Netflix/Payment
2. Ente
3. Click on the "Update paym
If you have any questions, we are
The Netflix Team
PayPal
Account Verification Required
To help us provide a safe environment for the PayPal network, you need to verify your PayPal account.
Verify your paypal account
Your personal information is protected by PayPal's Privacy Policy and encrypted by industry-standard SSL technology.
Yours sincerely,
PayPal
PayPal. Safer. Simpler. Smarter.
• Use your debit or credit card without revealing your details to retailers.
• Speed through checkout without the need to enter your card number or postal address.
• Send money to family and friends for free.
Fight fake emails
• Forward suspicious emails to spoof@paypal.com.
• Make sure you're using the latest Internet browser.

07. mar. 2017 - 10:30 | Smári Pálmarsson

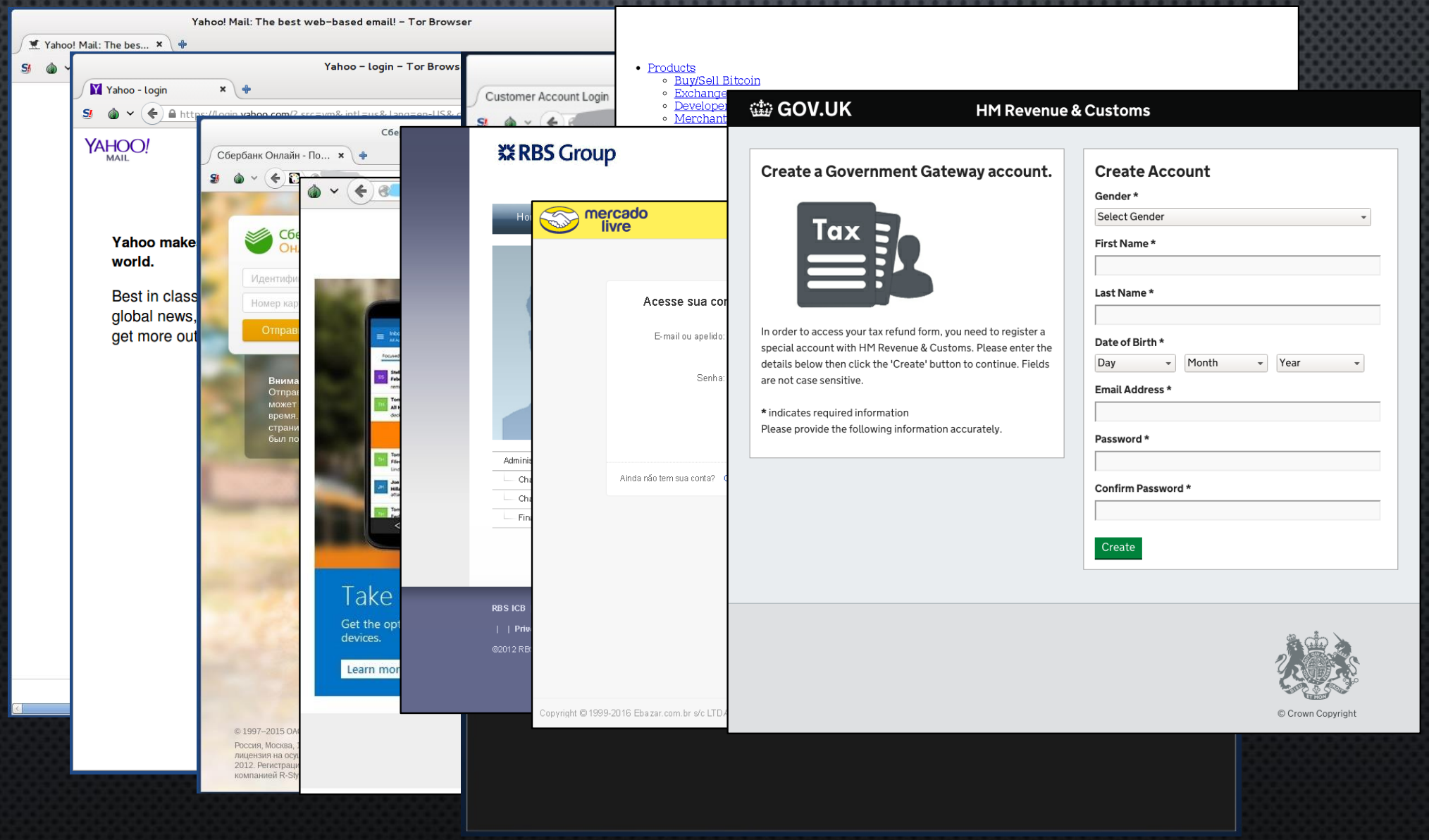
Nýr vírus breiðist hratt út í íslenskum Facebook-hópum – Þetta þarft þú að varast

Nýr vírus hefur gert vart við sig á Facebook og verið sérstaklega áberandi síðasta sólarhring. Meðlimir íslenskra Facebook hópa hafa ef til vill orðið varir við vírusinn en honum var deilt í fjölda þeirra í gær. Vírusinn líkist í fyrstu einfaldri GIF hreyfimynd sem undir venjulegum kringumstæðum spilast á Facebook þegar notandinn smellir á hana. Þannig blekkir þessu vírus notendur til þess að smella og leiðir þá síðan yfir á aðra síðu.

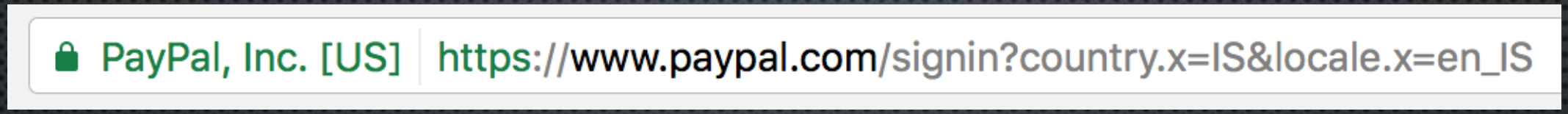
FEST Á

Skotfærin – "payload"

- Hlekkur á Phishing síðu – t.d. falssíða sem líkir eftir raunverulegri innskráningarmynd
- Spillikóði – hlekkur á „exploit kit“ eða viðhengi
  - Njósnabúnaður
  - Banka „trojan“
  - Ransomware


Yahoo! Mail: The best web-based email! – Tor Browser
Yahoo! Mail: The bes...
Yahoo – login – Tor Brows
Yahoo - login
YAHOO!
MAIL
Yahoo make
world.
Best in class
global news,
get more out
Customer Account Login
Products
Buy/Sell Bitcoin
Exchange
Developer
Merchant
Сбербанк Онлайн - По...
Отправ
Take
Get the opt
devices.
Learn mor
RBS Group
mercado livre
Acesse sua con
E-mail ou apelido:
Senha:
Ainda não tem sua conta?
RBS ICB
©2012 RB
Copyright © 1999-2016 Ebazar.com.br s/c LTDA
GOV.UK
HM Revenue & Customs
Create a Government Gateway account.
Tax
In order to access your tax refund form, you need to register a special account with HM Revenue & Customs. Please enter the details below then click the 'Create' button to continue. Fields are not case sensitive.
* indicates required information
Please provide the following information accurately.
Create Account
Gender *
Select Gender
First Name *
Last Name *
Date of Birth *
Day
Month
Year
Email Address *
Password *
Confirm Password *
Create
© Crown Copyright

SLÓÐIN



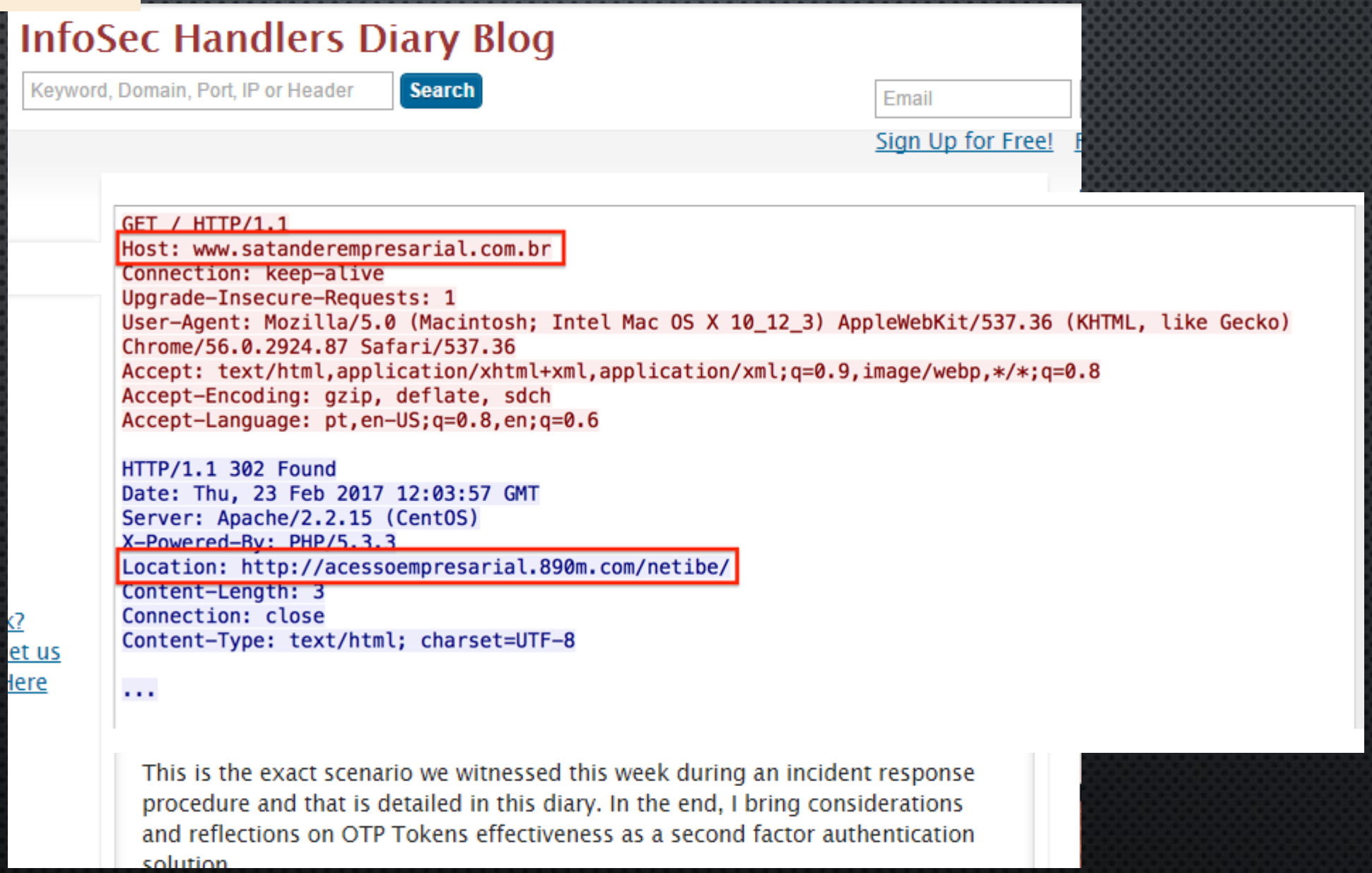
http://worldfamouscarpets.com/blogs/posts/ahtyyloq23/login

http://www.paypa1.com

http://www.paypoi.info

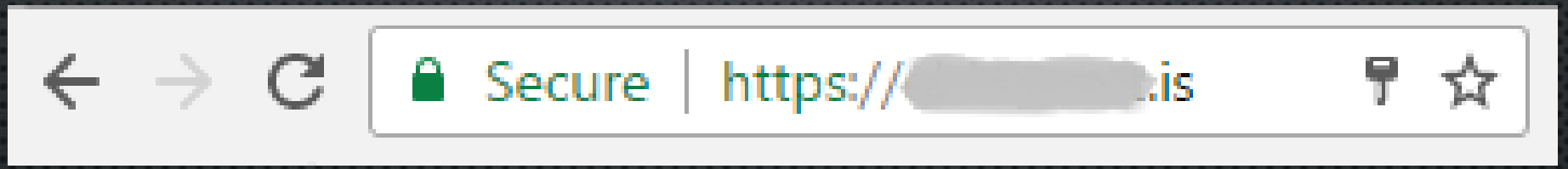
http://www.paypal-payments.com-paypay-service.xyz

https://isc.sans.edu/



https://isc.sans.edu/diary/A+very+convincing+Typosquatting+++Social+Engineering+campaign+is+targeting+Santander++corporate+customers+in+Brazil/22157

HVAÐ MEÐ HTTPS?



censys

About Search Reports API Raw Data Login

paypal AND parsed.issuer_dn: "C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3"

IPv4 Hosts | Top Million Websites | Certificates

CN=paypal-limited.com.mpp.webapps-signin.ax171

C=US, O=

29cfbef

Trusted Le

parsed.ext

parsed.iss

CN=paypal-verify.service.g

C=US, O=Let's Encrypt, C

1a7f0b5cdddedd297d391

Trusted Leaf Certificate

parsed.extensions.subjec

parsed.issuer_dn: C=US,

CN=paypal-

C=US, O=

35ca79be20ace901d37a7aca40cbd00d215f3e3

Trusted Leaf Certificate

parsed.ext

parsed.iss

CN=verify.secure-paypal-update.co

C=US, O=Let's Encrypt, CN=Let's E

130a17764176e3a2c93d1ee71419

Trusted Leaf Certificate

parsed.extensions.subject_alt_nam

parsed.issuer_dn: C=US, O=Let's

CN=paypal-

C=US, O=

a1624e5

Trusted Le

parsed.extensions.subject_alt_name.dns_names: pay

parsed.issuer_dn: C=US, O=Let's Encrypt,

Whois & Quick Stats

Registrant Org	Repossessed by Go Daddy is associated with ~148,297 other domains
Registrar	GODADDY.COM, LLC
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	Created on 2016-09-01 - Expires on 2017-09-01 - Updated on 2016-09-08
Name Server(s)	NS09.DOMAINCONTROL.COM (has 41,188,295 domains) NS10.DOMAINCONTROL.COM (has 41,188,295 domains)
IP Address	160.153.162.23 - 1,047 other sites hosted on this server
IP Location	- Arizona - Scottsdale - Godaddy.com Llc
ASN	AS26496 AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US (registered Oct 01, 2002)
Domain Status	Registered And Active Website
Whois History	17 records have been archived since 2004-07-05
IP History	29 changes on 15 unique IP addresses over 13 years
Registrar History	4 registrars with 3 drops
Hosting History	26 changes on 12 unique name servers over 11 years

DÆM

for using PayPal. To see the full transaction details,
****
log in to your PayPal account.</td>

PayPal

Jan 10, 2017 05:38:32 PST
Transaction ID: 1337

Your funds will be transferred when the merchant processes your payment. Any m
PayPal account at that time will be used before any other payment source.

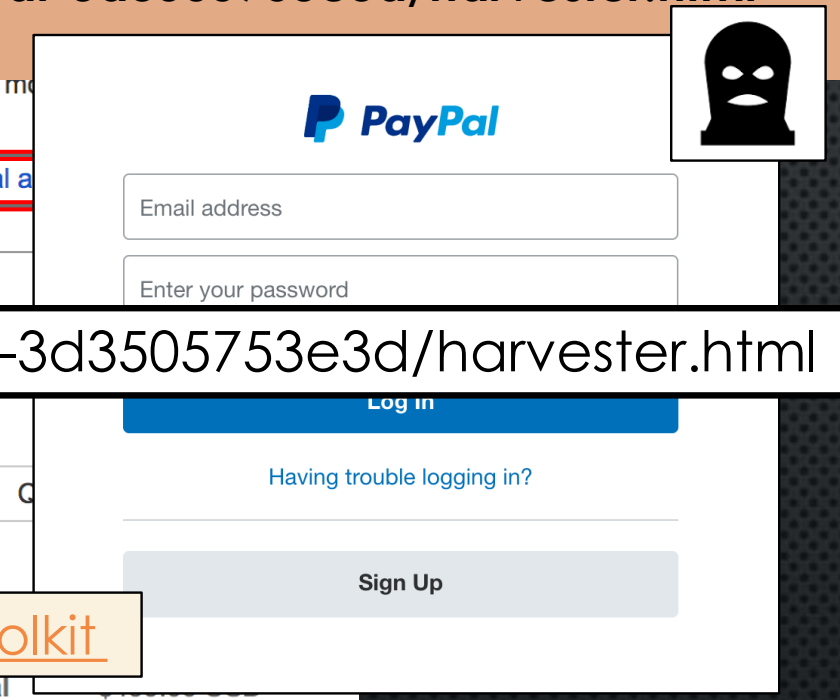
Thanks for using PayPal. To see the full transaction detail, log in to your PayPal a

Description | Unit price | Q

$499.00 USD

Subtotal
Total $499.00 USD

Charge will appear on your credit card statement as "PAYPAL *COURSERAINC"
Payment sent to paypal@coursera.org. See our refunds policy if you believe you have been overcharged.



Secure https://foo.bar.com/2623df9f-8274-43b7-96af-3d3505753e3d/harvester.html

https://github.com/trustedsec/social-engineer-toolkit

See our **refunds policy**

URL Shortener https://goo.gl/

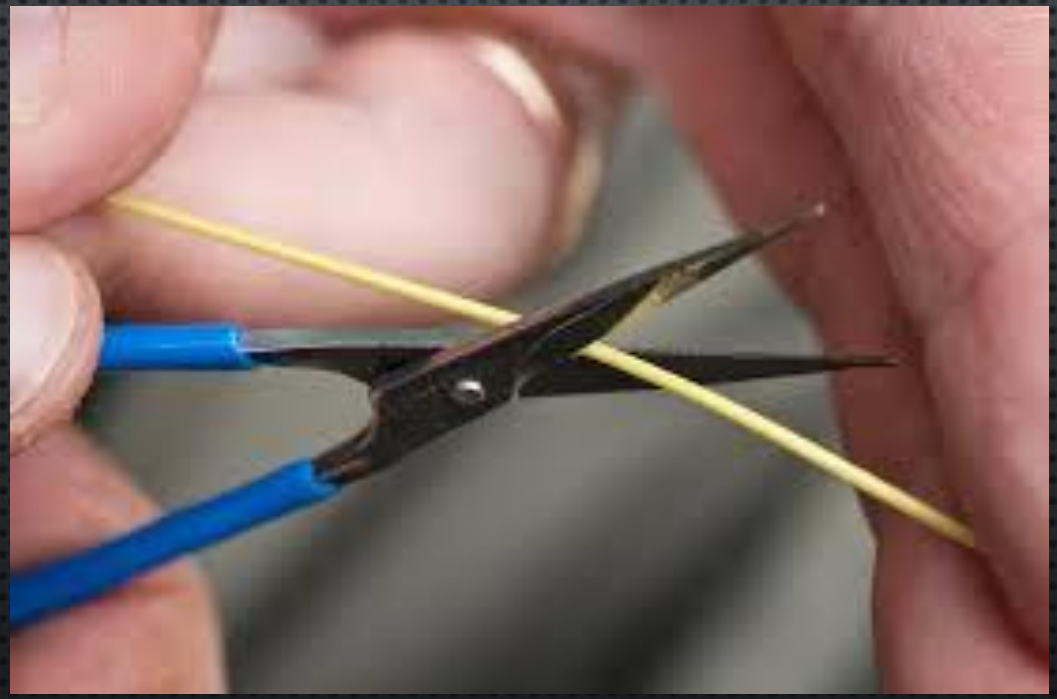
http://checkshorturl.com/expand.php

Aðferðir til að dyljast

Markmið: Torvelda rannsókn og fela slóð

- Löng keðja vísana
- Blokklistar sem útiloka þekkta rannsakendur
- Leyfa hverri IP tölu aðeins takmarkaðan aðgang
- GeoBlocking
- DNS tækni s.s. Fast flux
- …

KLIPPT Á TAUMINN

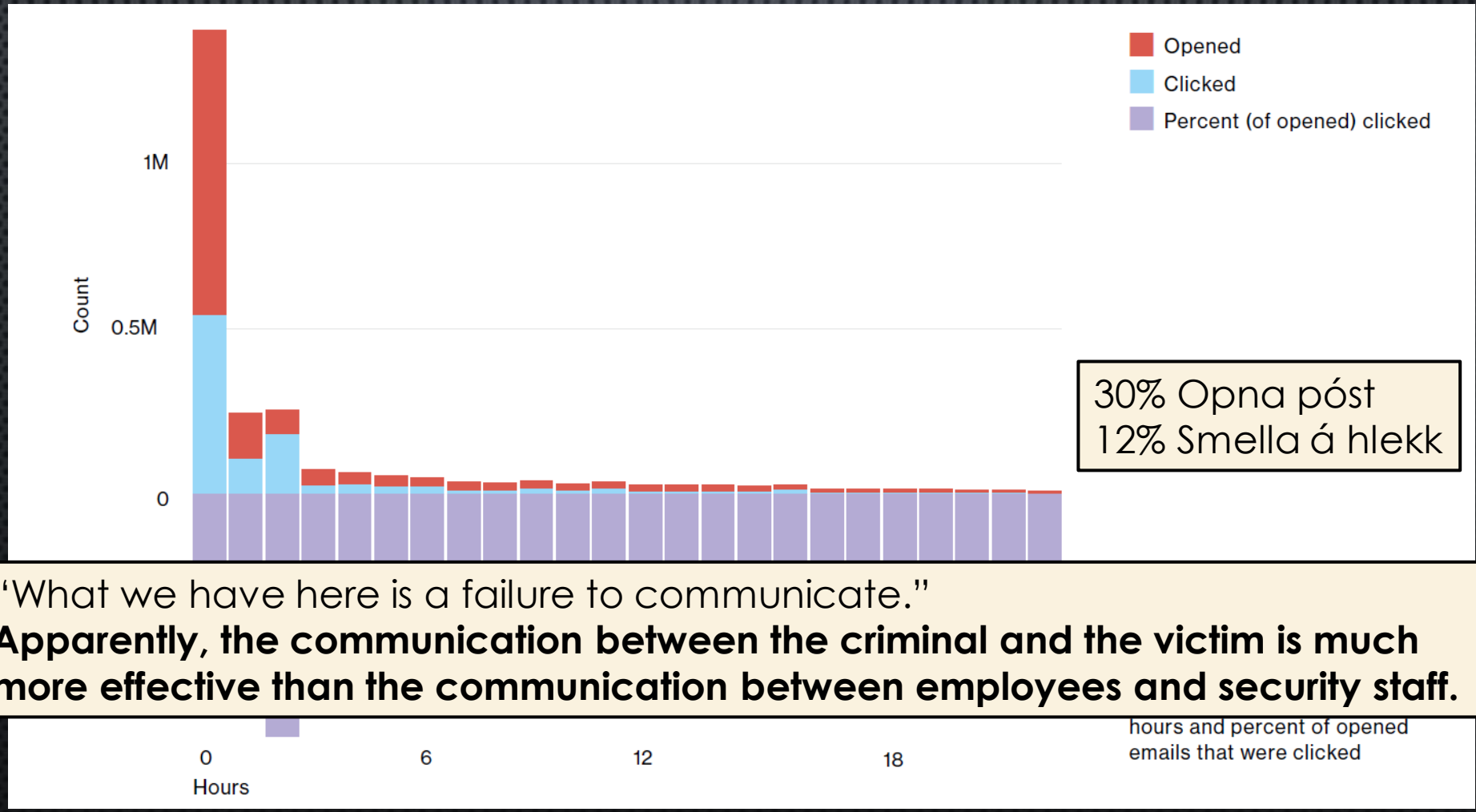


Viðbrögð CERT og hýsingaraðila

- Virkt alþjóðlegt samstarf CERT teyma og einkaaðila
- Ábyrgðaraðilar beiðnir að loka / hreinsa
- Tímabundin lokun á IP tölum

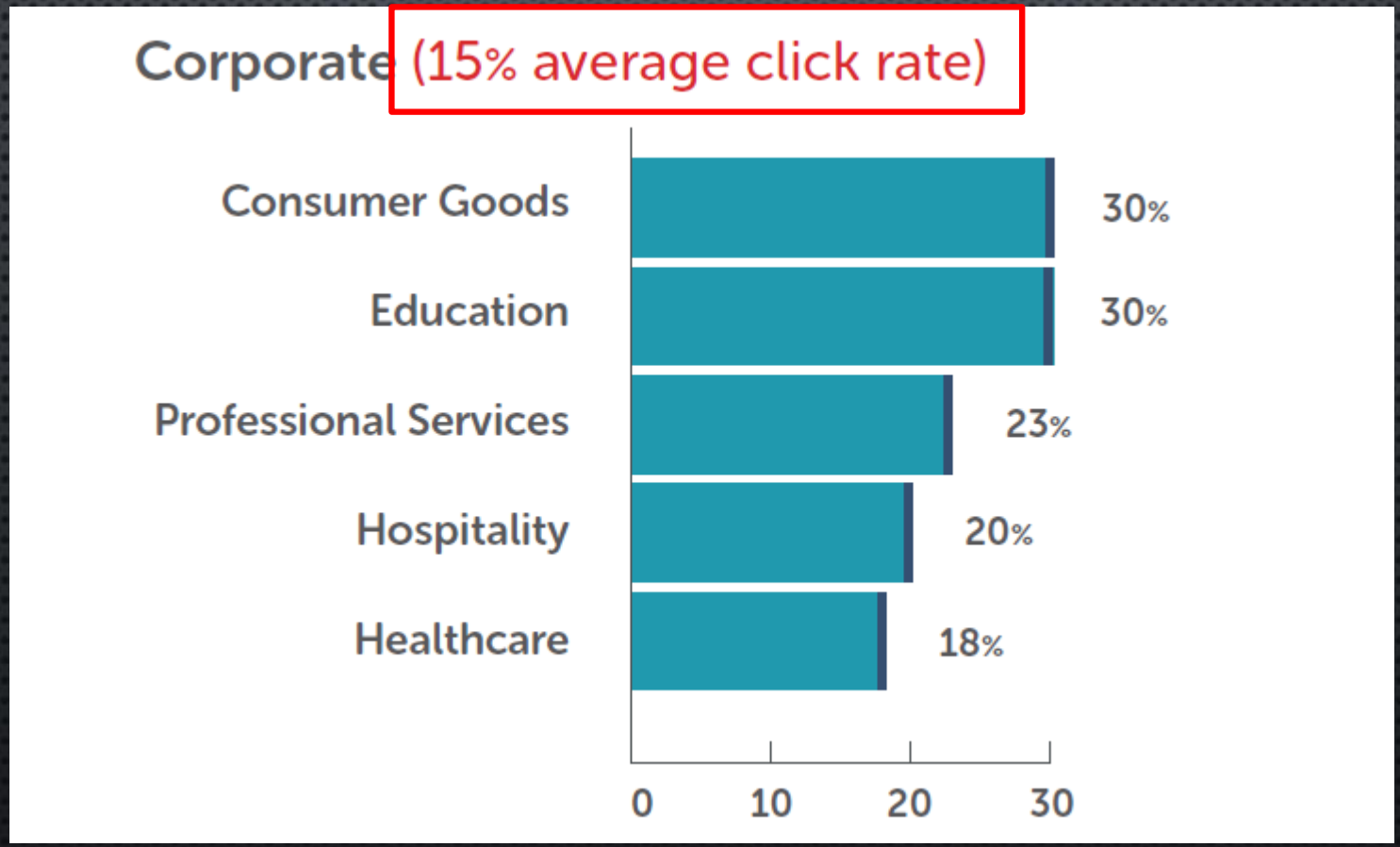
NOTANDINN: ÉG FELL EKKI FYRIR ÞESSU

Verizon: DBIR 2016



30% Opna póst
12% Smella á hlekk

"What we have here is a failure to communicate."
Apparently, the communication between the criminal and the victim is much more effective than the communication between employees and security staff.



Wombat: State of the phish 2017

FORVARNIR - ÞJÁLFA NOTANDANN

- Ekki taka skyndiákvarðanir – Ekki smella án þess að hugsa – Varist tilbúið neyðarástand
- Skoða sendanda – áttu von á pósti frá þessum aðila?
- Skoða efnislínu og ávarp
- Skoða tungumál, málvillur og stafsetningarvillur
- Skoða hlekki og hvað RAUNVERULEGA er bak við þá
- Varast hlekki og fara frekar gegnum þjónustuvef fyrirtækis
- Varist viðhengi – fæst fyrirtæki senda viðskiptavinum viðhengi óumbeðið
- Skoða URL línu þegar hlekkjuð síða er opin í vafra
  - Misritun? Líkleg blekking? HTTPS?
- Hvað er beðið um? Fyrirtæki biðja notendur t.d. ekki um viðkvæmar upplýsingar í tölvupósti.
- Hugsa áður en viðkvæmar upplýsingar eru slegnar inn – hringja í sendanda ef í vafa
- Henda vafasömum pósti – Raunveruleg fyrirtæki ítreka erindi
- Áframsenda beint á þekktan viðtakanda ef í vafa með beiðni um staðfestingu

https://www.cert.is/is/node/33.html

Verja kerfi

- Ruslpóstsíur
- Blokkun á þekkt slæm lén og jafnvel þekkt "slæm" TLD https://www.spamhaus.org/statistics/tlds/
- "Vírusvarnir" sem greina hlekki í pósti og URL línur sem öruggar
- Scriptblocker, Ad-blocker, popup-blocker í vafra
- Text-only & ekki "preview" á tölvupósti
- **Uppfæra allan hugbúnað reglulega!**

AÐGERÐIR TIL AÐ MINNKA SKAÐA

- EINSTÖK OG FLÓKIN LYKILORÐ
- TRYGG SKRÁNING Á LYKILORÐUM
- TVEGGJA ÞÁTTA AUÐKENNING

LastPass •••|

dashlane

KANNA/SKRÁ PHISHING LÉN OG SENDENDUR

https://www.phishtank.com/

https://safebrowsing.google.com/safebrowsing/report_phish/?hl=en

https://virustotal.com

VARNIR GEGN FÖLSUN TÖLVUPÓSTS

- AUÐKENNING MEÐ RAFRÆNNI UNDIRRITUN
- DMARC, SPF, DKIM

https://www.gnupg.org/

https://dmarc.org/

Bregðast við leka

- Gera ljóst hvað telst vera möguleg veiðitilraun og hvert á að tilkynna
  - Starfsmaður tilkynnir um tapað lykilorð
  - Starfsmaður tilkynnir um að hafa smellt á vafasaman hlekk
  - Starfsmaður tilkynnir um að hafa opnað „skrítið“ viðhengi
- **Ekki skömm að falla í gildruna**
- Gera áætlun um viðbrögð
  - Breyta lykilorðum
  - Aftengja tölvur og rannsaka
  - Tilkynna kortafyrirtæki – loka kortum

Takk fyrir