



# Internet 101

How secure are you?

Warren Finch

<https://wiki.apnictraining.net/20201201-pacnog>

# Attack Trends



## LIVE CYBER THREAT MAP

25,662,149 ATTACKS ON THIS DAY

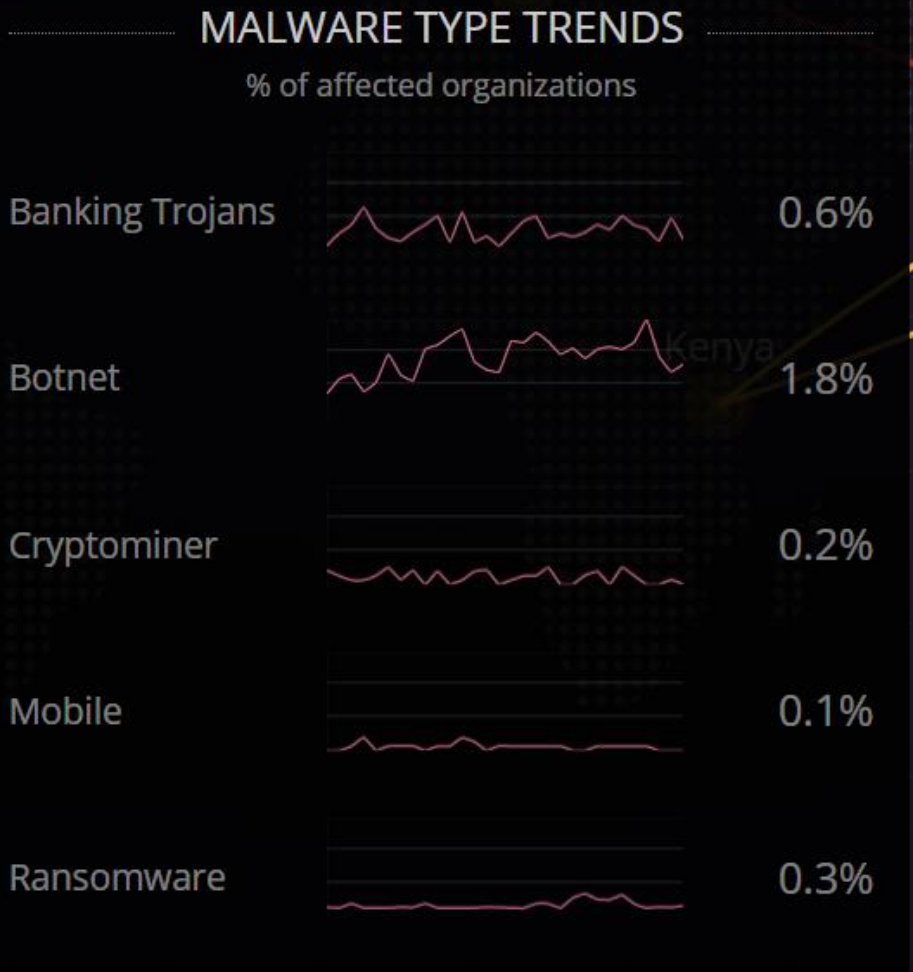
**DON'T WAIT TO BE ATTACKED  
PREVENTION STARTS NOW >**

RECENT DAILY ATTACKS



ATTACKS Current rate **4**

- cnc server.TC.gfrb  
12:14:22 US, United States → Vietnam
- Web Client Enforcement Violation  
12:14:22 Netherlands → United Kingdom
- infecting website.TC.gkrk  
12:14:22 US, United States → Switzerland
- Andromeda.TC.bzn  
12:14:21 Russia → India
- NTP Enforcement Violation  
12:14:21 Italy → Italy
- infecting website.TC.gkrk  
12:14:21 US, United States → Switzerland
- Web Client Enforcement Violation  
12:14:21 South Korea → Kenya



TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Nepal
- Mongolia
- Indonesia
- Guatemala
- Taiwan

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Government
- Communications

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

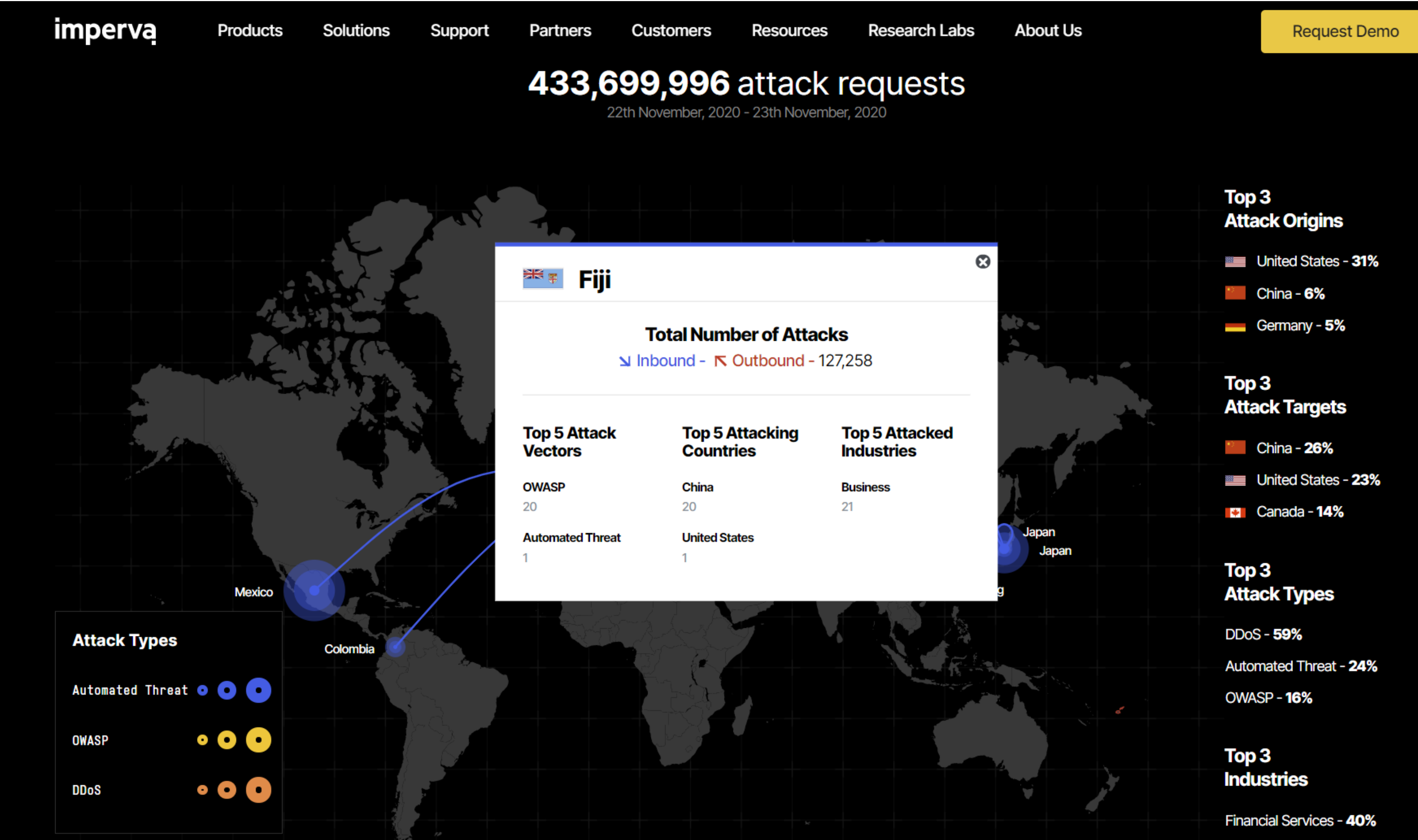
- Backdoor
- Banking
- Botnet

- Malware
- Phishing
- Exploit





# Attack Trends



<https://www.imperva.com/cyber-threat-attack-map/>

# Internet usage



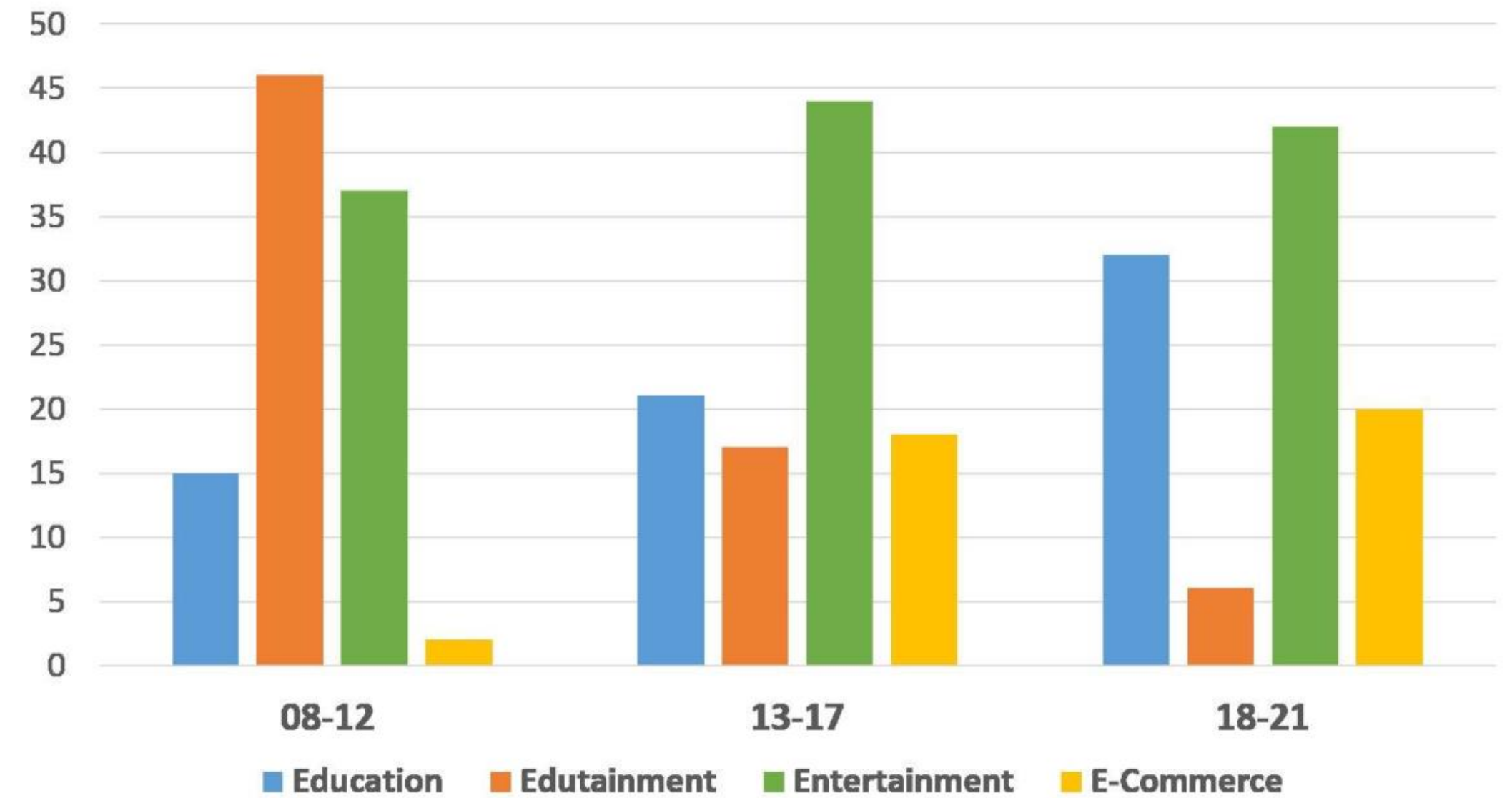
Internet Usage and Population Statistics for Oceania - 2019						
OCEANIA	Population (2019 Est.)	Users, in Dec/2000	Internet Usage, 30-June-2019	% Population (Penetration)	Internet % users	Facebook 31-Dec-2018
<a href="#">American Samoa</a>	55,727	n/a	24,000	43.1 %	0.1 %	22,000
<a href="#">Antarctica</a>	2,700	n/a	4,400	100.0 %	0.0 %	1,800
<a href="#">Australia</a>	25,088,636	6,600,000	21,711,706	86.5 %	75.8 %	15,000,000
<a href="#">Australia, Ext. Terr.</a>	1,651	n/a	n/a	n/a	n/a	n/a
<a href="#">Christmas Island</a>	2,205	464	1,000	45.4 %	0.0 %	400
<a href="#">Cocos (Keeling) Is.</a>	596	n/a	80	13.4%	0.0 %	70
<a href="#">Cook Islands</a>	17,462	n/a	11,377	65.2 %	0.0 %	8,600
<a href="#">Fiji</a>	918,757	7,500	500,958	54.5 %	1.7 %	470,000
<a href="#">French Polynesia</a>	288,506	8,000	209,744	72.7 %	0.7 %	150,000
<a href="#">Guam</a>	167,245	5,000	134,649	80.5 %	0.5 %	110,000
<a href="#">Kiribati</a>	120,428	1,000	32,947	27.4%	0.1 %	30,000
<a href="#">Marshall Islands</a>	53,211	500	20,593	38.7 %	0.1 %	20,000
<a href="#">Micronesia</a>	106,983	2,000	56,193	52.5 %	0.2 %	21,000
<a href="#">Nauru</a>	11,260	n/a	6,418	57.0 %	0.0 %	3,400
<a href="#">New Caledonia</a>	283,376	24,000	232,368	82.0 %	0.8 %	150,000
<a href="#">New Zealand</a>	4,792,409	830,000	4,351,987	90.8 %	15.2 %	3,100,000
<a href="#">Niue</a>	1,618	450	1,485	91.2 %	0.0 %	820
<a href="#">Norfolk Island</a>	1,748	n/a	796	45.5 %	0.0 %	80
<a href="#">Northern Marianas</a>	55,246	n/a	40,000	72.4 %	0.1 %	36,000
<a href="#">Palau</a>	22,206	n/a	7,860	35.4 %	0.0 %	5,800
<a href="#">Papau New Guinea</a>	8,586,525	135,000	962,550	11.2 %	3.4 %	670,000
<a href="#">Pitcairn Islands</a>	50	n/a	170	n/a	n/a	150
<a href="#">Samoa</a>	198,909	500	100,000	50.3%	0.3 %	94,000
<a href="#">Smaller Territories (4)</a>	3,902	n/a	n/a	n/a	n/a	n/a
<a href="#">Solomon Islands</a>	635,254	2,000	75,722	11.9 %	0.3 %	68,000
<a href="#">Terres Australes</a>	n/a	n/a	n/a	n/a	n/a	n/a
<a href="#">Tokelau</a>	1,340	66	800	59.7%	0.0 %	410
<a href="#">Tonga</a>	110,041	1,000	57,822	52.5 %	0.2 %	54,000
<a href="#">Tuvalu</a>	11,393	n/a	5,619	49.3 %	0.0 %	1,700
<a href="#">Vanuatu</a>	288,017	3,000	82,764	28.7%	0.3 %	63,000
<a href="#">Wallis &amp; Futuna</a>	11,617	n/a	3,900	33.6 %	0.0 %	3,400
<b>TOTAL OCEANIA</b>	<b>41,839,201</b>	<b>7,620,480</b>	<b>28,636,278</b>	<b>68.4 %</b>	<b>100.0 %</b>	<b>20,068,690</b>

<https://www.internetworldstats.com/stats6.htm>

# Internet usage



- How do you use the internet?
- What information do you share?
- What information do you look at?
- What information do you search for?
- Do you use it for banking?



Age	Male	Female	NA	Total	Ratio
08-12	256	145	43	444	20.91
13-17	325	346	89	760	35.80
18-21	421	285	213	919	43.29

TABLE I: Statistics of age and gender-wise participation

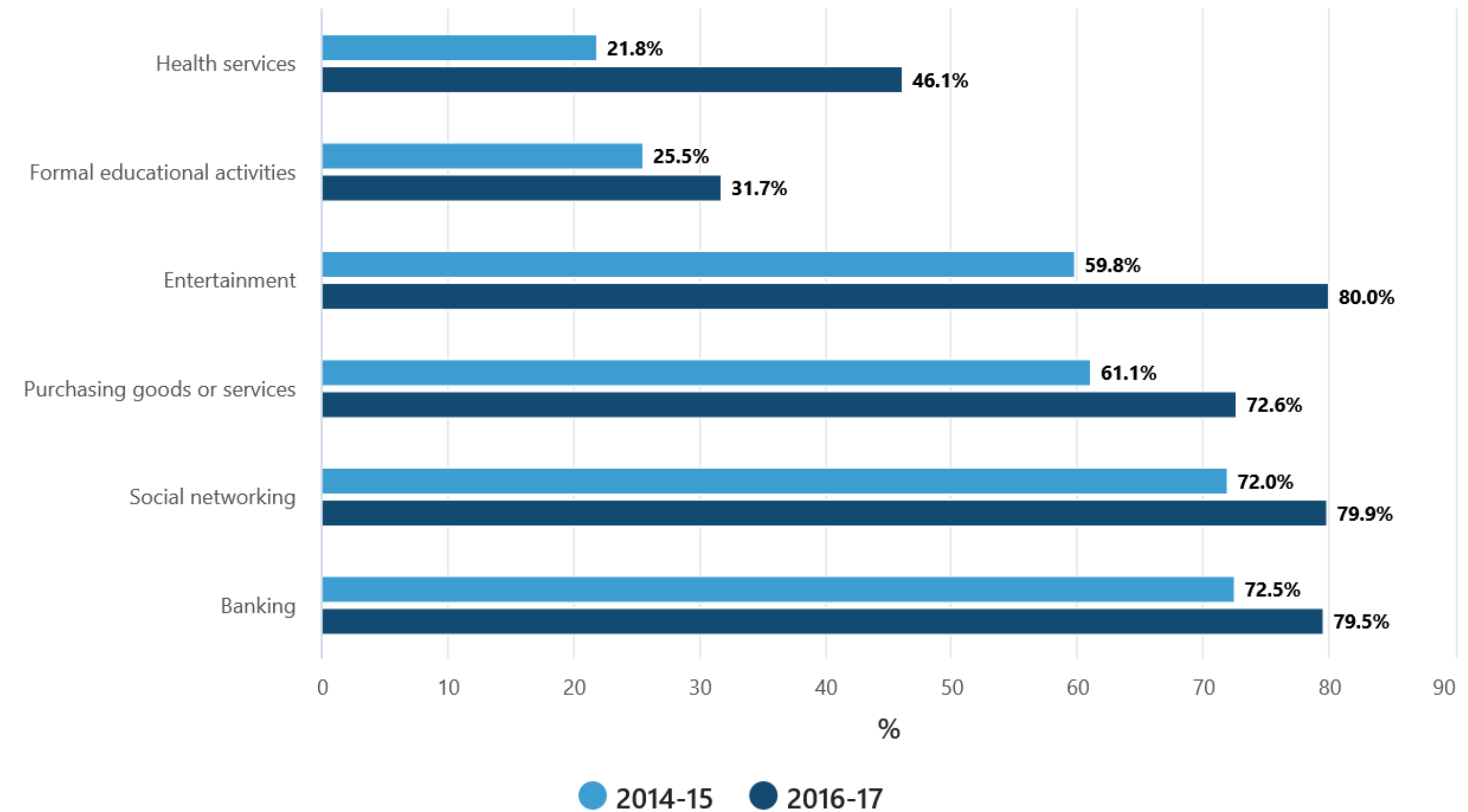


# Internet usage



- How do you use the internet?
- What information do you share?
- What information do you look at?
- What information do you search for?
- Do you use it for banking?

Internet users, by reasons for accessing the internet, 2014-15 and 2016-17

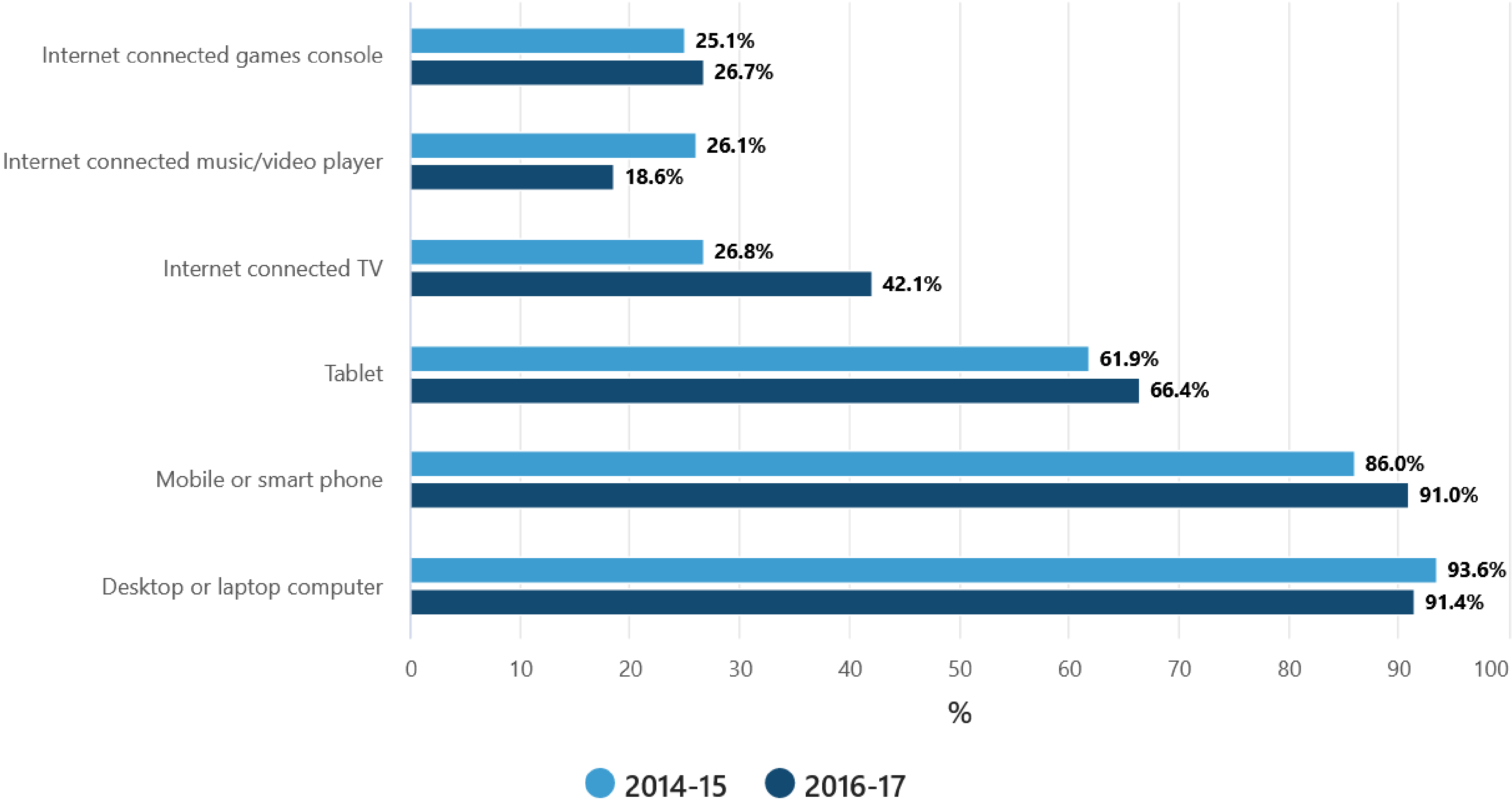


<https://www.abs.gov.au/statistics/industry/technology-and-innovation/household-use-information-technology/latest-release>

# Which Device



- What devices do you use?



<https://www.abs.gov.au/statistics/industry/technology-and-innovation/household-use-information-technology/latest-release>



# YOU ARE A TARGET



You may not realize it, but you are a target for cyber criminals. Your computer, mobile devices, accounts and your information have tremendous value. Check out the different methods a criminal could use your information against you to make money or commit other crimes.



## Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- Your bank or financial accounts, where they can steal or transfer your money
- Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data
- Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name
- Your UPS or FedEx accounts, where they ship stolen goods in your name

## Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- All the names, email addresses and phone numbers from your contact list
- All of your personal or work email

## Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- Your credit card information
- Your tax records and past filings
- Your financial investments and retirement plans

## Extortion

Once hacked, cyber criminals can take over by:

- Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures
- Encrypting all the data on your computer and demanding payment to decrypt it
- Tracking all websites you visit and threatening to publish them

## Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- Your online gaming characters, gaming goods

## Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- Sending out spam to millions of people
- Launching Denial of Service attacks

## Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- Your Facebook, Twitter or LinkedIn account
- Your email accounts
- Your Skype or other IM accounts

## Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:




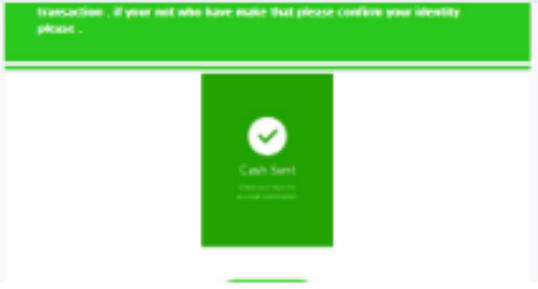








- Hosting phishing websites to steal other people's usernames and passwords
- Hosting attacking tools that will hack people's computers
- Distributing child pornography, pirated videos or stolen music

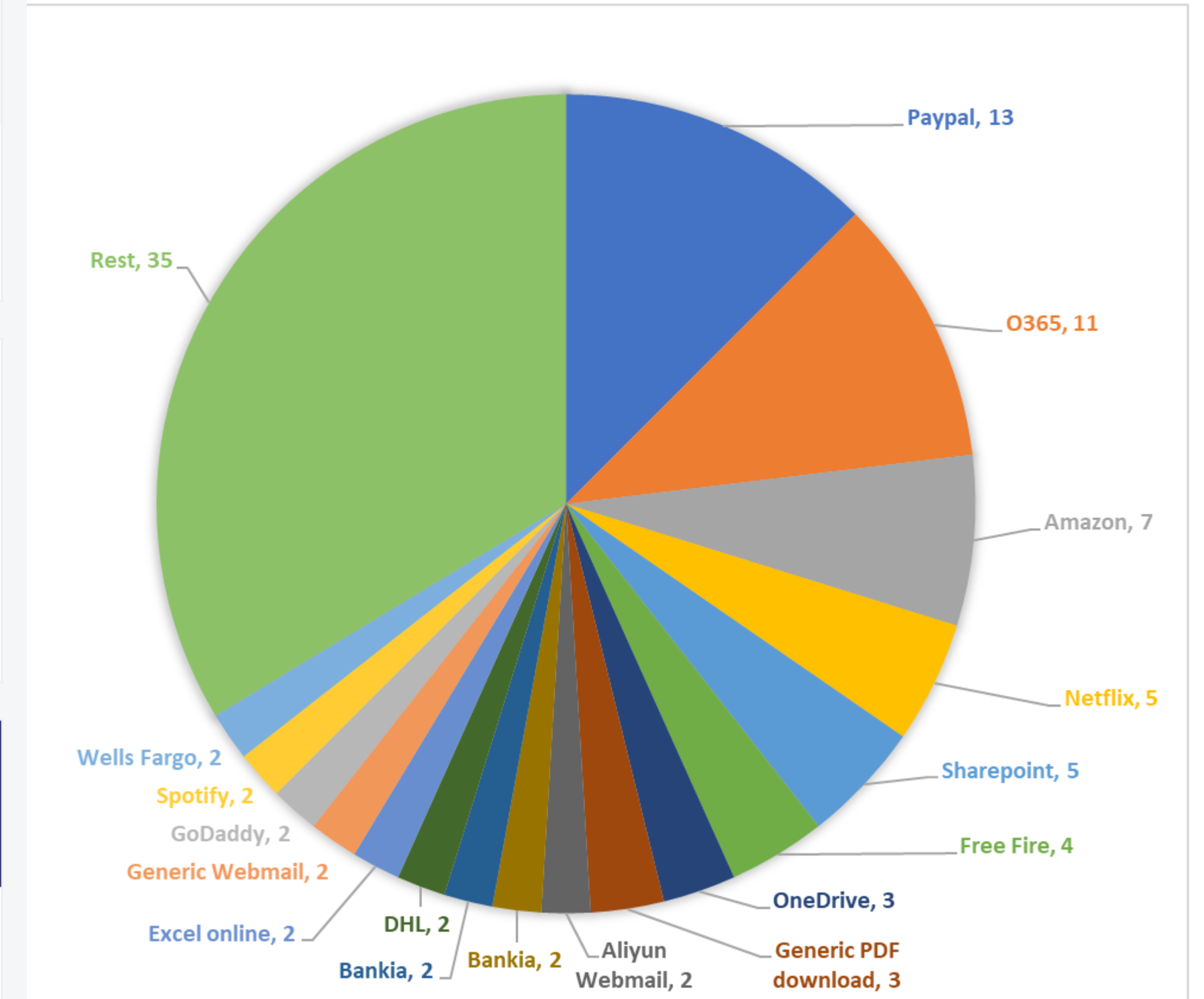
Fortunately, by taking a few simple steps, you can protect your organization and your family. To learn more, visit: [sans.org/security-awareness](https://www.sans.org/security-awareness). This poster was developed from security awareness expert **Brian Krebs**. Learn more about cyber criminals at: [krebsonsecurity.com](https://www.krebsonsecurity.com).



# Phishing kits



 APPLE LETTER INBOX TO ALL \$5.00	 Amazon.com LETTER INBOX TO ALL 2020   V1 \$3.00	 10 K Chase Login , + Email Access \$400.00	 LifeTime Celeron Letter CASHUP Inbox To ALL 2020 \$15.00
 Capital One Scampage 2020   FRESH AND PRIVATE \$30.00	 TUNNEL BEAR VPN CONFIG OPEN BULLET   CPM +1K \$5.00	 Office365 Emails Checker 2020 \$25.00	 Commonwealth Bank Scampage 2020 - AUS SCAMPAGE \$50.00
 Scotiabank (Online Banking) Scampage 2020 - CA SCAMPAGE \$50.00	 Huntington Bank INBOX   Letter INBOX   BYPASS BOTS   V2 \$8.00	 Westpac One Bank (Online Banking) Scampage 2020 - AUS SCAMPA... \$50.00	 NATWEST UK Bank (Online Banking) Scampage 2020 - UK SCAMPAGE... \$25.00



<https://isc.sans.edu/forums/diary/Phishing+kits+as+far+as+the+eye+can+see/26660/>

# How much is your data worth?



Your identity is a steal on the Dark Web. Here are what the most common pieces of information sell for:

**PrivacyAustralia**

<b>Social security number</b> \$1	<b>Online payment services login info</b> (e.g. Paypal) \$20-\$200	<b>Credit or debit card</b> (credit cards are more popular) With CVV number \$5 With bank info \$15 Fullz info* \$30
<b>Drivers license</b> \$20	<b>Loyalty accounts</b> \$20	<b>General non-financial institution logins</b> \$1
<b>Diplomas</b> \$100-\$400	<b>Passports (US)</b> \$1000-\$2000	<b>Subscription services</b> \$1 - \$10
		<b>Medical records</b> \$1 - \$1000**

\*Fullz info is a bundle of information that includes a "full" package for fraudsters: name, SSN, birth date, account numbers and other data that make them desirable since they can often do a lot of immediate damage.

\*\*Depends on how complete they are as well as if it is a single record or an entire database.

**Note:** Prices can vary over time and prices listed below are an estimation and aggregation based on reference articles and hands on experience of Experian cyber analyst the last two years.

<https://privacyaustralia.net/dark-web-personal-data/>



# What data are you leaking?



- Operating system
- Browser details
- Hardware details
- Location information
- Passwords
- Auto-fill information

BrowserLeaks.com IP Address Lookup

It has long been believed that IP addresses and Cookies are the only reliable digital fingerprints used to track people online. But after a while, things got out of hand when modern web technologies allowed interested organizations to use new ways to identify and track users without their knowledge and with no way to avoid it.

BrowserLeaks is all about browsing privacy and web browser fingerprinting. Here you will find a gallery of web technologies security testing tools that will show you what kind of personal identity data can be leaked, and how to protect yourself from this.

IP Address JavaScript

The main tool that illustrates server-side can determine the user's identity. It has basic features such as IP Address and HTTP Headers, IP-based geolocation, and DNS Leak Test, IPv6 Leak Test.

WebRTC Leak Test

IP address detection using JavaScript. WebRTC API, the web browser communication protocol, allows a web browser to connect to a server and shares information about local IP addresses even if you are behind NAT and using a VPN.

WebGL Report

WebGL Browser Report checks WebGL support and other WebGL and GPU capabilities to produce WebGL Fingerprinting, exposes your browser identity. Also, this page can enable or disable WebGL in your web browser.

### Device Info

- Accepted Content Types
- Accepted Content Encodings
- Accounts Logged In
- ActiveX
- Ad Blocker
- AudioContext
- Battery Status
- Bluetooth
- Browser
- Browser Full Screen Mode
- Browser MIME Types
- Browser Plugins
- Browser Window Size
- Cache-Control
- Canvas
- City
- Connection Type
- Content Filtering
- Cookies

**Device Type / Model:** Desktop or laptop

**Operating System:** Windows 10 version 10.0 (64-bit) or 2019 version 10.0 (64-bit)

**True Operating System Core:** Unknown. Detected as Windows 10.0 (64-bit) blocked by browser setting(s)/extension(s).

**Browser:** Opera version 71.0.3770.198 (64-bit) (Engine: Blink)

**True Browser Core:** Chrome

**Browser Build Number / Identifier:** 2003-01-07 / Unknown. Detected as Opera blocked by browser setting(s)/extension(s).

**IP Address (WAN):** 106.70. (IPv4)

**Tor Relay IP Address:** No

**VPN IP Address:** Not detected

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	10.73	1698.7	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 OPR/71.0.3770.198
HTTP_ACCEPT Headers	2.8	6.98	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.9
Browser Plugin Details	6.94	122.52	Plugin 0: Chromium PDF Plugin; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf); Plugin 1: Chromium PDF Viewer; (mhjfbmdgcfjbbpaeojofohoefghehjai; (application/pdf; pdf); Plugin 2: News feed handler; (emrlgamfkfdemjmlfjeipglcfpomikn; (application/atom+xml; application/rss+xml; rss).
Time Zone Offset	5.82	56.53	-600
Time Zone	8.24	301.8	Australia/Brisbane
Screen Size and Color Depth	15.27	39636.33	2048x1153x24
System Fonts	3.86	14.55	Arial, Arial Black, Arial Narrow, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Are Cookies Enabled?	0.18	1.13	Yes
Limited supercookie test	1.55	2.93	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: true, indexed db: true
Hash of canvas fingerprint	5.07	33.48	184c42ab72952c9ea0b2ef182038a365
Hash of WebGL fingerprint	6.4	84.69	768371105602a80687eeb0#0d3260bc
WebGL Vendor & Renderer	5.45	43.81	Google Inc.--ANGLE (Intel(R) UHD Graphics 620 Direct3D11 vs_5_0 ps_5_0)
DNT Header Enabled?	1.04	2.06	True
Language	0.98	1.97	en-US
Platform	1.34	2.52	Win32
Touch Support	0.73	1.86	Max touchpoints: 0, TouchEvent supported: false, onTouchStart supported: false
Ad Blocker Used	0.38	1.3	False
AudioContext fingerprint	3.29	9.79	124.04347527516074
CPU Class	0.15	1.11	N/A
Hardware Concurrency	2.22	4.66	8
Device Memory (GB)	2.48	5.59	8

# What data are you leaking?



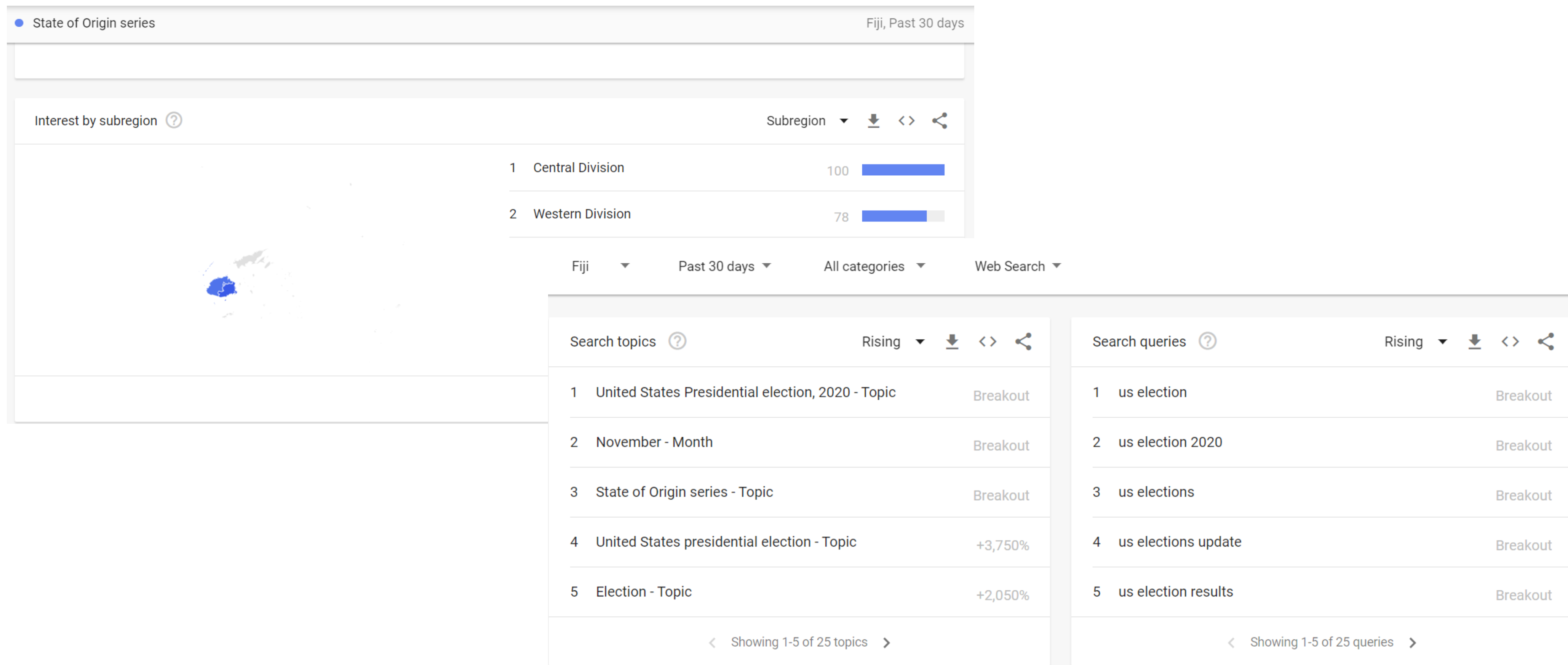
- Every time you visit a web page, you leave a trace.
- Demo websites:
  - <https://webkay.robinlinus.com>
  - <https://clickclickclick.click/>
  - <https://browserleaks.com>
  - <https://browserleaks.com/social>
  - <http://www.deviceinfo.me/>
  - <https://www.ghacks.net/2015/12/28/the-ultimate-online-privacy-test-resource-list/>



# What do you search?



- Every time you search, you leave a trace.
- <https://trends.google.com.au/trends/explore?geo=FJ>



# Are you being tracked?



- Browser fingerprinting
- Tracking ads
- Do not track option

Our tests indicate that you have you have **strong protection against Web tracking**, though your software isn't checking for Do Not Track policies.

## IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Unblocking 3rd parties that honor <u>Do Not Track</u> ?	<u>No</u>
Protecting you from <u>fingerprinting</u> ?	<u>Your browser has a unique fingerprint</u>

<https://coveryourtracks.eff.org>

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	⚠ partial protection
Does your blocker stop trackers that are included in the so-called “ <b>acceptable ads</b> ” whitelist?	✓ yes
Does your browser unblock 3rd parties that promise to honor <b>Do Not Track</b> ?	✗ no
Does your browser protect from <b>fingerprinting</b> ?	✗ your browser has a unique fingerprint

<https://panoptickick.eff.org>



# What websites you visit?



- What happens when you visit a website?
- You may get more than you think?
- How are these sites connected?
  - <https://academy.apnic.net>
  - <https://nog.bt/>
  - <https://kuenselonline.com/>

Extension ...beam 3.0 | moz-extension://dbef457e-5bd5-46a7-9fce-a670cab205e6/index.html

DATA GATHERED SINCE: OCT 13 2020    YOU HAVE VISITED: 5 SITES    YOU HAVE CONNECTED WITH: 23 THIRD PARTY SITES

### Recent Site

GRAPH VIEW

The graph illustrates the network of connections between the visited sites and their associated third-party sites. The central node is NOG, which is connected to a blue square node and a white circular node with a blue grid pattern. The white circular node is further connected to another white circular node with a blue grid pattern. Each of these nodes is connected to several smaller white triangular nodes representing other third-party sites.

<https://addons.mozilla.org/en-US/firefox/addon/lightbeam-3-0/>

# Passwords

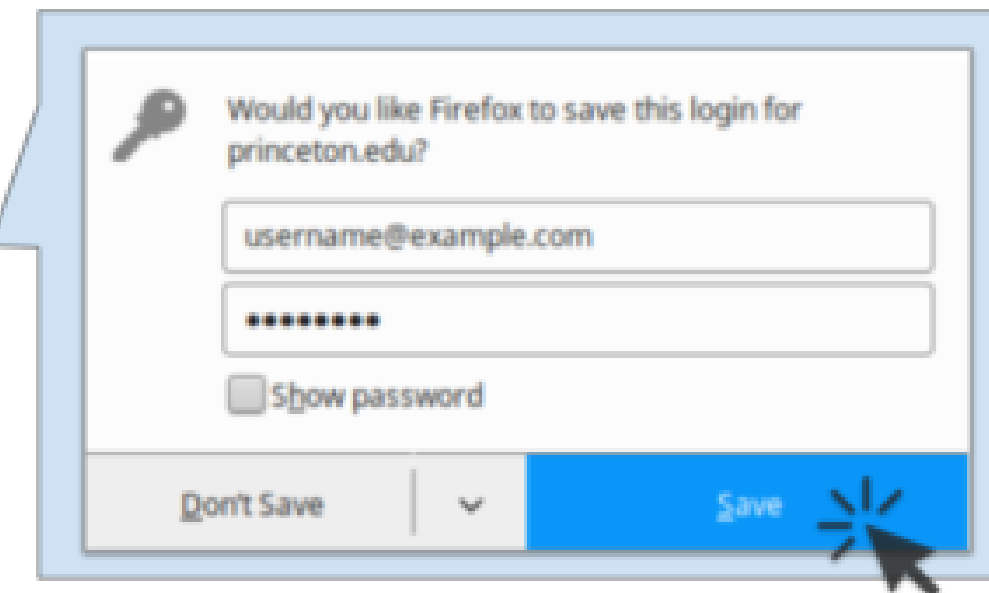


- Do you save passwords in the web browser?

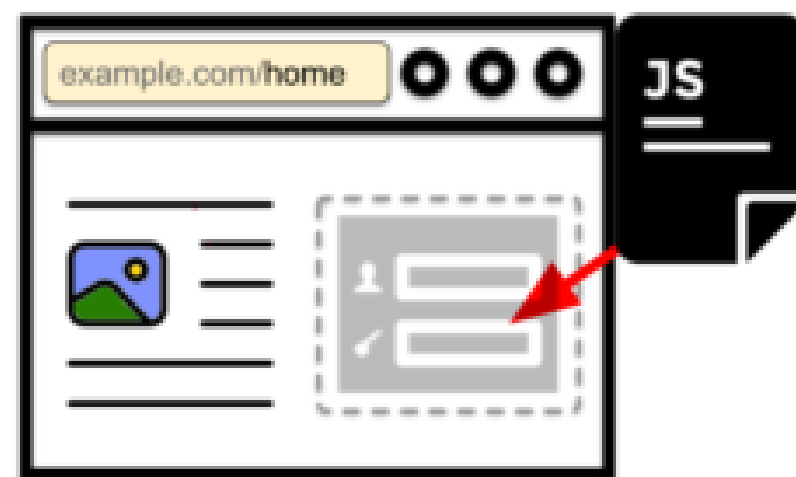
User submits a login or registration form, clicks "Save" to store the credentials.



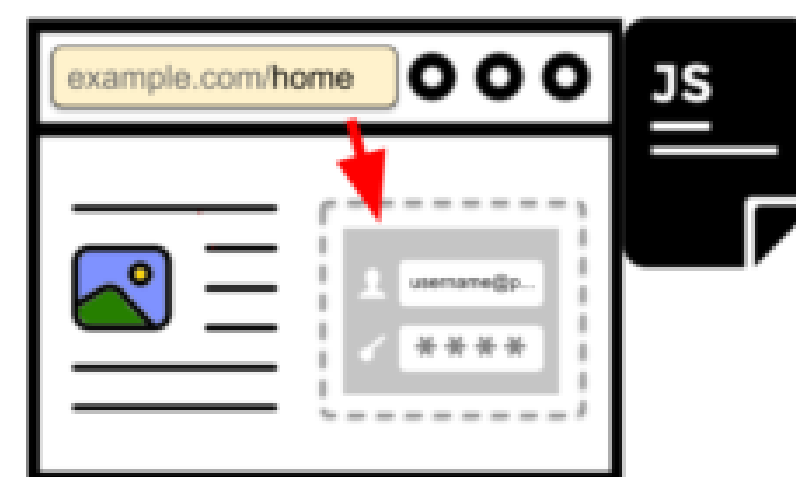
Third-party script is not present on the login page



User visits a non-login page on the same site; this time the third party script is present



1. Third-party script injects an invisible login form



2. Login manager fills in user's email and password



3. The script reads the email address from the form and sends it hashes to third-party servers

- MD5(email)
- SHA1(email)
- SHA256(email)

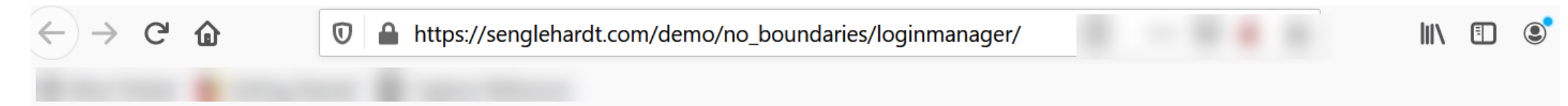
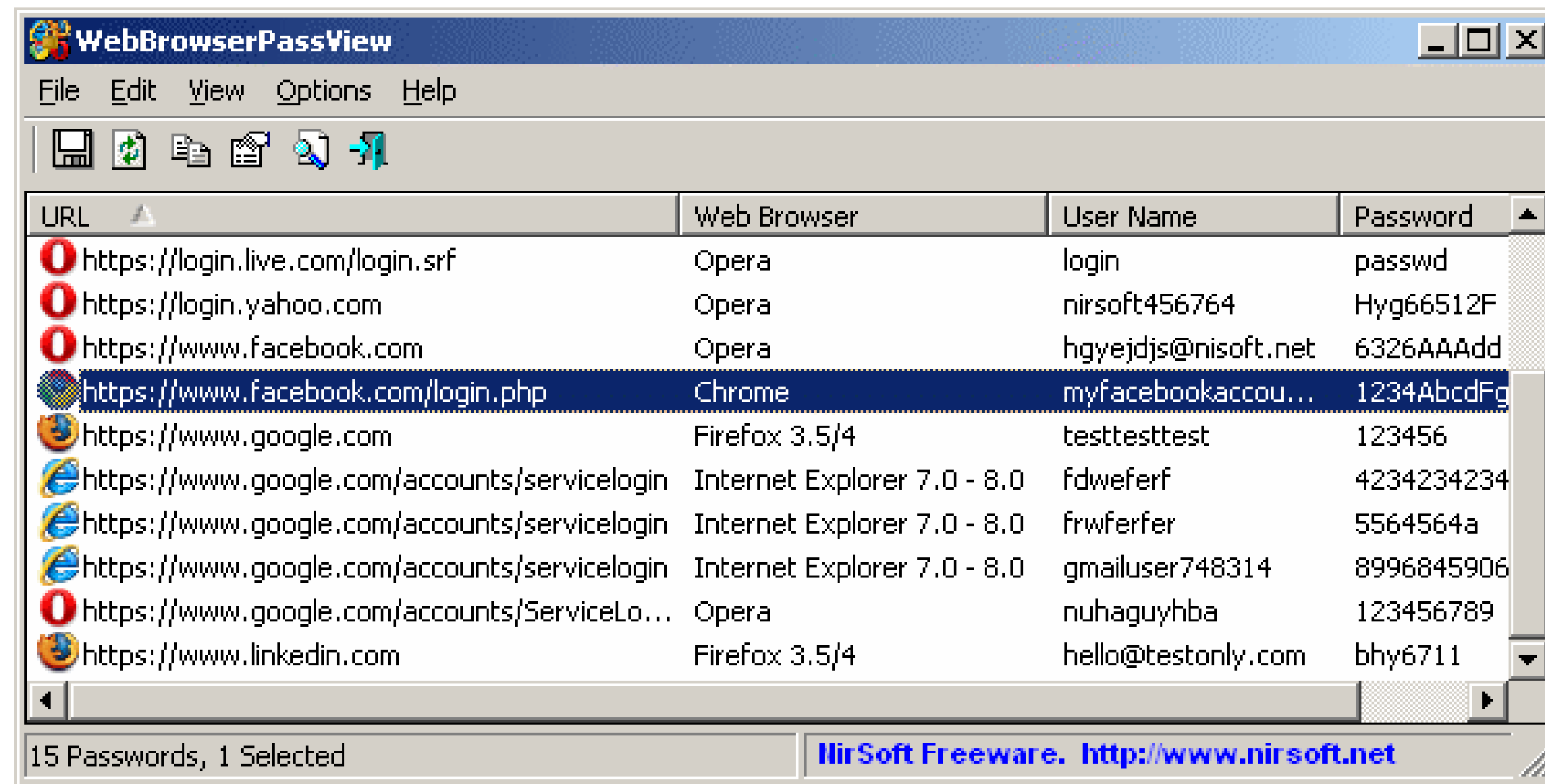
<https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/>



# Passwords



- Do you save passwords in the web browser?



## Demo - Login manager autofill abuse

This demo checks whether your browser's built-in login manager will automatically fill an invisible login form.

We found tracking companies using the login managers built-in to browsers to sniff email addresses without any visual indication to the user. Check out our [blog post](#) for more information.

To start, we'll need you to save some test credentials using the form below. On a later page, we'll demonstrate how a third-party script can retrieve these saved credentials. Note that the third party does not need to be present when the credentials are saved, and that none are present on this page.

### Demo steps

1. Submit the following form with **fake credentials**
2. Your browser will ask whether you want to save this login. Click "Save".

Fake Email address

Please do not enter a real email address.

Fake Password

Please do not enter a real password.

## Demo - Login manager autofill abuse

### Result

Sniffed email: **fake@fake.com**

Sniffed password: **fakepassword**

On Chrome you need to interact with the page (i.e., click anywhere) for the password to be sniffed.

An invisible form has been injected into this page by a script loaded from a third-party domain (also controlled by us). This causes the browser's built-in login manager to automatically fill the injected form with the credentials you saved on the [previous page](#). These credentials belong to the first-party domain (senglehardt.com). Once the form is filled, our third-party script retrieves the information and displays it above. Check out our [blog post](#) for more information.

[https://senglehardt.com/demo/no\\_boundaries/loginmanager/](https://senglehardt.com/demo/no_boundaries/loginmanager/)

[https://www.nirsoft.net/utils/web\\_browser\\_password.html](https://www.nirsoft.net/utils/web_browser_password.html)



# Uploading photos



www.pic2map.com/ezvtcb.html



## PHOTO EXIF DATA

The photo was shot using a SONY HDR-PJ820E camera at an aperture of f/4, 1/50 sec. shutter speed and ISO 0. 2.9-34 compulsory flash mode. The original image file has a resolution of 6592 x 3712 pixels, or in other words 24.5 megapixels. The megabytes.

According to the image metadata, the photo was shot on Monday 4th of July 2016. The local time was 20:51:26. No wrong if the date and time weren't set correctly in the digital camera.

**No GPS information was found...**

Camera: SONY HDR-PJ820E

Date: Mon 4th of July 2016

Exposure: 1/50

F Number: f/4

ISO: ISO 0

Lens: 2.9-34.8mm f/1.8-3.4

View More Info

Delete Photo

## CAMERA INFORMATION

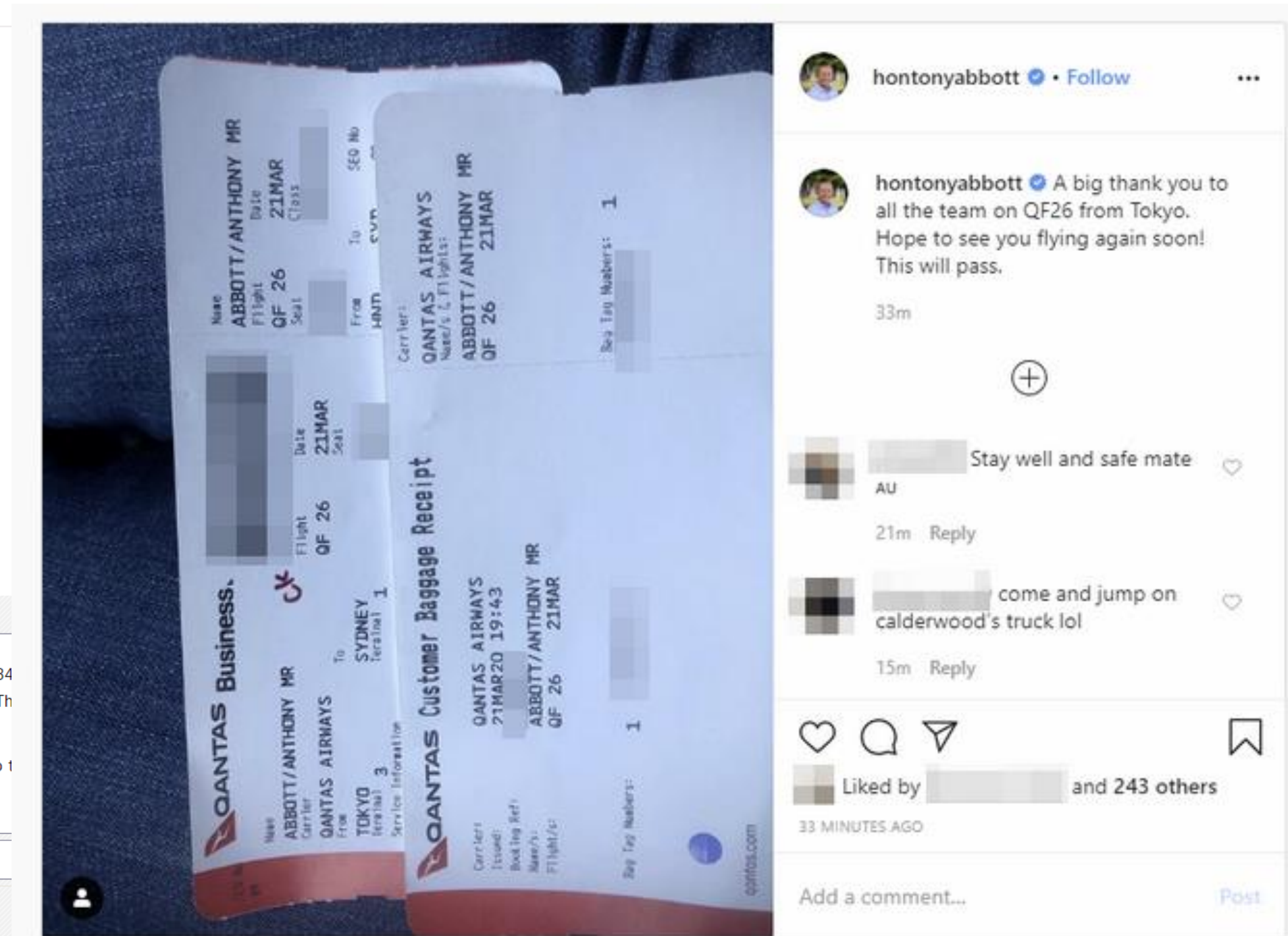
Brand: SONY	Model: HDR-PJ820E	Lens Info: 2.9-34.8mm f/1.8-3.4
Shutter: 1/50 (0.02 seconds)	F Number: f/4	ISO Speed: ISO 0
Flash: Not Used	Focal Length: 2.9 mm	Color Space: sRGB

## FILE INFORMATION

File Name: track1-routing-group[1].jpg	Image Size: 6592 x 3712 pixels	Resolution: 24.5 megapixels
Unique ID:	MIME Type: image/jpeg	Dots/Inch: 350 DPI

## DATE & TIME

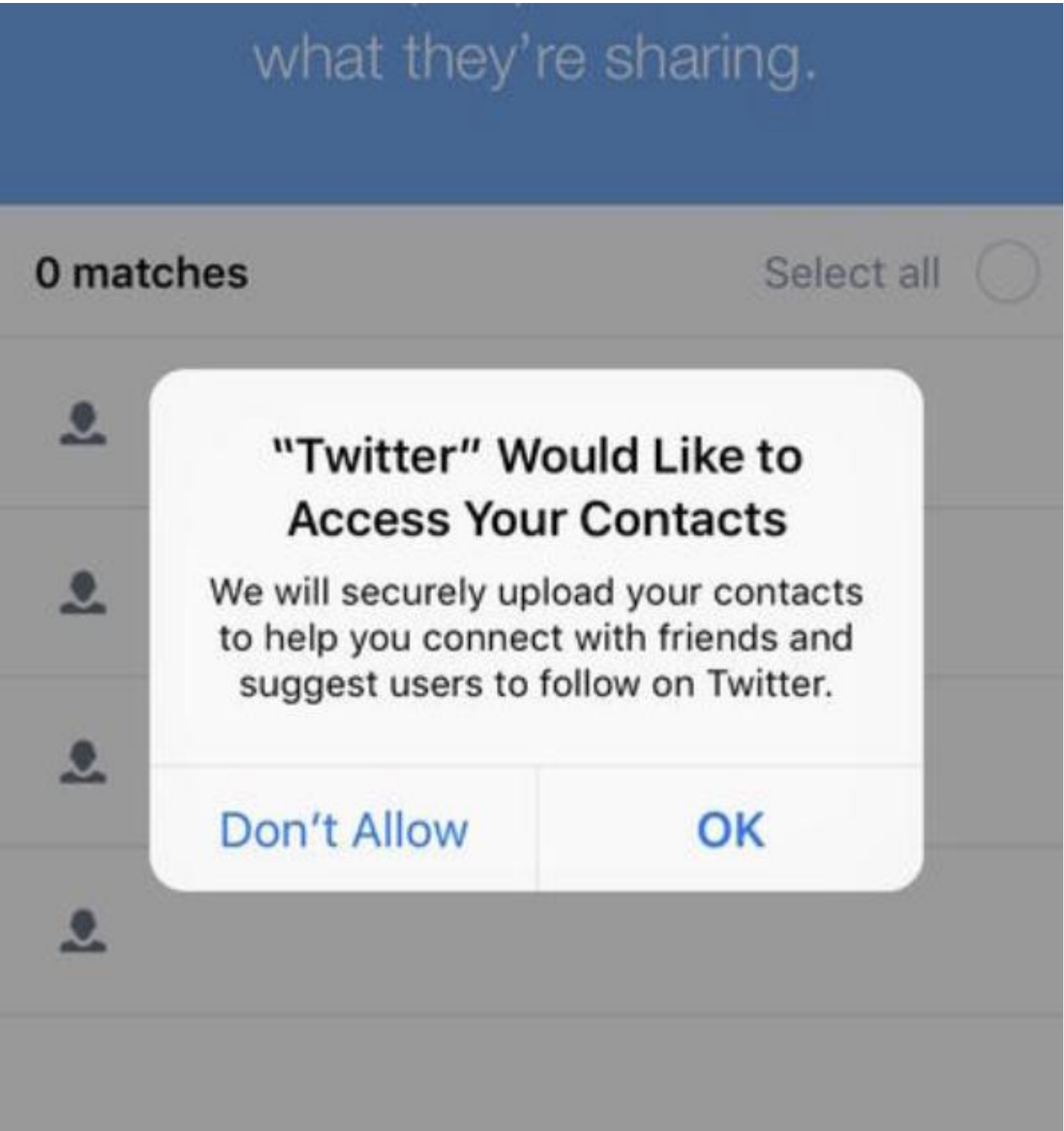
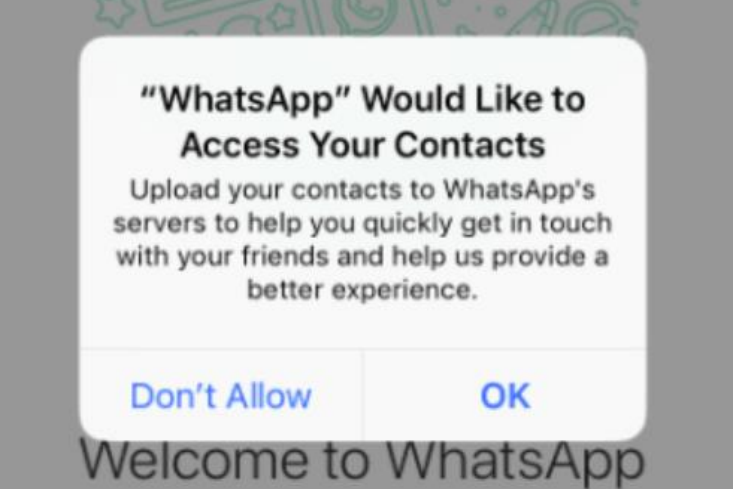
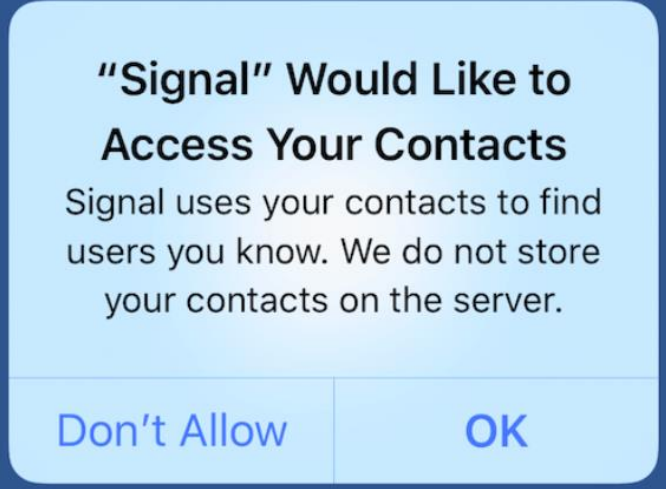
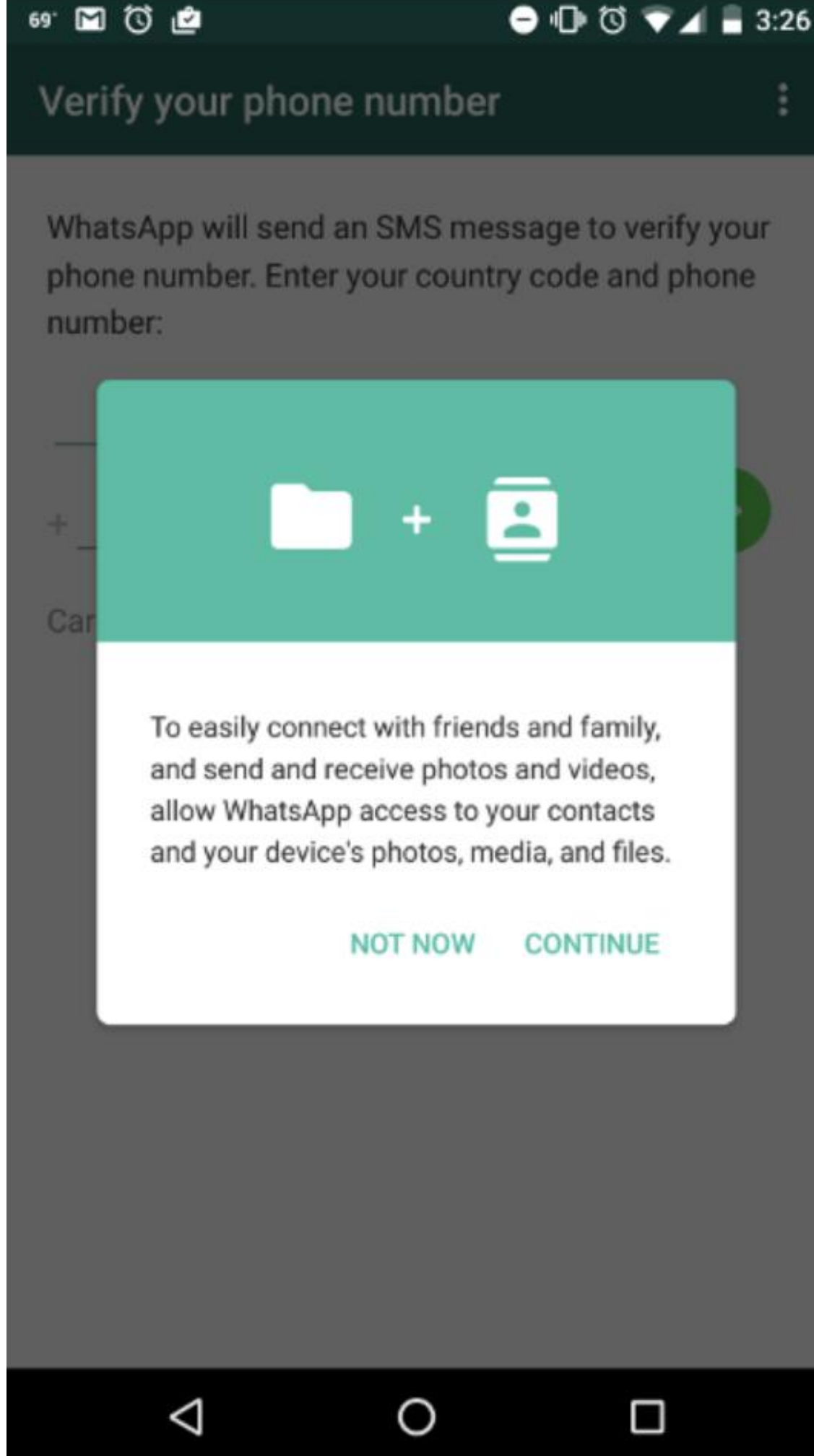
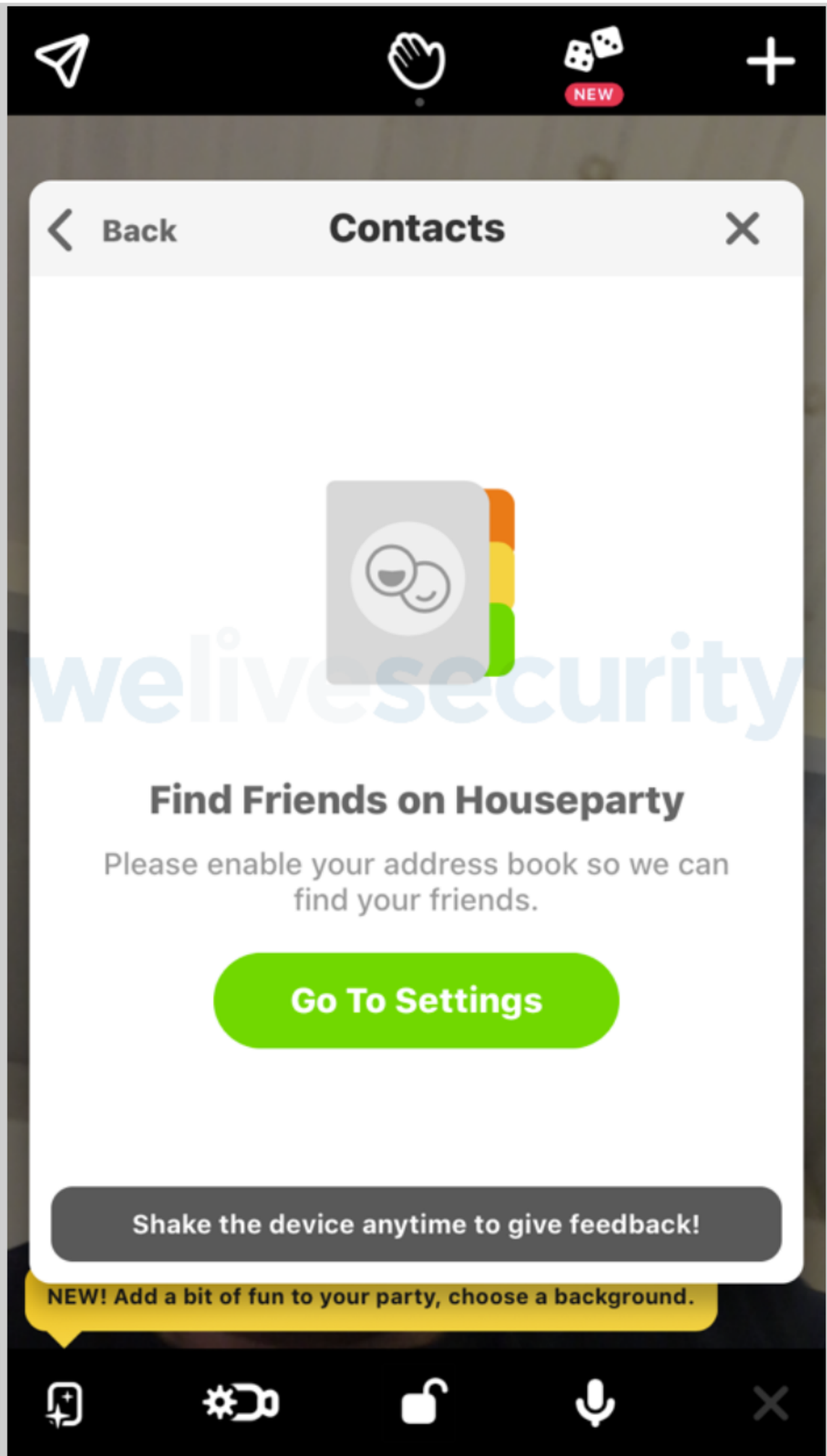
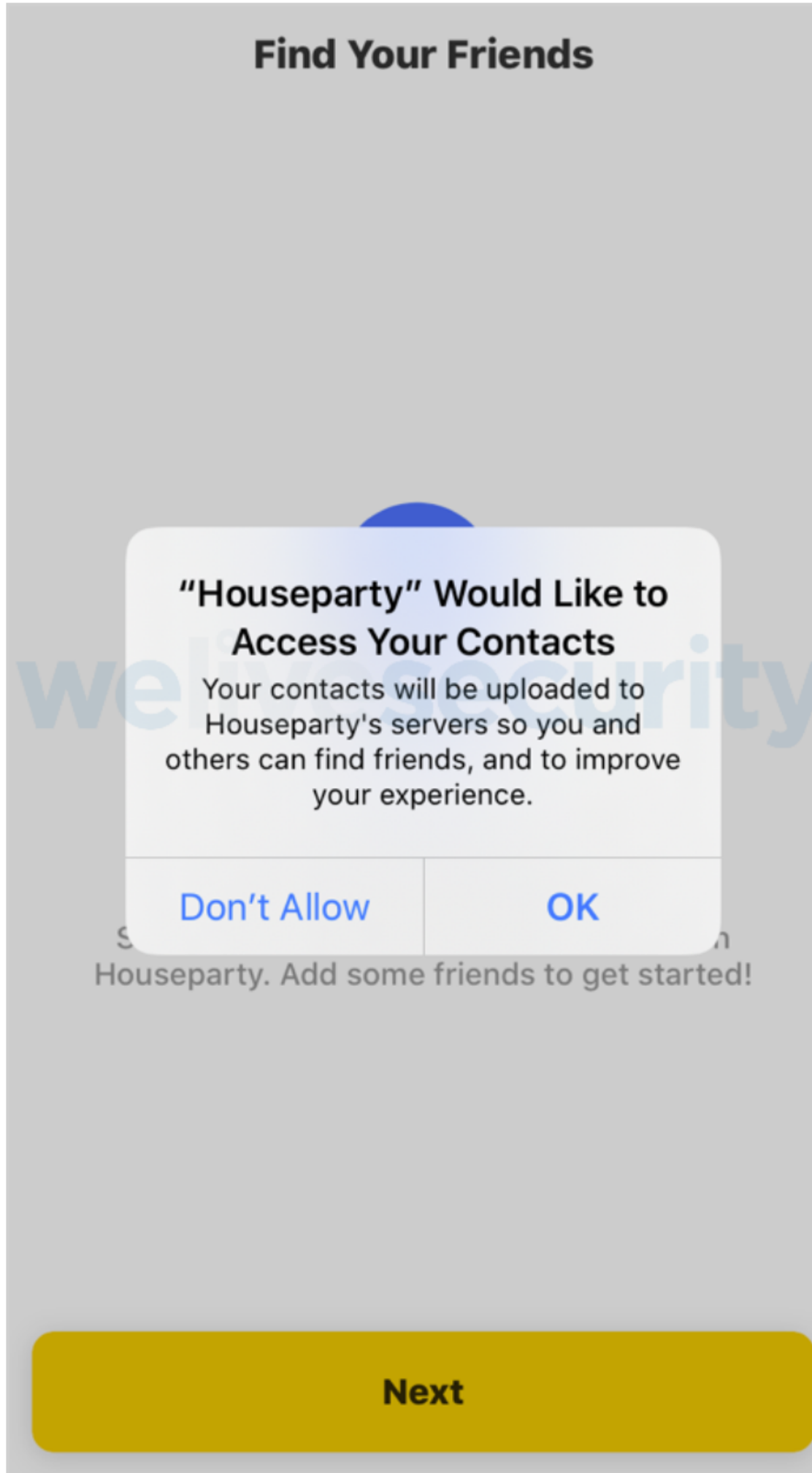
Date: 2016-07-04	Time: 20:51:26	Time Zone: Unknown
------------------	----------------	--------------------



<https://mango.pdf.zone/finding-former-australian-prime-minister-ony-abbotts-passport-number-on-instagram>



# Social media and other apps



<https://www.welivesecurity.com/2020/10/09/so-you-thought-your-personal-data-was-deleted-not-so-fast/>



# Social media and other apps



**Find Your Friends**

**"Houseparty" Would Like to Access Your Contacts**  
Your contacts will be uploaded to Houseparty's servers so you and others can find friends, and to improve your experience.

Don't Allow OK

Next

**Signal** Would Like to Access Your Contacts  
Signal uses your contacts to find users you know. We do not store your contacts on the server.

Don't Allow OK

**WhatsApp** Would Like to Access Your Contacts  
Upload your contacts to WhatsApp's servers to help you quickly get in touch with your friends and help us provide a better experience.

Don't Allow OK

Welcome to WhatsApp

what they're sharing.

0 matches Select all

**Twitter** Would Like to Access Your Contacts  
We will securely upload your contacts to help you connect with friends and suggest users to follow on Twitter.

Don't Allow OK

**CONSTITUTION OF THE REPUBLIC OF FIJI**

*Right to privacy*

24.—(1) Every person has the right to personal privacy, which includes the right to—

- (a) confidentiality of their personal information;
- (b) confidentiality of their communications; and
- (c) respect for their private and family life.

<https://www.welivesecurity.com/2020/10/09/so-you-thought-your-personal-data-was-deleted-not-so-fast/>



# Credentials and personal info



- Do you use the:
  - same email address to login for multiple sites?
  - same password?
  - same personal information?
  - auto-fill option in browsers?
  - Facebook or Google Single Sign-On
  - multi-factor or two-factor authentication
- If a site asks for personal information, do you think why?
- What other information is being gathered?

# Think before you click



- Everything online is tracked
- Everything online is logged
- Your personal information is worth something \$\$\$\$
- Your digital habits/behaviour impacts this worth
- Your friends and online contacts share your personal information



# Strategies

















- At a minimum:
  - Setup ad blocker
  - Enable do not track
  - Use some sort of end point protection
  - Use privacy mode for sensitive pages eg banking sites
  - Use email aliases (eg Gmail pacnog+apnictalk@gmail.com)
- Which device?
- Which browser?
- What plugins?
- What search engine?
- Uninstall unused apps, plugins or software

# Strategies



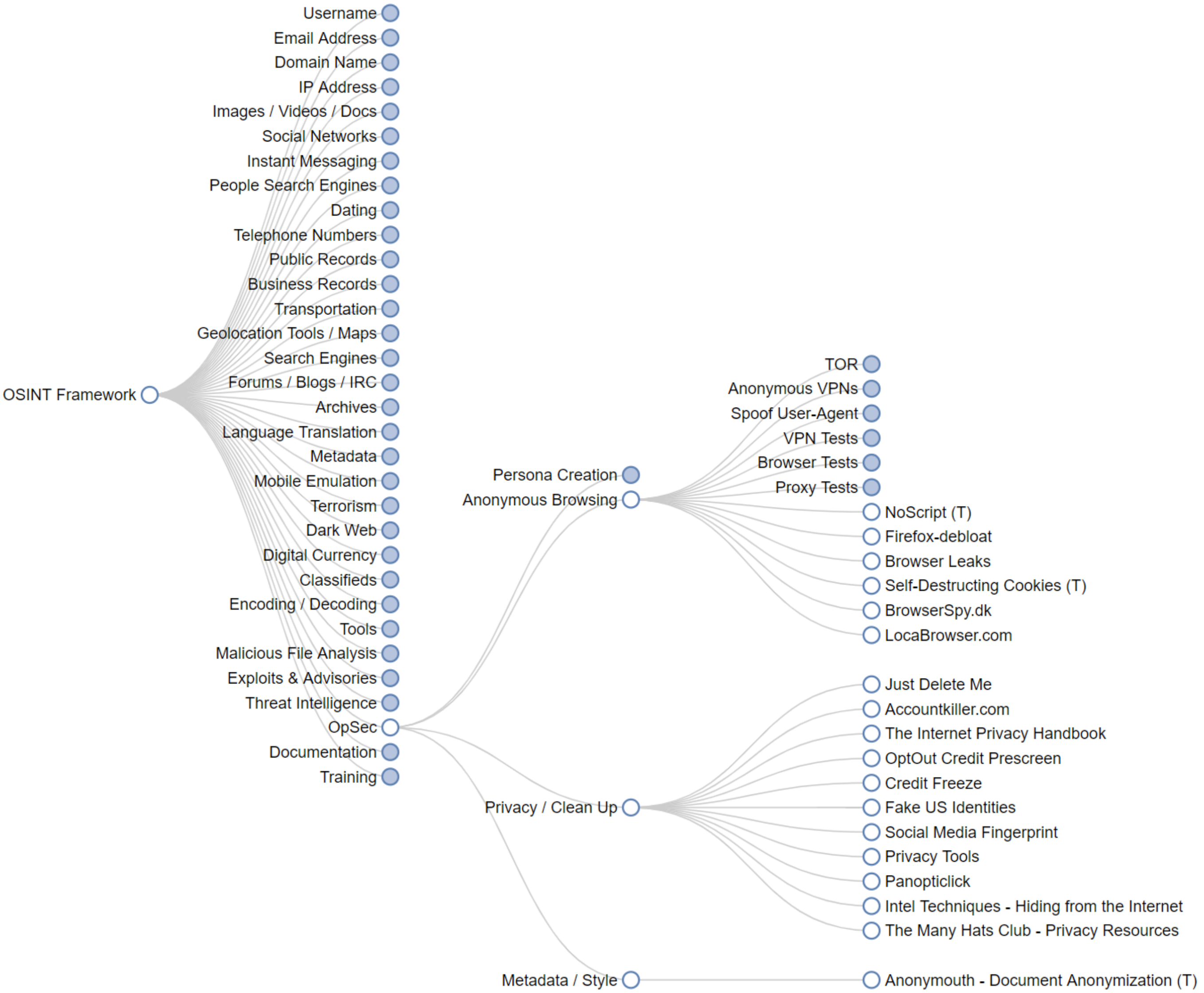
## Browser extensions

Extension	Description	Website		
 uBlock Origin	An efficient ad and tracker blocker with a small performance footprint!	<a href="#">Website</a>	<a href="#">Firefox</a>	<a href="#">Chrome</a>
 Ghostery	Protect your privacy by blocking trackers on the Web and by learning who is watching you!	<a href="#">Website</a>	<a href="#">Firefox</a>	<a href="#">Chrome</a>
 HTTPS Everywhere	Encrypt the web! Enable HTTPS automatically on websites that are known to support it. A project by the EFF (Electronic Frontier Foundation). This extension includes an option to verify SSL certificates directly by <a href="#">the EFF SSL Observatory</a> .	<a href="#">Website</a>	<a href="#">Firefox</a>	<a href="#">Chrome</a>
 Lightbeam	Visualize in details the servers you are contacting when you are surfing on the Internet! Developed by Mozilla. <a href="#">Presentation of Lightbeam</a> by Gary Kovacs, former CEO of Mozilla, in a TED talk.	<a href="#">Website</a>	<a href="#">Firefox</a>	
 Adblock Plus	Block advertisements, trackers and more! We recommend the use of additional lists like the <a href="#">Fanboy Complete Adblock list</a> .	<a href="#">Website</a>	<a href="#">Firefox</a>	<a href="#">Chrome</a>
 Disconnect	Stop tracking by third-party sites and visualize who is tracking you!	<a href="#">Website</a>	<a href="#">Firefox</a>	<a href="#">Chrome</a>
 Privacy Badger	Block spying ads and invisible trackers! A project by the EFF (Electronic Frontier Foundation).	<a href="#">Website</a>	<a href="#">Firefox</a>	<a href="#">Chrome</a>
 NoScript	Take control of what is running in your browser by blocking unwanted scripts!	<a href="#">Website</a>	<a href="#">Firefox</a>	
 Self-Destructing Cookies	Remove cookies that are no longer used as soon as you close a tab!		<a href="#">Firefox</a>	

<https://amiunique.org/tools/>



# Strategies



<https://osintframework.com>

# Thank You!

