

Cybersecurity Management

1.2. Information Gathering

2022-2023

Prof. Raül Roca

raul.roca-canovas@upc.edu

[linkedin.com/in/roca-cybersecurity](https://www.linkedin.com/in/roca-cybersecurity)

Contents

- Network Information Gathering
- People Information Gathering
- People Hacking
- Extra Resources

Network Information Gathering

Widening the scope and reducing the unknown

WHOIS and Reverse WHOIS

- [WHOIS](#) query by domain
- WHOIS query by IP
- [Reverse WHOIS](#) query by registrant
- Reverse WHOIS query by company
- Reverse WHOIS query by registrant's email

RIR (Regional Internet Registry)	Organisation
Europe, Russia, Asia (Central, West)	RIPE
USA, Canada	ARIN
Oceania, Asia (South and East)	APNIC
Latin America	LACNIC
Africa	AFRINIC

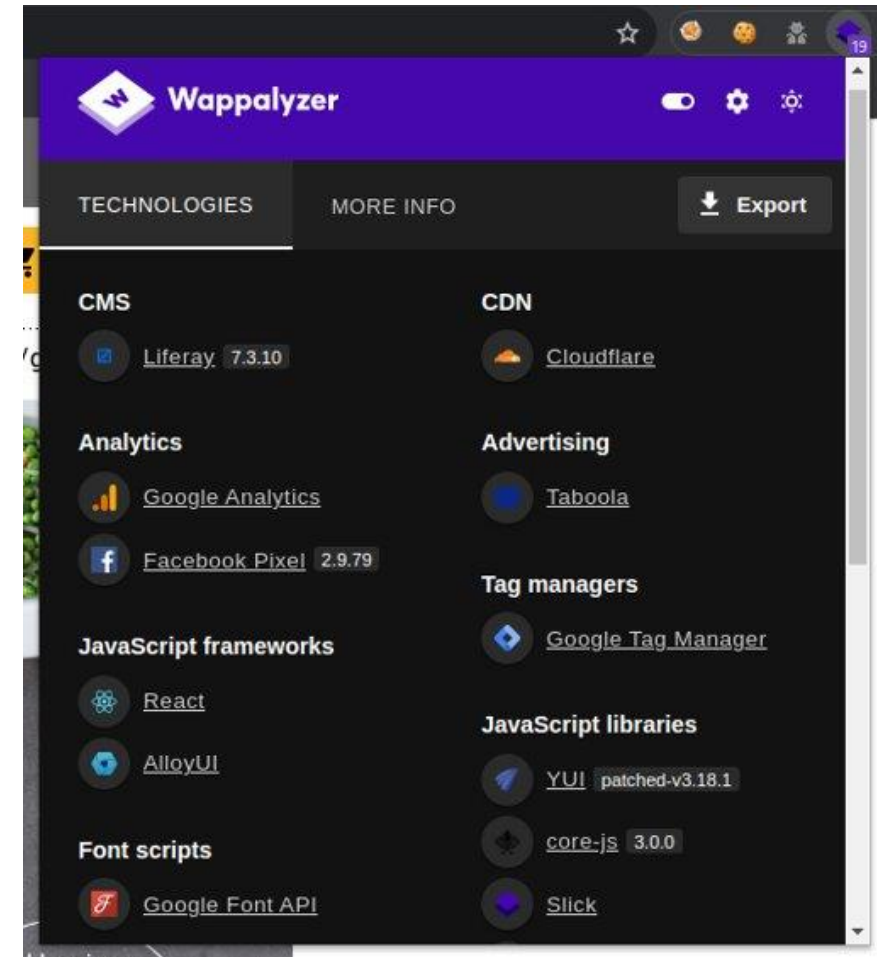
```
Registry Registrant ID:  
Registrant Name: REDACTED FOR PRIVACY  
Registrant Organization: Mercadona, S.A.  
Registrant Street: REDACTED FOR PRIVACY  
Registrant City: REDACTED FOR PRIVACY  
Registrant State/Province: VALENCIA  
Registrant Postal Code: REDACTED FOR PRIVACY  
Registrant Country: ES  
Registrant Phone: REDACTED.FORPRIVACY  
Registrant Phone Ext:  
Registrant Fax: REDACTED.FORPRIVACY  
Registrant Fax Ext:  
Registrant Email: https://domaincontact.nominalia.com/contact-domain  
Registry Admin ID:  
Admin Name: REDACTED FOR PRIVACY  
Admin Organization: REDACTED FOR PRIVACY  
Admin Street: REDACTED FOR PRIVACY  
Admin City: REDACTED FOR PRIVACY  
Admin State/Province: REDACTED FOR PRIVACY  
Admin Postal Code: REDACTED FOR PRIVACY  
Admin Country: REDACTED FOR PRIVACY  
Admin Phone: REDACTED.FORPRIVACY  
Admin Phone Ext:  
Admin Fax: REDACTED.FORPRIVACY  
Admin Fax Ext:  
Admin Email: https://domaincontact.nominalia.com/contact-domain  
Registry Tech ID:  
Tech Name: REDACTED FOR PRIVACY  
Tech Organization: REDACTED FOR PRIVACY  
Tech Street: REDACTED FOR PRIVACY  
Tech City: REDACTED FOR PRIVACY  
Tech State/Province: REDACTED FOR PRIVACY  
Tech Postal Code: REDACTED FOR PRIVACY  
Tech Country: REDACTED FOR PRIVACY  
Tech Phone: REDACTED.FORPRIVACY  
Tech Phone Ext:  
Tech Fax: REDACTED.FORPRIVACY  
Tech Fax Ext:  
Tech Email: https://domaincontact.nominalia.com/contact-domain  
Name Server: ARTEMIS.TTD.NET  
Name Server: MINERVA.TTD.NET
```

Domains and Subdomains

- Passive
 - Manual: [Google dorks](#), pages (like crt.sh).
 - Automated: amass, dnsenum, dnsrecon, sublist3r, etc.
- Active
 - Zone transfer (it should be vulnerable)
 - [DNS Zone Walk](#) (it should be vulnerable)
 - Crawling, some good tools: ZAPProxy, BurpSuite, [FortiPenTest](#)
 - Brute force, some tools: ffuf, [gobuster](#), wfuzz
 - Brute force with subdomain
 - Brute force with HTTP Host header

Technologies in Use

- Useful to search for vulnerabilities
- Tools
 - Extensions: [Wappalyzer](#)
 - CLI: WhatWeb



Resources – Special Files

- sitemap.xml →
- robots.txt
- [humans.txt](#)
- security.txt
- .well-known/

```
(gz@kali)-[~/info-gathering]
$ curl -sS https://www.bugcrowd.com/robots.txt
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
(gz@kali)-[~/info-gathering]
$
```

```
(gz@kali)-[~/info-gathering]
$ curl -sS https://www.google.com/sitemap.xml | grep '<loc>'
<loc>https://www.google.com/gmail/sitemap.xml</loc>
<loc>https://www.google.com/forms/sitemaps.xml</loc>
<loc>https://www.google.com/slides/sitemaps.xml</loc>
<loc>https://www.google.com/sheets/sitemaps.xml</loc>
<loc>https://www.google.com/drive/sitemap.xml</loc>
<loc>https://www.google.com/docs/sitemaps.xml</loc>
<loc>https://www.google.com/get/sitemap.xml</loc>
<loc>https://www.google.com/flights/sitemap.xml</loc>
<loc>https://www.google.com/admob/sitemap.xml</loc>
<loc>https://www.google.com/business/sitemap.xml</loc>
<loc>https://www.google.com/services/sitemap.xml</loc>
<loc>https://www.google.com/partners/about/sitemap.xml</loc>
<loc>https://www.google.com/adwords/sitemap.xml</loc>
<loc>https://www.google.com/search/about/sitemap.xml</loc>
<loc>https://www.google.com/adsense/start/sitemap.xml</loc>
<loc>https://www.google.com/retail/sitemap.xml</loc>
<loc>https://www.google.com/sitemap_search.xml</loc>
<loc>https://www.google.com/webmasters/sitemap.xml</loc>
<loc>https://www.google.com/chromebook/sitemap.xml</loc>
<loc>https://www.google.com/chrome/sitemap.xml</loc>
<loc>https://www.google.com/calendar/about/sitemap.xml</loc>
<loc>https://www.google.com/photos/sitemap.xml</loc>
<loc>https://www.google.com/nonprofits/sitemap.xml</loc>
<loc>https://www.google.com/finance/sitemap.xml</loc>
(gz@kali)-[~/info-gathering]
$
```

Resources – "Hidden" Resources

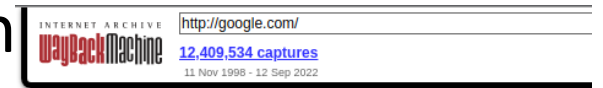
- No link pointing to them
- They are found by brute force
 - The response differ in some properties
 - Status code
 - Size
 - Words
 - Lines
 - Characters
 - Response time
- Tools: ffuf, gobuster, feroxbuster, wfuzz, etc.

Resources – Open Source Projects

- Open Source hosting platforms
 - GitHub
 - GitLab
 - BitBucket
- There might be sensitive information
 - Credentials
 - Emails
 - API keys
- Do not forget other branches and previous commits
- GitHub Dorks ([list](#), [keywords](#), [tools](#))

Resources – Archive

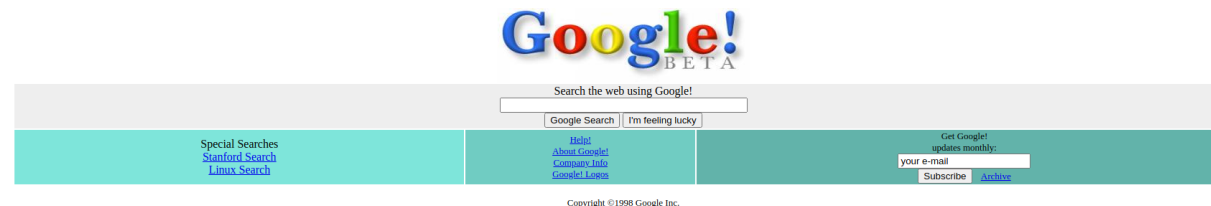
- Previous versions may contain sensitive information
- Internet Archives: [WaybackMachine](https://web.archive.org/web/20220912111111/http://google.com/)
- Cached websites (Google dork)
- Automated tools: waybackurls



Welcome to Google

[Google Search Engine Prototype](#)
[Might-work-some-of-the-time-prototype that is much more up to date.](#)

11/11/1998: Google in alpha version



02/12/1998: Google in beta version

More than just Web

- IoT Search Engines: [Shodan](#), Censys, ZoomEye
- CLI option: shodan (API key needed)

The screenshot shows the Shodan search engine interface. At the top, there's a navigation bar with 'SHODAN', 'Explore', 'Pricing', and a search bar containing 'tesla.com'. Below the navigation bar, the search results are displayed. On the left, there's a sidebar with 'TOTAL RESULTS' (6), 'TOP COUNTRIES' (United States: 3, France: 2, Philippines: 1), 'TOP PORTS' (443: 4, 80: 1, 8081: 1), and 'TOP ORGANIZATIONS' (Microsoft Corporation: 2, OVH SAS: 2). The main content area shows three search results. The first result is for IP 188.165.41.239, located in France, Roubaix, with a date of Fri, 09 Sep 2022 00:45:25 GMT. The second result is for IP 202.124.131.5, located in Philippines, Manila, with a date of Thu, 08 Sep 2022 10:05:04 GMT. The third result is for IP 188.165.41.239, located in France, Roubaix, with a date of Thu, 08 Sep 2022 03:46:05 GMT. Each result includes a 'View Report' and 'View on Map' link. There's also a 'New Service' banner for 'Shodan Monitor'.

The screenshot shows the Shodan search engine interface for the IP address 3.8.8.8. At the top, there's a navigation bar with '3.8.8.8', 'Regular View', 'Raw Data', and 'History'. Below the navigation bar, the search results are displayed. On the left, there's a sidebar with 'General Information' (Hostnames: dns.google, Domains: DNS.GOOGLE, Country: United States, City: Mountain View, Organization: Google LLC, ISP: Google LLC, ASN: AS15169). On the right, there's a sidebar with 'Open Ports' (53, 443). The main content area shows detailed information for the IP address 3.8.8.8, including a date of Thu, 08 Sep 2022 03:46:05 GMT, a server of Apache, a location of https://tesla.com/, and a content-type of text/html; charset=UTF-8. There's also a 'SSL Certificate' section showing the certificate details for the IP address.

More than just Web

- Shodan Dorks (API key needed)

SHODAN os:"windows xp"

TOTAL RESULTS
2,482

View Report Download Results Historical Trend
View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

TOP COUNTRIES

Korea, Re...	1,376
China	466
United States	68
Taiwan	64
Russian Fed...	60
More...	

TOP PORTS

1433	1,361
23	922
465	35
25	24
80	19

115.195.166.216 2022-09-12T17:26:08.48285

CHINANET-ZJ Hangzhou node network
OS: Windows XP SP2
OS Build: 5.1.2600
China, Hangzhou
database

220.74.113.94 2022-09-12T17:13:57.05840

Korea Telecom
OS: Windows XP SP2
OS Build: 5.1.2600
Korea, Republic of, Ansan-si
database

218.6.214.238 2022-09-12T17:08:52.13141

238.214.6.21
8.broad.my.s
c.dynamic.16
3data.com.cn
CHINANET
Sichuan province
network
China, Hangzhou

SHODAN os:"windows xp" country:"ES"

TOTAL RESULTS
57

View Report Download Results Historical Trend
View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

TOP CITIES

Madrid	10
Barcelona	6
Bilbao	4
Palma	4
Zaragoza	3
More...	

80.24.45.155 2022-09-12T14:46:42.727505

155.red-80-24-45.staticip.rima-tde.net
TELEFONICA DE ESPANA
Spain, Palma
database

MS-SQL NTLM Info:
OS: Windows XP SP2
OS Build: 5.1.2600

TOP PORTS

1433	37
60011	11
1077	2
3397	2
10433	2
More...	

80.32.214.102 2022-09-12T14:12:49.908927

102.red-80-32-214.staticip.rima-tde.net
TELEFONICA DE ESPANA
Spain, Girona
database

MS-SQL NTLM Info:
OS: Windows XP SP2
OS Build: 5.1.2600

TOP ORGANIZATIONS

TELEFONIC...	18
TELEFONIC...	12

70.red-2-136-0.staticip.rima-tde.net
TELEFONICA DE ESPANA

MS-SQL NTLM Info:
OS: Windows XP SP2
OS Build: 5.1.2600

More than just Web

- Port Scan
 - Passive
 - Shodan
 - Censys
 - [ZoomEye](#)
 - Active
 - Nmap
 - Masscan

```
(gz@kali)-[~/Documents/research/tools/shodan]
$ dig +noall +answer airbnb.com
airbnb.com.      5      IN      A       52.2.74.15
airbnb.com.      5      IN      A       52.23.57.177
airbnb.com.      5      IN      A       52.71.105.113
(gz@kali)-[~/Documents/research/tools/shodan]
$ shodan download airbnb "ip:52.2.74.15"
Search query:      ip:52.2.74.15
Total number of results: 2
Query credits left: 99
Output file:      airbnb.json.gz
[#####] 50% 00:00:03
Saved 2 results into file airbnb.json.gz
(gz@kali)-[~/Documents/research/tools/shodan]
$ gzip -d airbnb.json.gz
(gz@kali)-[~/Documents/research/tools/shodan]
$ jq -rs '.[].port,.product' airbnb.json | xargs -n2
443 nginx
80 nginx
(gz@kali)-[~/Documents/research/tools/shodan]
$ nmap -np- -Pn --min-rate 200 52.2.74.15 -oN tcpPorts
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 15:02 EDT
Nmap scan report for 52.2.74.15
Host is up (0.10s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 658.15 seconds
(gz@kali)-[~/Documents/research/tools/shodan]
$
```

People Information Gathering

When there is too much information on the Internet

OSINT (Open-Source Intelligence)

- Not every piece of information publicly available is public information
- Public information is more than just the Internet
- Greatest OSINT sources
 - Clear Net
 - Deep Web
 - Dark Net
- Best tool: Search engines

OSINT – Search Engines

- Search Engines: [Google](#), [Bing](#), [DuckDuckGo](#), [Yandex](#), [Baidu](#), [CarrotSearch](#), [Ask](#), etc.
 - Specialised Search Engines: [Wolfram](#), [IntelligenceX](#), [Shodan](#), [Censys](#), [ZoomEye](#), etc.
 - Advanced Search: [Dorks](#) (e.g.: [GHDB](#): *Google Hacking Database*).
- Video Search Engine: [Youtube](#) ([unlisted videos](#)), [Vimeo](#), etc.
- Reverse Image : [Yandex](#), [Bing](#), [Google](#), [TinEye](#), etc.
- Archives: [Wayback Machine](#), etc.
- Source code: [GitHub](#), [GitLab](#), [BitBucket](#), etc.

OSINT – Tools

- Social media accounts: namecheckup.com (also domains)
- Leaked passwords
 - [HIBP](https://h1bp.com) (it does not show the password)
 - Pwndb (it used to be available on the *dark net* **Tor**)
 - [IntelligenceX](https://intelligence.x) (paid service, may offer some free information)
 - [BreachCompilation](https://breachcompilation.com) (<https://pwdquery.xyz/>), etc.
- Automated tools: [theHarvester](https://theharvester.com), [Sherlock](https://sherlockproject.com), etc.
- Password generators
 - [CeWL](https://cewlproject.com) (wordlist out of a webpage)
 - [CUPP](https://cupp.sh) (wordlist out of a profile)

OSINT – Gathering Emails

1. What is the domain of the organisation/corporation?
 - <https://www.crunchbase.com/>, search engines.
2. What is the email format they use?
 - <https://hunter.io/>
3. Create emails with (ex-)employees from LinkedIn:
 - [CrossLinked](#)
4. Which of those emails are valid?
 - <https://www.verifyemailaddress.org/>
- Is there a better/supplementary way? [Phonebook.cz](#) (by IntelligenceX)

OSINT – Gathering Credentials

'--have i been pwned?

Check if your email or phone is in a data breach

thisisgood@gmail.com pwned?

Oh no — pwned!

Pwned in 7 data breaches and found no pastes (subscribe to search sensitive breaches)

PWDQUERY

Check if your passwords have been compromised from a data leak...

thisisgood@gmail.com pwd check

☐ I'm not a robot

passwords found (1)

bo*****1!

```
(gz@kali)-[/usr/share/wordlists]
$ echo 'bo*****1!' | tr '*' '.'
bo.....1!
(gz@kali)-[/usr/share/wordlists]
$ grep -Pn '^bo.....1!$' rockyou.txt
9499938:bowwow101!
9535845:bollocks1!
9540681:bogies101!
(gz@kali)-[/usr/share/wordlists]
$
```

Resources	Info
HIBP	Was it leaked?
PwdQuery	Password features
Wordlists	Possible passwords
COMB	Leaked passwords

```
/COMB/CompilationOfManyBreaches
└─ ./query.sh thisisgood@gmail.com
thisisgood@gmail.com:Mashasemenova
thisisgood@gmail.com:bordeaux1!
thisisgood@gmail.com:march32114
└─
```

Hashes

- Features
 - 1 bit change produces more than 50% of bits change
 - Fix length
 - Irreversible
 - Same input, same output
- Case uses
 - Data integrity
 - "Password" storage
- Concepts: collision, cracking, brute-force attack, dictionary attack, [rainbow tables](#), salt.

Algorithm	Bits	Strong
MD5	128	false
SHA-1	160	false
SHA-256	256	true
SHA-512	512	true

Password Policy

- Tendency to re-use username/password
- Strong password
 - Length: +10 characters
 - Characters: `/(?=[a-z])(?=[A-Z])(?=\d)(?=[^a-zA-Z0-9]).{10,}/`
 - Non-relatable information (personal data, hobbies, etc.)
 - It cannot be made out of words
 - It should not have been leaked
 - It must seem completely random
 - It should be easy to remember

How secure is my password?

Top passwords

If you'd like to change your password please fill out the form below and we will change your password on the system you indicate. | Full Name | System (Yard, email, ect.) | Current password | New password | |---------------------------|----------------------------|------------------|----------------| | Kyle Smith
ITC 1001017 | Email | Scater 44\$ | 5tker442 | | | PHONE | 89621 | 4261 | | Jack H. | Email | Password | Password 2 | | Big Ed | Facebook | redsteph | mimimim | | Sam Adams | Pike Pass | h | born lower 100 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | *Call when case 1* *Come See Me - Shawn*

Password Policy – A Little more

- Do not tell anyone your password
- Do not save it in clear text (your wallet, post-it, etc.)
- Change it regularly (especially if there has been data breaches)
- Different passwords for different services

How to achieve so?

- Password managers (online, offline).
- **MFA** (*Multi-Factor Authentication*), **2FA** (*Two-Factor Authentication*).

OSINT – Gathering Accounts

Note: Not every account belongs to our victim.

Try some possible variations.

Namecheckup.com

whatsmyname.app

Search for accounts using the search bar and filters.

Found: 74 Processed: 460 / 460

Buttons: Show All, Show Found, Show Not Found

Grid of account categories:

Audiogungle Category: music Account Found	Blogspot Category: blog Account Found	Disqus Category: social Account Found	Chess.com Category: gaming Account Found	Bandibab Category: music Account Found
codeforces Category: coding Account Found	depop Category: shopping Account Found	imgur Category: images Account Found	Jeuxvideo Category: gaming Account Found	JSFiddle Category: coding Account Found
kaggle Category: coding	itchess Category: gaming	cracked_to Category: social	3dtoday Category: hobby	ArtBreeder Category: art

Found Accounts Table:

SITE	CATEGORY	LINK
3dtoday	hobby	https://3dtoday.ru/blogs/thisisgood
Ameblo	blog	https://ameblo.jp/thisisgood
Aminapps	blog	https://aminapps.com/ru/thisisgood
Archive Of Our O...	hobby	https://archiveofourown.org/users/thisisgood
ArtBreeder	art	https://www.artbreeder.com/thisisgood
ask.fm	social	https://ask.fm/thisisgood
Audiogungle	music	https://audiogungle.net/user/thisisgood
Bandcamp	music	https://bandcamp.com/thisisgood

Click on domains after search for purchase options and whois info

Legend: Available (Green), Taken (Red), Invalid (Yellow)

.com	.net	.org	.co	.biz \$49.99	.io \$49.99	.at	.us	.me
.co.uk	.eu	.info	.xyz	.live	.pro	.am \$89.99	.tv \$39.99	.shop
.life	.ch	.today	.in	.club	.cc	.tech	.site	.online
.store	.space	.website	.vip	.host	.press	.digital	.guru	.de
.ltd	.tk	.nl	.ca	.tw \$29.99	.fun	.ws	.work	.tools

Hurry! Web Hosting with FREE domain. On sale! One-click install! [Get Now!](#)

Username

Facebook	Twitter	YouTube	TikTok	Pinterest	Medium	Twitch	Tumblr	Github
Deqis	me About.me	Yelp	Periscope	Patreon	Balancer	LiveJournal	BuzzFeed	Vk
Blogger	WordPress	Spotify	Gravatar	Bitbucket	99designs	IFTTT	SlideShare	DeviantArt
CNET	Shopify	ask.fm	Sourceforge	SoundCloud	Etsy	Shutterstock	OK.RU	Last.FM
Vimeo	Dribbble	MySpace	Slack	Quora	Wikipedia	Dailymotion	Goodreads	Indiegogo
TaskRabbit	Ovi.to	9gag	Houzz	GrubHub	Mastodon	ImageShack	Steam	Hacker Noon
WU WikiHow	Discord	Telegram	eBay	Product Hunt	DonationAlerts	Linktree	Photobucket	Roblox
IGN	Basecamp	Quora	Genius	StumbleUpon	Fandom			

OSINT - Gathering Accounts

Automated tools: [Sherlock](#)

```
(venv)-(gz@kali)-[~/Documents/research/tools/Sherlock]
$ python3 sherlock/sherlock/sherlock.py --timeout 1 thisisgood
[*] Checking username thisisgood on:

[+] 9GAG: https://www.9gag.com/u/thisisgood
[+] Academia.edu: https://independent.academia.edu/thisisgood
[+] AskFM: https://ask.fm/thisisgood
[+] Audiojungle: https://audiojungle.net/user/thisisgood
[+] Bandcamp: https://www.bandcamp.com/thisisgood
[+] Blogger: https://thisisgood.blogspot.com
[+] BuzzFeed: https://buzzfeed.com/thisisgood
[+] Chaturbate: https://chaturbate.com/thisisgood
[+] Chess: https://www.chess.com/member/thisisgood
[+] Clubhouse: https://www.clubhouse.com/@thisisgood
[+] Codecademy: https://www.codecademy.com/profiles/thisisgood
[+] DeviantART: https://thisisgood.deviantart.com
```

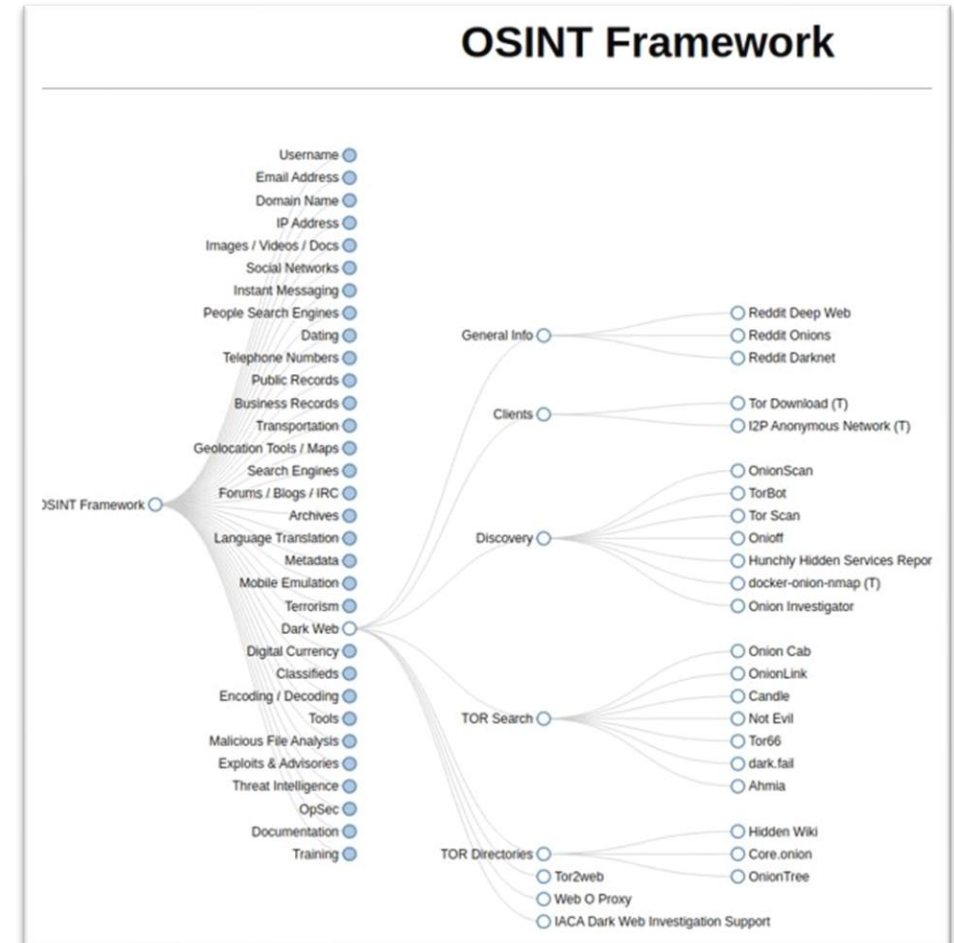
```
[+] Scribd: https://www.scribd.com/thisisgood
[+] Slack: https://thisisgood.slack.com
[+] SlideShare: https://slideshare.net/thisisgood
[+] Smule: https://www.smule.com/thisisgood
[+] SoundCloud: https://soundcloud.com/thisisgood
[+] Splice: https://splice.com/thisisgood
[+] Star Citizen: https://robertsspaceindustries.com/citizens/thisisgood
[+] SteamGroup: https://steamcommunity.com/groups/thisisgood
[+] TETR.IO: https://ch.tetr.io/u/thisisgood
[+] Telegram: https://t.me/thisisgood
[+] Tellonym.me: https://tellonym.me/thisisgood
[+] ThemeForest: https://themeforest.net/user/thisisgood
[+] Twitch: https://www.twitch.tv/thisisgood
[+] Typeracer: https://data.typeracer.com/pit/profile?user=thisisgood
[+] Ultimate-Guitar: https://ultimate-guitar.com/u/thisisgood
[+] VK: https://vk.com/thisisgood
[+] VSCO: https://vSCO.co/thisisgood
[+] Wattpad: https://www.wattpad.com/user/thisisgood
[+] Whonix Forum: https://forums.whonix.org/u/thisisgood
[+] Wikipedia: https://en.wikipedia.org/wiki/Special:CentralAuth/thisisgood?uselang=qqx
[+] WordPress: https://thisisgood.wordpress.com/
[+] Wykop: https://www.wykop.pl/ludzie/thisisgood
[+] Xvideos: https://xvideos.com/profiles/thisisgood
[+] YouPorn: https://youporn.com/uservids/thisisgood
[+] aminoapp: https://aminoapps.com/u/thisisgood
[+] drive2: https://www.drive2.ru/users/thisisgood
[+] fl: https://www.fl.ru/users/thisisgood
[+] geocaching: https://www.geocaching.com/p/default.aspx?u=thisisgood
[+] jeuxvideo: http://www.jeuxvideo.com/profil/thisisgood?mode=infos
[+] last.fm: https://last.fm/user/thisisgood
[+] mercadolibre: https://www.mercadolibre.com.br/perfil/thisisgood
[+] metacritic: https://www.metacritic.com/user/thisisgood
[+] osu!: https://osu.ppy.sh/users/thisisgood
[+] pikabu: https://pikabu.ru/@thisisgood
[+] xHamster: https://xhamster.com/users/thisisgood

[*] Results: 81

[!] End: The processing has been finished.
(venv)-(gz@kali)-[~/Documents/research/tools/Sherlock]
$
```


OSINT - Frameworks

- Many OSINT tools
- Recopilation:
 - [OSINTFramework](#)
 - [Awesome-OSINT](#)
- OSINT tools integrated:
 - [IKy](#)
 - [Lampyre](#)
 - [Maltego](#)



People Hacking

The weakest link

Spear Phishing – Avatar

Avatar: fake profile

- False information: <https://www.fakenamegenerator.com/>
- False face: <https://thispersondoesnotexist.com/>
- Virtual phone numbers: <https://hushed.com/>
- Virtual credit cards: *do some OSINT*
- [Voice changer](#), Instagram filters, Deep Fake ([Tom Cruise](#), [How it was made](#)), realistic human face masks, etc.

Spear Phishing - More Resources

- [OneMillionTweetMap](#)
- [IKnowWhereYourCatLives](#)
- [IKnowWhatYouDownload](#)
- [CanaryTokens](#)

People Hacking

- Not trained enough
- Some techniques
 - Identity Spoofing
 - Identity Theft
 - Hardware Introduction
 - Insider Agent



Social Engineering

- Human Vulnerabilities
 - Intense Emotions
 - Fear
 - Euphoria
 - Curiosity
 - Rage
 - Guilt
 - Urgency
 - Trust



Social Engineering - Phishing

- Spam (*mass phishing*)
 - Smishing (*SMS phishing*)
- Vishing (*Voice phishing*)
- Pharming
- Spear Phishing
 - Whaling

Some Techniques

Spoof sender email

Attach malicious files

Use of malicious links

Some Features of mass phishing

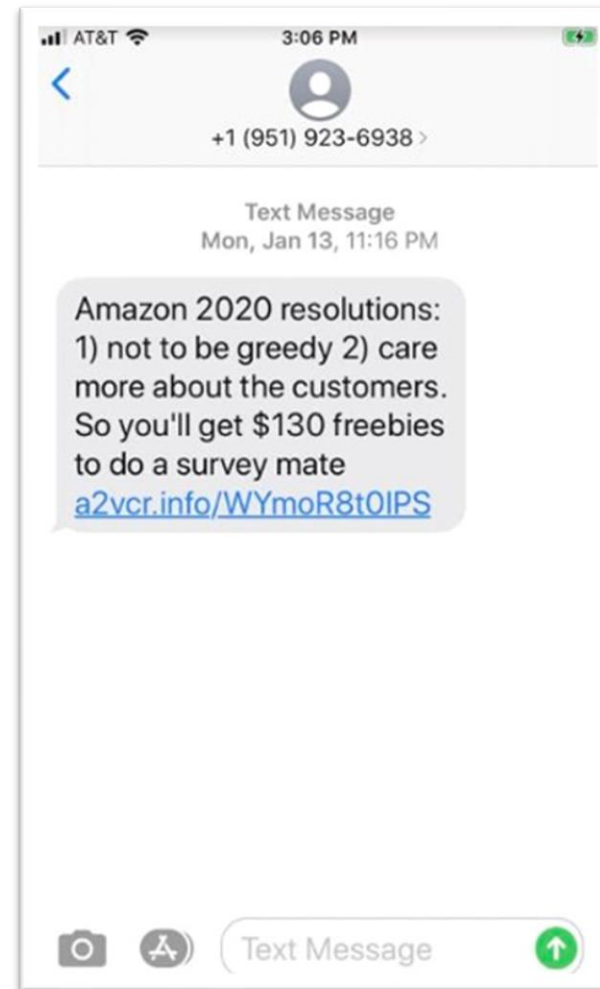
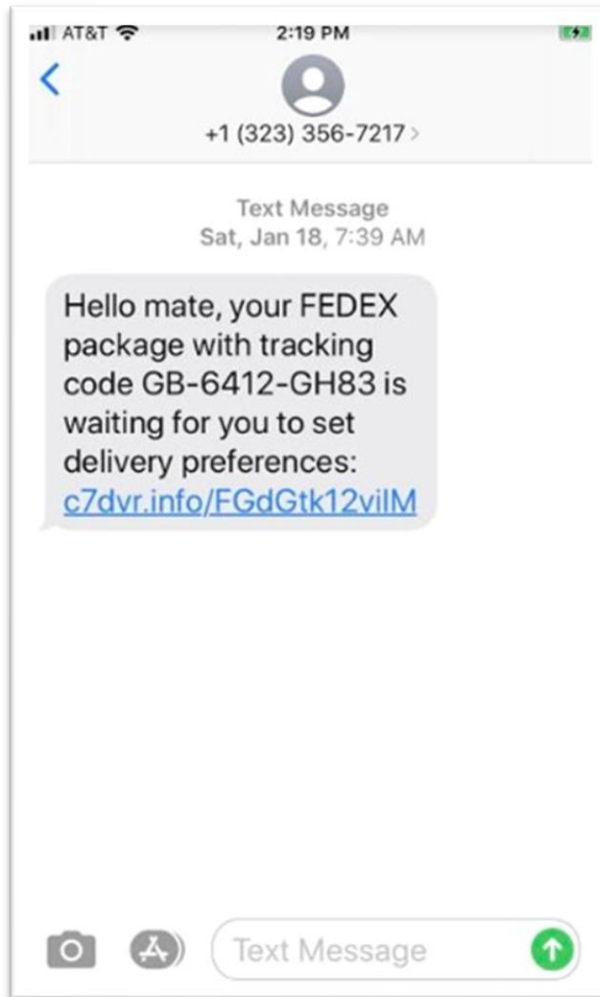
Generic, not personalised

Loads of typos

Unnatural writing

Senseless messages

Social Engineering – Phishing – Smishing



Social Engineering – Phishing – Vishing

- More effective
 - Immediate response – little or no time to think
 - Victim's feedback – attacker can manipulate them
 - People tend to trust voice call more
- Some common methods
 - Virtual kidnapping ([link](#))
 - Computer technician calling for a virus
 - Romance scam

Techniques
Spoof telephone number
Record your voice
Synthesize someone's voice

Social Engineering – Phishing – Masking URLs

- Masking link with another link
 - Example: `google.com`
 - Solution: Hover over links
- Triggering a function through an event
 - Example: ``
 - Solution: Deactivate Scripts on the browser
- Using short links
 - Solution: Use an unshortener, e.g.: unshorten.it.

Social Engineering – Phishing – Typosquatting

- Registering a misspelled domain

technique	example	technique	example
omission	gogle.com	hyphenation	goo-gle.com
repetition	gooogle.com	subdomain	g.oogle.com
insertion	googl1e.com	homoglyph	googfe.com
transposition	goolge.com	bitsquatting	coogle.com
replacement	google.com	tld swapping	google.corn

- Easy to spot, isn't it?

Social Engineering – Phishing – Typosquatting

- Generation
 - DNSTwist
 - [Web](#)
 - [CLI](#)

```
replacement googlr.com 216.58.215.132 2a00:1450:4003:800::2004 NS:ns1.google.com MX:
replacement googls.com -
replacement googlw.com NS:dns1.name-services.com MX:mx.googlw.com,cust.a.hostedemail.com
replacement googlz.com 66.81.199.55 NS:ns1.dsredirects.com
replacement googoe.com 66.81.199.51 NS:ns1.dsredirection.com
replacement googpe.com -
replacement goohle.com 47.254.33.193 NS:ns3.dns.com
replacement gootle.com 66.81.199.51 NS:ns1.dsredirection.com
replacement goovle.com 23.82.12.34 NS:ns1.brainydns.com
replacement gooyle.com 66.81.199.51 NS:ns1.dsredirection.com
replacement goozle.com 50.62.97.1 NS:ns29.domaincontrol.com MX:mailstore1.secureserver.net
replacement gopgle.com -
replacement gpogle.com 192.157.56.141 NS:ns1.kirklanddc.com
replacement hoogle.com 107.180.25.196 NS:ns41.domaincontrol.com MX:mailstore1.secureserver.net
replacement toogle.com 107.161.23.204 NS:ns1.dnsowl.com
replacement voogle.com 3.64.163.50 NS:ns1.dan.com
replacement yoogle.com 127.0.0.1 NS:ns1.sedoparking.com MX:localhost
replacement zoogle.com 15.197.142.173 NS:ns53.domaincontrol.com MX:mailstore1.secureserver.net
subdomain g.oogle.com 104.21.19.57 2606:4700:3032::ac43:b945 NS:amir.ns.cloudflare.com MX:mx.zoho.com
subdomain go.ogle.com -
subdomain goo.gle.com 13.248.216.40 NS:ns3.afternic.com MX:
subdomain goog.le.com -
transposition gogole.com 142.250.184.4 2a00:1450:4003:808::2004 NS:ns1.google.com MX:
transposition googel.com 142.250.200.68 2a00:1450:4003:80d::2004 NS:ns1.google.com MX:
transposition goolge.com 142.250.200.68 2a00:1450:4003:80d::2004 NS:ns1.google.com MX:
transposition ogoogle.com 142.250.200.132 2a00:1450:4003:80f::2004 NS:ns1.google.com MX:
various googlecom.com 142.250.201.68 2a00:1450:4003:811::2004 NS:ns1.google.com MX:
vowel-swap gaogle.com 107.180.51.12 NS:ns25.domaincontrol.com MX:mail.gaogle.com
vowel-swap geogle.com 78.41.204.31 NS:ns1.torresdns.com MX:mail.h-email.net
vowel-swap goagle.com 89.145.66.234 NS:ns1.netnames.net MX:relay1.netnames.net
vowel-swap goegle.com 103.224.182.246 NS:ns1.above.com MX:park-mx.above.com
vowel-swap googli.com 162.255.119.253 NS:freedns1.registrar-servers.com
vowel-swap googlo.com -
vowel-swap gouggle.com NS:ns1.googledomains.com
vowel-swap guogle.com 64.190.63.111 NS:ns1.sedoparking.com MX:localhost
```

Social Engineering – Phishing – Homoglyph

- Punycode: ASCII representation of Unicode characters

text (homoglyphs)	punycode
google.com	
google.com	
google.com	
google.com	

- [Punycode converter](#), [russian keyboard](#), [homoglyph generator](#).
- Analysing domains: [URLVoid](#), [URLScan](#), [DNSDumpster](#), [TalosIntelligence](#), [VirusTotal](#).

Social Engineering – Quizzes

- Phishingbox: <https://www.phishingbox.com/phishing-iq-test>
- Complete-it (context): <https://www.complete-it.co.uk/cyber-security-phishing-quiz/>
- Security Inside (actions taken): <https://phishingquiz.securityinside.com/quiz/start?id=1>
- Google Phishing Quiz (interactive): <https://phishingquiz.withgoogle.com/>

InfoSec culture:

- CybSafe (interactive): <https://www.cybsafe.com/quizzes/>

Social Engineering – USB – USB Drop

I have just found a thumb drive, lucky me!

- Attack vectors
 - Social Engineering
 - Vulnerability: curiosity
 - Bait (appealing): salary, XXX, etc.
 - HID Spoofing (e.g.: Rubber Ducky)
 - 0-day (e.g.: *Stuxnet*)

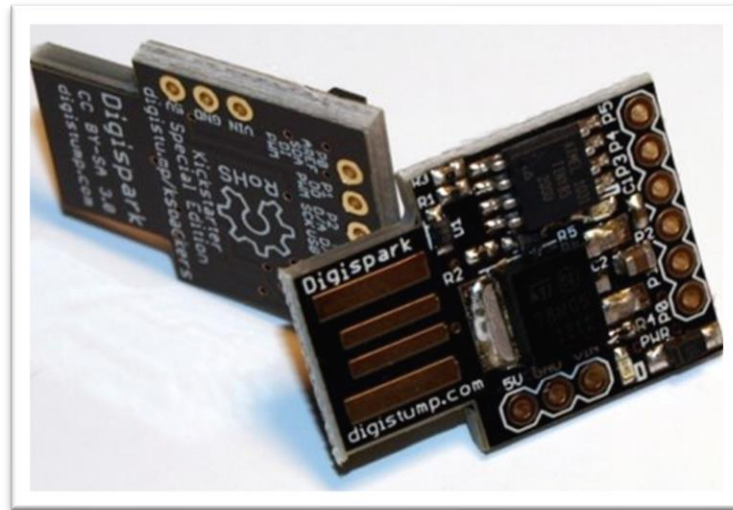


[Does dropping USB drives really work? BlackHat USA \(2006\)](#)

Social Engineering – USB – Rubber Ducky

When you have little time span to type

- HID (Human Interface Device)
 - It behaves as a keyboard
 - It bypasses USB block policies



Social Engineering – USB – Juice Jacking

The dangers of public USB charging stations

- Solution
 - Carry your own portable charger
 - Use a Datablocker



Social Engineering – USB – USB Killer

When data is not the main target...

- Why?
 - The competition (companies)
 - Sabotage (ex-employee, vandalism)



Note: this technique will **not** be useful to gather information.

Student destroyed US\$ 58,000 worth of college computers: [link](#).

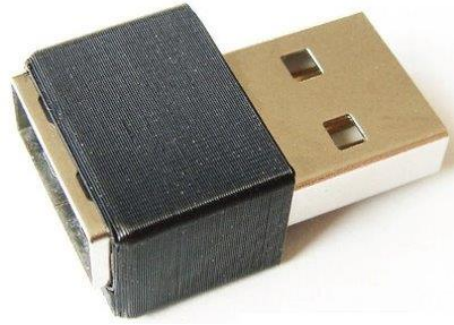
Malware

Malware (***Malicious Software***)

- Some examples
 - Virus
 - Ransomware
 - Worm
 - Trojan
 - Backdoor
 - Spyware
 - Keylogger
 - Screenlogger
 - Logic/Time bomb

Malware – Spyware – Keylogger

- Target information: credentials, cryptowallets, PINs, etc.
- Types
 - Hardware
 - Software
 - Local
 - Remote



[O.MG cable](#)

Malware – Spyware – Screenlogger

- Target information: credentials, cryptowallets, PINs, etc.
- Types
 - Hardware
 - Software
- There is a context, unlike with a keylogger
- Content from protected fields not seen
 - Example: `<input type="password" name="pwd">`
 - Solution: use along with keylogger



Extra Resources

There is more...

Documentaries, presentations, CTFs and more

- [From email address to telephone number. A new OSINT approach, by Martin Vigo \(BSides 2019\) \[31:05\]](#).
- [Live recon and automation on Shopify's Bug Bounty Program with @TomNomNom \(NahamSecCon 2021\) \[1:17:17\]](#).
- [The Bug Hunter's methodology v4 – Recon edition by @jhaddix \(NahamSecCon 2020\) \[1:39:42\]](#).
- [Anatomy of a Killing – BBC \[11:06\]](#).
- [Hackers Find Missing People for Fun \[6:06\]](#).
- CTF (Capture The Flag): cybersecurity challenges.
 - Contests: <https://ctftime.org/>
 - Set of CTF pages: <https://ctfsites.github.io/>
 - OSINT CTFs: [OsintDojo](#), [OsintGames](#), [Trace Labs](#) (searching for missing people).
 - DFIR CTFs: [CyberDefenders](#).
 - Web3 CTFs: [Ethernaut](#) (Smart Contracts).
- Bug bounty platforms: websites where companies' security can be assessed and "pay" for bugs hunted.
 - [BugCrowd](#), [HackerOne](#), [Intigriti](#).
- More (useful?) links: [IsItHacked](#), [IsItUp](#), [PanoptiClick](#).



References

Links

- <https://domaineye.com/reverse-whois/>
- <https://github.com/OWASP/Amass>
- <https://github.com/fwaeytens/dnsenum>
- <https://github.com/darkoperator/dnsrecon>
- <https://github.com/aboul3la/Sublist3r>
- zonetransfer.me
- <https://github.com/ffuf/ffuf>
- <https://github.com/tomnomnom/assetfinder>
- <https://github.com/tomnomnom/httpprobe>
- <https://github.com/tomnomnom/waybackurls>
- <https://github.com/tomnomnom/anew>
- <https://github.com/wappalyzer/wappalyzer>
- <https://github.com/urbanadventurer/WhatWeb>
- <https://github.com/zaproxy/zaproxy>
- <https://portswigger.net/burp/communitydownload>

Links

- https://cheatsheet.haax.fr/open-source-intelligence-osint/dorks/github_dorks/
- <https://github.com/random-robbie/keywords/blob/master/keywords.txt>
- <https://github.com/obheda12/GitDorker>
- https://github.com/ROCXYROCK/CTF_Beginners_Git_Challenge
- <https://www.shodan.io/search/filters> (Shodan dorks)
- <https://github.com/achillean/shodan-python>
- <https://censys.io/>
- <https://search.censys.io/search/examples?resource=hosts> (Censys dorks)
- <https://nmap.org/>
- <http://advangle.com/> (Dorks)
- <https://www.exploit-db.com/google-hacking-database> (GHDB)
- <https://unlistedvideos.com/> (unlisted Youtube videos)
- <https://archive.org/search.php> (WaybackMachine)
- <https://github.com/laramies/theHarvester> (theHarvester)
- <https://github.com/sherlock-project/sherlock> (Sherlock)

Links

- <https://www.namecheck.com/>
- <https://haveibeenpwned.com/> (HIBP)
- <https://intelx.io/> (IntelligenceX)
- <https://github.com/martintjj/BreachCompilation>
- <https://pwdquery.xyz/>
- <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- <https://github.com/digininja/cewl>
- <https://github.com/Mebus/cupp>
- <https://www.crunchbase.com/>
- <https://hunter.io/>
- <https://github.com/m8sec/CrossLinked>
- <https://www.verifyemailaddress.org/>
- <https://phonebook.cz/>
- <https://gchq.github.io/CyberChef/>
- <https://crackstation.net/>

Links

- <https://howsecureismypassword.net/>
- https://en.wikipedia.org/wiki/List_of_the_most_common_passwords
- <https://whatsmyname.app/>
- <https://osintframework.com/>
- <https://www.maltego.com/>
- <https://kennbroorg.gitlab.io/ikyweb/>
- <https://lampyre.io/>
- <https://github.com/jivoi/awesome-osint>
- <https://github.com/smicallef/spiderfoot>
- <https://www.fakenamegenerator.com/>
- <https://thispersondoesnotexist.com/>
- <https://hushed.com/> (Virtual phone number service)
- <https://www.voicemod.net/>
- <https://www.youtube.com/watch?v=qTgPSKKjfVg> (DALL-E 2)
- <https://onemilliontweetmap.com/>

Links

- <https://iknowwheryourcatlives.com/>
- <https://iknowwhatyoudownload.com>
- <https://www.canarytokens.org/>
- <https://www.youtube.com/watch?v=opRMrEfAlil> *(What is your password?)*
- <https://cybernews.com/editorial/fake-kidnap-scams-from-a-prison-cell-in-mexico-to-the-boardroom-of-a-top-firm/>
- <https://www.which.co.uk/consumer-rights/advice/microsoft-phone-scam-aYceu8o7aO4c>
- <https://www.truecaller.com/>
- <https://www.listarobinson.es/>
- <https://dnstwist.it/> *(DNSTwist web)*
- <https://github.com/elceef/dnstwist.git> *(DNSTwist CLI)*
- <https://www.punycoder.com/>
- <https://www.lexilogos.com/keyboard/russian.htm>
- <https://www.irongeek.com/homoglyph-attack-generator.php>
- <https://urlvoid.com/>
- <https://urlscan.io/>

Links

- <https://dnsdumpster.com>
- <https://talosintelligence.com/>
- <https://www.virustotal.com/>
- <https://www.phishingbox.com/phishing-iq-test> (phishing quiz)
- <https://www.complete-it.co.uk/cyber-security-phishing-quiz/> (phishing quiz)
- <https://phishingquiz.securityinside.com/quiz/start?id=1> (phishing quiz)
- <https://phishingquiz.withgoogle.com/> (phishing quiz)
- <https://www.cybsafe.com/quizzes/> (quiz)
- <https://www.youtube.com/watch?v=ZI5fvU5QKwQ> (USB drop - BlackHat USA 2016)
- <https://juicejacking.org/product/datablock/>
- <https://usbkill.com/>
- <https://www.youtube.com/c/UsbKill> (Testing the USBKill)
- <https://www.theverge.com/2019/4/17/18412427/college-saint-rose-student-guilty-usb-killer-destroyed-computers>
- https://www.youtube.com/watch?v=-jL_Xz-BKBM (O.MG Keylogger cable)
- <https://www.keydemon.com/> (Spyware)