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

MALWARE TYPE TRENDS
% of affected organizations

Banking Trojans 0.6%
Botnet 1.8%
Cryptominer 0.2%
Mobile 0.1%
Ransomware 0.3%

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

https://threatmap.checkpoint.com
Attack Trends

https://www.imperva.com/cyber-threat-attack-map/
# Internet usage

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>American Samoa</td>
<td>55,727</td>
<td>n/a</td>
<td>n/a</td>
<td>43.1%</td>
<td>0.1%</td>
<td>22,000</td>
</tr>
<tr>
<td>Antarctica</td>
<td>2,700</td>
<td>n/a</td>
<td>n/a</td>
<td>196.0%</td>
<td>0.0%</td>
<td>1,800</td>
</tr>
<tr>
<td>Australia</td>
<td>25,086,638</td>
<td>6,800,000</td>
<td>21,711,706</td>
<td>86.5%</td>
<td>75.8%</td>
<td>15,000,000</td>
</tr>
<tr>
<td>Australia, Ext. Terr.</td>
<td>1,651</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Christmas Island</td>
<td>2,205</td>
<td>404</td>
<td>1,000</td>
<td>45.4%</td>
<td>0.0%</td>
<td>400</td>
</tr>
<tr>
<td>Cocos (Keeling) Is.</td>
<td>598</td>
<td>n/a</td>
<td>80</td>
<td>13.4%</td>
<td>0.0%</td>
<td>70</td>
</tr>
<tr>
<td>Cook Islands</td>
<td>17,402</td>
<td>n/a</td>
<td>11,377</td>
<td>65.2%</td>
<td>0.0%</td>
<td>8,000</td>
</tr>
<tr>
<td>Fiji</td>
<td>918,757</td>
<td>7,500</td>
<td>500,958</td>
<td>54.5%</td>
<td>1.7%</td>
<td>470,000</td>
</tr>
<tr>
<td>French Polynesia</td>
<td>286,509</td>
<td>8,000</td>
<td>209,744</td>
<td>72.7%</td>
<td>0.7%</td>
<td>150,000</td>
</tr>
<tr>
<td>Guam</td>
<td>167,245</td>
<td>5,000</td>
<td>134,449</td>
<td>86.5%</td>
<td>0.5%</td>
<td>110,000</td>
</tr>
<tr>
<td>Kiribati</td>
<td>120,420</td>
<td>1,000</td>
<td>32,547</td>
<td>27.4%</td>
<td>0.1%</td>
<td>30,000</td>
</tr>
<tr>
<td>Marshall Islands</td>
<td>53,211</td>
<td>500</td>
<td>20,593</td>
<td>38.7%</td>
<td>0.1%</td>
<td>20,000</td>
</tr>
<tr>
<td>Micronesia</td>
<td>106,983</td>
<td>2,000</td>
<td>56,193</td>
<td>52.5%</td>
<td>0.2%</td>
<td>21,000</td>
</tr>
<tr>
<td>Nauru</td>
<td>11,269</td>
<td>n/a</td>
<td>6,418</td>
<td>57.0%</td>
<td>0.0%</td>
<td>3,400</td>
</tr>
<tr>
<td>New Caledonia</td>
<td>283,376</td>
<td>24,000</td>
<td>232,368</td>
<td>82.0%</td>
<td>0.8%</td>
<td>150,000</td>
</tr>
<tr>
<td>New Zealand</td>
<td>4,792,409</td>
<td>830,000</td>
<td>4,351,987</td>
<td>96.8%</td>
<td>15.2%</td>
<td>3,100,000</td>
</tr>
<tr>
<td>Niue</td>
<td>1,618</td>
<td>450</td>
<td>1,485</td>
<td>91.2%</td>
<td>0.0%</td>
<td>820</td>
</tr>
<tr>
<td>Norfolk Island</td>
<td>1,748</td>
<td>n/a</td>
<td>796</td>
<td>45.6%</td>
<td>0.0%</td>
<td>80</td>
</tr>
<tr>
<td>Northern Marianas</td>
<td>55,246</td>
<td>n/a</td>
<td>40,000</td>
<td>72.4%</td>
<td>0.1%</td>
<td>36,000</td>
</tr>
<tr>
<td>Palau</td>
<td>22,209</td>
<td>n/a</td>
<td>7,860</td>
<td>35.4%</td>
<td>0.0%</td>
<td>5,800</td>
</tr>
<tr>
<td>Papua New Guinea</td>
<td>8,586,525</td>
<td>135,000</td>
<td>962,650</td>
<td>11.2%</td>
<td>3.4%</td>
<td>670,000</td>
</tr>
<tr>
<td>Pitcairn Islands</td>
<td>59</td>
<td>n/a</td>
<td>170</td>
<td>n/a</td>
<td>n/a</td>
<td>150</td>
</tr>
<tr>
<td>Samoa</td>
<td>196,909</td>
<td>500</td>
<td>190,000</td>
<td>50.3%</td>
<td>0.3%</td>
<td>94,000</td>
</tr>
<tr>
<td>Smaller Territories</td>
<td>3,902</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Solomon Islands</td>
<td>635,254</td>
<td>2,000</td>
<td>75,722</td>
<td>11.9%</td>
<td>0.3%</td>
<td>68,000</td>
</tr>
<tr>
<td>Terre Australes</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Tokelau</td>
<td>1,340</td>
<td>60</td>
<td>800</td>
<td>59.7%</td>
<td>0.0%</td>
<td>410</td>
</tr>
<tr>
<td>Tonga</td>
<td>110,041</td>
<td>1,000</td>
<td>57,822</td>
<td>52.5%</td>
<td>0.2%</td>
<td>54,000</td>
</tr>
<tr>
<td>Tuvalu</td>
<td>11,393</td>
<td>n/a</td>
<td>5,619</td>
<td>48.3%</td>
<td>0.0%</td>
<td>1,700</td>
</tr>
<tr>
<td>Vanuatu</td>
<td>288,017</td>
<td>3,000</td>
<td>82,764</td>
<td>28.7%</td>
<td>0.3%</td>
<td>63,000</td>
</tr>
<tr>
<td>Wallis &amp; Futuna</td>
<td>11,617</td>
<td>n/a</td>
<td>3,900</td>
<td>33.6%</td>
<td>0.0%</td>
<td>3,400</td>
</tr>
<tr>
<td><strong>TOTAL OCEANIA</strong></td>
<td><strong>41,836,201</strong></td>
<td><strong>7,520,480</strong></td>
<td><strong>26,836,278</strong></td>
<td><strong>88.4%</strong></td>
<td><strong>100.0%</strong></td>
<td><strong>20,668,690</strong></td>
</tr>
</tbody>
</table>

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?

https://www.researchgate.net/publication/316449708_A_survey_on_internet_usage_and_cybersecurity_awareness_in_students

<table>
<thead>
<tr>
<th>Age</th>
<th>Male</th>
<th>Female</th>
<th>NA</th>
<th>Total</th>
<th>Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>08-12</td>
<td>256</td>
<td>145</td>
<td>43</td>
<td>444</td>
<td>20.91</td>
</tr>
<tr>
<td>13-17</td>
<td>325</td>
<td>346</td>
<td>89</td>
<td>760</td>
<td>35.80</td>
</tr>
<tr>
<td>18-21</td>
<td>421</td>
<td>285</td>
<td>213</td>
<td>919</td>
<td>43.29</td>
</tr>
</tbody>
</table>

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?

Which Device

• What devices do you use?

- Internet connected games console: 25.1% (2014-15), 26.7% (2016-17)
- Internet connected music/video player: 18.6% (2014-15), 26.1% (2016-17)
- Internet connected TV: 26.8% (2014-15), 42.1% (2016-17)
- Tablet: 61.9% (2014-15), 66.4% (2016-17)
- Mobile or smart phone: 86.8% (2014-15), 91.0% (2016-17)
- Desktop or laptop computer: 93.6% (2014-15), 91.4% (2016-17)

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

Extortion
Once hacked, cyber criminals can take over your:

- 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

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

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.

This poster was developed from security awareness expert Brian Krebs. Learn more about cyber criminals at: krebsonsecurity.com.
Phishing kits

https://isc.sans.edu/forums/diary/Phishing+kits+as+far+as+the+eye+can+see/26660/
How much is your data worth?

https://privacyaustralia.net/dark-web-personal-data/
What data are you leaking?

- Operating system
- Browser details
- Hardware details
- Location information
- Passwords
- Auto-fill information
What data are you leaking?

• Every time your 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.
Are you being tracked?

- Browser fingerprinting
- Tracking ads
- Do not track option

https://panopticlick.eff.org

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

Is your browser:

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

https://coveryourtracks.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/

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.

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

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
Enter a fake email
Please do not enter a real email address.

Fake Password
Enter a fake password
Please do not enter a real password.

https://senglehadt.com/demo/no_boundaries/loginmanager/
https://www.nirsoft.net/utils/web_browser_password.html
Uploading photos

www.pic2map.com/ezvtcb.html

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

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 (e.g., banking sites)
  - Use email aliases (e.g., Gmail pacnog+apnictalk@gmail.com)

- Which device?
- Which browser?
- What plugins?
- What search engine?
- Uninstall unused apps, plugins or software
## Strategies

### Browser extensions

<table>
<thead>
<tr>
<th>Extension</th>
<th>Description</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>uBlock Origin</td>
<td>An efficient ad and tracker blocker with a small performance footprint!</td>
<td></td>
</tr>
<tr>
<td>Ghostery</td>
<td>Protect your privacy by blocking trackers on the Web and by learning who is watching you!</td>
<td></td>
</tr>
<tr>
<td>HTTPS Everywhere</td>
<td>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 the EFF SSL Observatory.</td>
<td></td>
</tr>
<tr>
<td>Lightbeam</td>
<td>Visualize in detail the servers you are contacting when you are surfing on the Internet! Developed by Mozilla. Presentation of Lightbeam by Gary Kovacs, former CEO of Mozilla, in a TED talk.</td>
<td></td>
</tr>
<tr>
<td>AdBlock Plus</td>
<td>Block advertisements, trackers and more! We recommend the use of additional lists like the Fanboy Complete AdBlock list.</td>
<td></td>
</tr>
<tr>
<td>Disconnect</td>
<td>Stop tracking by third-party sites and visualize who is tracking you!</td>
<td></td>
</tr>
<tr>
<td>Privacy Badger</td>
<td>Block spying ads and invisible trackers! A project by the EFF (Electronic Frontier Foundation).</td>
<td></td>
</tr>
<tr>
<td>NoScript</td>
<td>Take control of what is running in your browser by blocking unwanted scripts!</td>
<td></td>
</tr>
<tr>
<td>Self-Destructing Cookies</td>
<td>Remove cookies that are no longer used as soon as you close a tab!</td>
<td></td>
</tr>
</tbody>
</table>

[https://amiunique.org/tools/](https://amiunique.org/tools/)
Thank You! (gif)