

# OSINT

Beware. Your data is out there.  
0xoposec - 19/01/2023

# Aviso Legal & Leis

# Aviso Legal

## Disclaimer - Boring but necessary

- ▶ Toda a informação contida nesta apresentação destina-se exclusivamente para **fins educacionais e de consciencialização**.
- ▶ **Apresentação ao vivo**. Não é um ambiente controlado e alguns conteúdos podem ser inapropriados para alguns participantes.
- ▶ **Declino qualquer responsabilidade** pelo uso, uso indevido, download, ou visualização dos links desta apresentação.
- ▶ Esta apresentação não está relacionada com o meu trabalho ou empregador.



# Aviso Legal

## Disclaimer - Avoid illegal activities

- ▶ Alguns links, sites, software ou outros itens listados podem ou não ser legais, delito, crime no seu país.
- ▶ Por favor, **verifique que lhe é permitida** a consulta dos sites, e o eventual uso do software listado.
- ▶ Ignorância acerca das leis aplicáveis **não é desculpa** para transgressões ou actividades ilegais.
- ▶ Atividades ilegais podem implicar problemas ou mesmo prisão.
- ▶ **Verifique sempre o que é legal e as leis aplicáveis.**



# Leis

## Portuguese Law and Organizations

- ▶ Lei
  - ▶ Diário República Eletrónico ([link](#))
  - ▶ ANACOM ([link](#))
- ▶ Organizações
  - ▶ CNCS – Centro Nacional de Cibersegurança ([link](#))
    - ▶ Incident Notification ([link](#))
    - ▶ CERT.PT ([link](#))
  - ▶ Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) ([link](#))
  - ▶ Ministério Público ([link](#))

OSINT Time

# OSINT - Open-source intelligence

## Digital Footprint

- ▶ Open-source intelligence (OSINT) consiste na recolha e análise de dados obtidos de fontes disponíveis ao público em geral, como jornais, revistas científicas e comunicação social para produzir informação inteligente.
- ▶ Colecionar dados de:
  - ▶ motores de busca (Google, ...)
  - ▶ redes sociais (Facebook, ...)
  - ▶ sites governamentais
  - ▶ mapas
  - ▶ ...
- ▶ E depois extrair/relacionar/inferir nova informação com maior valor/potencial.

# Who Am I

## Let's OSINT me 😊

- ▶ Just got a name
  - ▶ Pedro António Oliveira Vieira
- ▶ Google ([link](#)) ➡
- ▶ Google “Improved Search” ([link](#)) ➡
- ▶ Google “Improved Search” ([link](#)) ➡
- ▶ LinkedIn ([link](#)) ➡
  - ▶ Public profile was showing way too much
- ▶ Certified **Ethical** Hacker ([link](#)) ➡
- ▶ My github notes ([link](#)) ➡





# Search Engines

## Internet is more than Google

- ▶ Motores de busca diferentes → regras/crawlers diferentes → resultados diferentes
- ▶ Google ([link](#))
- ▶ Bing ([link](#))
- ▶ Yahoo ([link](#))
- ▶ DuckDuckGo ([link](#))
- ▶ Baidu (China) ([link](#))
- ▶ Yandex (Russia) ([link](#))
- ▶ You may ask to be removed from one search engine, not all ☹ ([link](#))

# Search operators

## Improve the search

- ▶ Google Advanced Search ([link](#)) ➡
- ▶ **filetype**: search your results based on the file extension
- ▶ **cache**: This operator allows you to view cached version of the web page.
- ▶ **allinurl**: This operator restricts results to pages containing all the query terms specified in the URL.
- ▶ **inurl**: This operator restricts the results to pages containing the word specified in the URL
- ▶ **allintitle**: This operator restricts results to pages containing all the query terms specified in the title.
- ▶ **link**: This operator searches websites or pages that contain links to the specified website or page.
- ▶ **info**: This operator finds information for the specified web page.
- ▶ **location**: This operator finds information for a specific location.
- ▶ **42 Advanced Operators** ([link](#))

# Search

## Dork Examples - Curriculum Vitae

- ▶ Google Search ([link](#)) ➡
- ▶ Google Search - List site/directories contents ([link](#)) ➡
- ▶ “curriculum vitae” filetype:pdf inurl:upload
  - ▶ “curriculum vitae” – keywords to look for
  - ▶ filetype:pdf - only pdf files
  - ▶ inurl:upload
- ▶ Available information on **pay slips** “recibo de vencimento” ([link](#))
  - ▶ Full name, address, nif, nib, marital status, number of children, ...

# Search

## Dork Examples - Hacked

- ▶ Google Search ([link](#)) ➡
- ▶ “hacked by” **site:pt**
  - ▶ “hacked by” - keyword to look for
  - ▶ site:pt - only “portuguese” sites (registered portuguese domains)
- ▶ About 13.400 results
  - ▶ Sites / pages that were “tagged”/”signed”
  - ▶ Attack and contents changed to show off skills (mainly kids) – compared to street tagging

# Google Dorks

## Commonly used searches

- ▶ Google Hacking Database ([link](#)) ➡
- ▶ gbhackers ([link](#))
- ▶ google-dork-list ([link](#))
- ▶ Google Advanced Operators Guide ([link](#))
- ▶ Google Advanced Operators Reference ([link](#))

# OSINTing

# OSINT yourself

## How the internet sees YOU

- ▶ Search your name on Google and analyze the results
  - ▶ As you saw the search can be improved
- ▶ Some results can/will include:
  - ▶ Family and Friends
  - ▶ Work
  - ▶ School grades
  - ▶ BI - Identity Card Number (yes)
  - ▶ NIF – Tax Identification Number
- ▶ That is typically information to **verify your identity** over a phone call.

# OSINT

## Portugal - Vehicle Information

- ▶ Automóvel On-line ([link](#)) ➡
- ▶ Certidão Permanente Automóvel ([link](#)) ➡
  - ▶ License Plate : “89-QS-04” ([link](#)) ➡
  - ▶ Result
    - ▶ Brand: MERCEDES-BENZ
    - ▶ VIN: WDD2221631A248762
  - ▶ Example ([link](#)) ➡
- ▶ Vehicle Information ([link](#))
  - ▶ Example ([link](#)) ➡
  - ▶ Information: Brand, Model, Location, Paint, Delivery Date, Extras, ...
- ▶ Hack across the globe by VIN ([link](#)) ➡



# OSINT

## Portugal - Insurance Information

- ▶ ASF – Autoridade de Supervisão de Seguros e Fundos de Pensões ([link](#)) ➡
  - ▶ Example ([link](#))
    - ▶ License Plate : “01-EF-34”
    - ▶ Date : “03-07-2022”
  - ▶ Example 2 ([link](#))
    - ▶ License Plate : “01-EF-34”
    - ▶ Date : “03-07-2012”
- ▶ Insurance Company
  - ▶ Current and Past
  - ▶ Length of the contract
  - ▶ Insurance policy number
  - ▶ Is it possible to get information for all license plates ????

# OSINT

## Portugal Specific

- ▶ DGES - Direção-Geral de Ensino Superior ([link](#)) ([link](#)) ➡
- ▶ DGAE - Direção – Geral da Administração Escolar ([link](#)) ➡
- ▶ DRE - Diário da República ([link](#))
  - ▶ Search DRE ([link](#))
- ▶ Ministério da Justiça – Publicações ([link](#)) ➡
- ▶ Instituto Nacional da Propriedade Industrial ([link](#)) ➡

# OSINT

## Portugal Specific

- ▶ Registo Predial Online ([link](#))
- ▶ Finanças - Penhorados ([link](#))
  - ▶ Example ([link](#)) ➡
  - ▶ Search Penhorados – ([link](#))
- ▶ Ministério da Justiça - Penhorados ([link](#)) ➡
- ▶ Plataforma Eletrónica de Compras (Administração Pública) ([link](#))
- ▶ Leaked information:
  - ▶ Full Names, Addresses, NIF, Company, Marital Status, ...

# OSINT

## Portugal - Public contracts

- ▶ Base ([link](#))
  - ▶ The example ([link](#)) ➡
- ▶ PDF of contract with PII strikethrough ([link](#))
  - ▶ Open with pdf reader and delete the strikethrough boxes
  - ▶ Name of employee who edited the document
    - ▶ Information on UA, LinkedIn, Facebook, ...
  - ▶ Metadata: “KONICA MINOLTA bizhub C454”
- ▶ Information leaked
  - ▶ Full Names, nif, addresses

# Deadly Social Media

## The Final Hours of Pop Smoke

- ▶ Rapper Pop Smoke Murdered in Home Invasion ... By 4 Masked Gunmen ([link](#)) ➡
- ▶ Instagram Posts
  - ▶ Location Tag
- ▶ Geolocation
  - ▶ Reverse Image
- ▶ Google Maps
  - ▶ Local Recon
- ▶ Airbnb/Zillow (Rent/Real-estate)
  - ▶ House photos (Outside and Inside)
  - ▶ Layout
- ▶ YouTube Video: The Cyber Mentor ([link](#))

# OSINT

## Profiling Awareness

- ▶ Mobile (how long have you been using the same number)
  - ▶ Sync me ([link](#))
- ▶ Usernames (you reuse usernames)
  - ▶ NameChk ([link](#)) ➡
  - ▶ WhatsMyName ([link](#))
  - ▶ NameCheckup ([link](#)) ➡
- ▶ Tinder
  - ▶ Username reuse ([link](#)) ➡
- ▶ New awesome tools are always being created

# OSINT

## Profiling Awareness

- ▶ What's my IP? ([link](#))
- ▶ Ip2Location ([link](#))
- ▶ Mylocation ([link](#)) ➡
- ▶ Twitter
  - ▶ Twitter Advanced Search ([link](#)) ➡
- ▶ Facebook
  - ▶ StalkFace ([link](#))
  - ▶ Sowdust Github ([link](#))
  - ▶ IntelligenceX Facebook Search ([link](#))

# OSINT

## Profiling - Professional

- ▶ LinkedIn ([link](#)) ➡
- ▶ Xing ([link](#)) ➡
- ▶ Curriculum Vitae
  - ▶ Sending CV with too much information – what is too much ☺
    - ▶ Home address – Street View
- ▶ Company Information
  - ▶ Technologies described in job adds (leaking information)
- ▶ Professional information phishing
  - ▶ Fake job adds (Is this a thing?)



# OSINT

## (Reverse) Image search

- ▶ One image is worth 1000 words, maybe more.
  - ▶ What information can be extracted from a photo ?
- ▶ Google Images ([link](#))
- ▶ Bing Images ([link](#)) ➡
- ▶ Yahoo Images ([link](#))
- ▶ TinEye ([link](#))
- ▶ Yandex ([link](#))
- ▶ The professionals (video explaining) ([link](#))


# OSINT - Photos Metadata

- Metadata
- GPS ([link](#)) ➡
- Google Maps ([link](#)) ➡

**exifdata**

**SUMMARY**  
**DETAILED**  
**LOCATION**  
**UPLOAD**

IMG\_20190223\_163027.jpg



(click for original)

**Camera**  
Xiaomi Redmi 3

**GPS Position**  
40.989952 degrees N, 7.395051 degrees W

**Date of Creation**  
2019:02:23 16:30:27

**Resolution**  
4160x3120

**SUMMARY**

Make	Xiaomi
Model	Redmi 3
Aperture	2
Exposure Time	1/1506 (0.00066401062416999 sec)
Focal Length	4.2 mm
Flash	Auto, Did not fire
File Size	1447 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	4160
Image Height	3120
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	72
Y Resolution	72
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
YCbCr Positioning	Centered
Exposure Program	Not Defined
Date and Time (Original)	2019:02:23 16:30:27
Metering Mode	Center-weighted average
Color Space	sRGB
Exposure Index	140
Sensing Method	Unknown (0)
Exposure Mode	Auto
Focal Length In 35 mm Format	0 mm
Scene Capture Type	Standard
Gain Control	Low gain up
ISO	100
Compression	JPEG (old-style)

# OSINT - Photos

## No Metadata but still lots of Information

- ▶ Where was this image taken?
  - ▶ Have you been there?
- ▶ When?
  - ▶ Date stamp on photo
  - ▶ Filename with date
  - ▶ Metadata
- ▶ What else?
- ▶ Image search
  - ▶ Identify the castle? ➡
- ▶ CleanUp ([link](#)) ➡
- ▶ AperiSolve ([link](#)) ➡



# OSINT

## Street View

- ▶ Google Street View ([link](#))
  - ▶ Identify house by address
  - ▶ Assess security (cameras, fences, ...)
  - ▶ Parked cars (timeline, ...)
  - ▶ People's habits/routines, timetables, ...
- ▶ View the past – timeline ([link](#)) ➡
- ▶ Instant Street View ([link](#))

# OSINT Maps

- ▶ Google Maps ([link](#))
- ▶ Bing Maps ([link](#))
- ▶ Wikimapia ([link](#))
- ▶ DualMaps ([link](#)) ➡
- ▶ Tips, Tricks and Techniques ([link](#))

# Search

## Satellite View

- ▶ Zoom Earth ([link](#))
- ▶ Satellites Pro ([link](#))
- ▶ World Imagery ([link](#))
  - ▶ Wayback ([link](#))
  - ▶ Wayback example ([link](#)) ➡
- ▶ View the past - timeline

# OSINT MEMORY

## Internet in the past

- ▶ Wayback Machine ([link](#))
  - ▶ Example ([link](#)) ➡
- ▶ Archive.is ([link](#))
- ▶ Cached Pages ([link](#))
- ▶ Cached View ([link](#))
- ▶ OldWeb.Today ([link](#))
- ▶ Time Travel ([link](#))
  
- ▶ Github commits 😊

# Databreach

## Company credentials ?

- ▶ Source
  - ▶ Publicly available list of credentials
  - ▶ More than 10k credentials just for Bosch
- ▶ Information gathered
  - ▶ Rule of email/login
    - ▶ (FirstName.LastName)@((Country).(company).com)
  - ▶ Rule of password complexity
  - ▶ List of users
    - ▶ Phishing campaigns
    - ▶ Brute force
    - ▶ Look for those users on Social Media
- ▶ HaveIBeenPwned ([link](#)) ➡

Email/Login	Password
data/m/i/c:mich	er@de.bosch.com:\$HEX[576569c3
data/m/i/c:mich	er@de.bosch.com:Weißer
data/m/i/c:mich	zkus@de.bosch.com:shannon
data/m/i/c:mich	tke@bosch.com:lumpi007
data/m/i/c:mich	der@de.bosch.com:a6fc6b19
data/m/i/c:mich	z4@de.bosch.com:jaguar
data/m/i/c:mich	@us.bosch.com:ultra06
data/m/i/c:mich	@cz.bosch.com:micsis
data/m/i/c:mich	ll@uk.bosch.com:frances
data/m/i/c:mich	@bosch.com:petros69
data/m/i/c:mich	us.bosch.com:mike5920
data/m/i/c:mich	n@us.bosch.com:radar123
data/m/i/c:mich	om@us.bosch.com:2af415a2174b1
data/m/i/c:mich	om@us.bosch.com:hardrock
data/m/i/c:mich	rger@za.bosch.com:mike123
data/m/i/c:mich	cn.bosch.com:Mikomido
data/m/i/c:mich	@us.bosch.com:bulldog3120
data/m/i/c:mich	@de.bosch.com:maccaroni
data/m/i/c:mich	mann@de.bosch.com:\$HEX
data/m/i/c:mich	mann@de.bosch.com:asdfjklö
data/m/i/c:mich	mann@de.bosch.com:asdfjklr¶
data/m/i/c:mich	comcast.net:mojopapa
data/m/i/c:mich	comcast.net:mojopapa1
data/m/i/c:mich	s.bosch.com:bogey
data/m/i/c:mich	cz.bosch.com:koqueti
data/m/i/c:mich	cz.bosch.com:wunazaqu
data/m/i/c:mich	zak@pl.bosch.com:igi74mick77
data/m/i/c:mich	z.bosch.com:hyqokibu
data/m/i/c:mich	@fr.bosch.com:CHOISNE
data/m/i/c:mich	@be.bosch.com:elsclaes
data/m/i/c:mich	de.bosch.com:janlasse79
data/m/i/c:mich	nl.bosch.com:Killer1
data/m/i/c:mich	ey@us.bosch.com:leander65
data/m/i/c:mich	r.bosch.com:ro67vsh5
data/m/i/c:mich	nte@it.bosch.com:michele
data/m/i/c:mich	lli@us.bosch.com:radica4
data/m/i/c:mich	de@br.bosch.com:m1s2g3a4
data/m/i/c:mich	hi@br.bosch.com:Talita
data/m/i/c:mich	@br.bosch.com:Orquideas1



# OSINT IOT

## Internet of Things

- ▶ Does it have radio?
  - ▶ Wireless, Bluetooth, ZigBee, ...
- ▶ Federal Communications Commission ([link](#))
  - ▶ FCCID.IO ([link](#)) ➡
  - ▶ ZDER3 ([internal](#)) ➡
- ▶ Datasheets
  - ▶ Datasheets ([link](#))
  - ▶ AllDatasheet ([link](#))

# Before you start OSINTing

Don't get under the spotlight.

# OSINT Notes

## My notes and some links

- ▶ My OSINT notes ([link](#)) ➡
  - ▶ OSINT (Presentation)
  - ▶ Awareness (Presentation)
- ▶ Sofia Santos - How to do a small OSINT investigation ([blog](#)) ([video](#))
- ▶ Michael Bazzel – IntelTechniques ([link](#)) ([book](#)) ([magazine](#))
- ▶ OSINT Combine ([link](#)) ([bookmarks](#))
- ▶ OSINT Dojo ([link](#))
- ▶ OSINTCurio.us ([link](#))
- ▶ OSINT Techniques ([link](#))
- ▶ Start.me pages ([link](#)) ([example](#)) ➡
- ▶ Technisette ([link](#))
- ▶ Open Source Intelligence Tools and Resources Handbook 2020 ([link](#))

# CTF

## Capture The Flag & Challenges

- ▶ TraceLabs CTF ([link](#)) ([notes](#))
- ▶ Hacktoria ([link](#)) ([notes](#))
- ▶ Cyber Detective CTF ([link](#))
- ▶ Cyber Investigator CTF ([link](#))
- ▶ TryHackMe ([link](#))
  - ▶ Search for OSINT ([link](#)) ([notes](#))
- ▶ Blue Team Labs Online - Cyber Range ([link](#))

# OSINT

## Sock Puppets

- ▶ Name Generator ([link](#)) ➡
- ▶ Photo - thispersondoesnotexist ([link](#))
- ▶ Sim Card - Local / Country / Electronic
- ▶ Credit Card - Privacy.com ([link](#))
- ▶ VPN - usefull to be some where else
- ▶ Email account
- ▶ Social Media accounts
- ▶ Sock Puppets Tutorials
  - ▶ The Art Of The Sock ([link](#))
  - ▶ My Process for Setting up Anonymous Sock Puppet Accounts ([link](#))

# OSINT

## Tools & more tools

- ▶ OSINT FRAMEWORK ([link](#)) ➡
  - ▶ Yups, only one link is all it takes. But others worth mentioning.
- ▶ OSINT4ALL ([link](#)) ➡
- ▶ Intel Techniques ([link](#)) ➡
- ▶ OSINT Techniques ([link](#))
- ▶ Technisette ([link](#))
- ▶ Cyber Detective ([link](#))
- ▶ OSINT Link ([link](#))
- ▶ Aware Online ([link](#))

# OSINT

## Virtual Machines

- ▶ Trace Labs VM ([link](#)) ➡
- ▶ Mandiant – Threat Pursuit VM ([link](#)) ➡
- ▶ CSI Linux ([link](#))
  
- ▶ Tails ([link](#))
- ▶ Kali ([link](#))
- ▶ Parrot ([link](#))
- ▶ Windows ([link](#))

Free to Share



# License

- ▶ Feel free to use/modify/share
- ▶ Teach someone
- ▶ Improve awareness

# Shodan

## Search Engine for Internet Of Things

- ▶ Internet Exposure Observatory
  - ▶ Exposure Dashboard ([link](#))
- ▶ Explore
  - ▶ Shodan explore ([link](#))
- ▶ Images
  - ▶ Shodan images ([link](#))
- ▶ Maps
  - ▶ Shodan maps ([link](#))

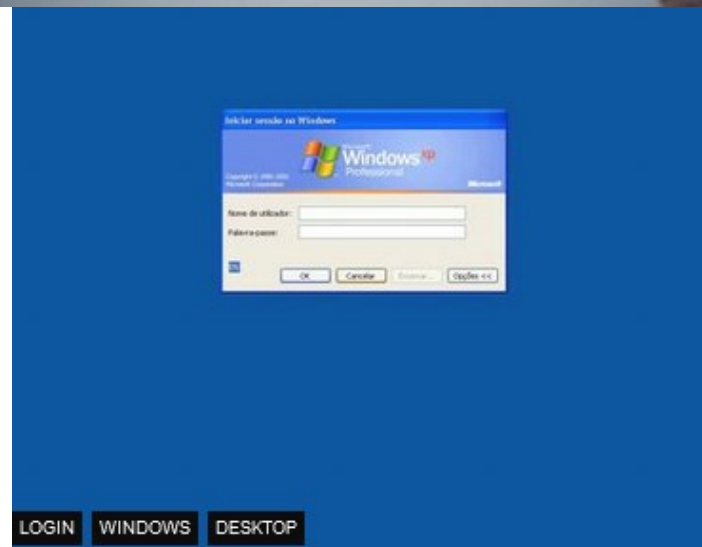
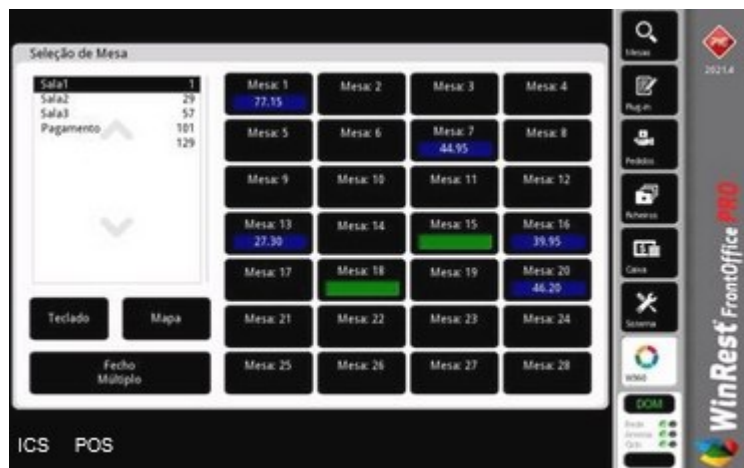
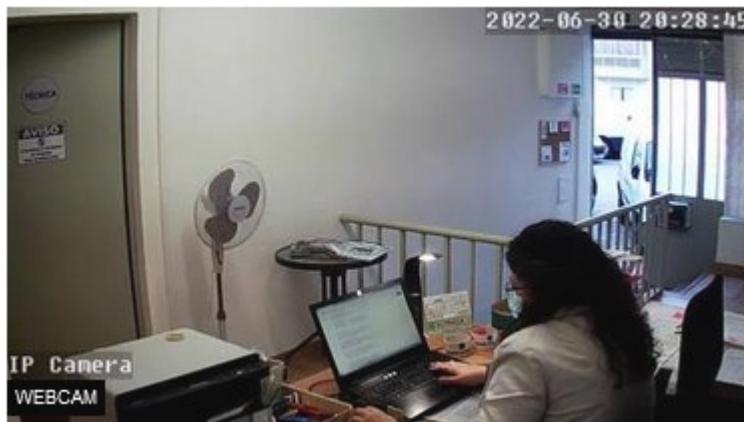
# Shodan

## Internet of Things

- ▶ Remote Desktop ([link](#))
  - ▶ Total results: 3,482,756
  - ▶ Braga ([link](#)) ➡
- ▶ Images
  - ▶ Braga ([link](#))
  - ▶ VNC Remote Access and Loggedin ([link](#)) ➡
- ▶ Authentication Disabled
  - ▶ Portugal ([link](#)) ➡
  - ▶ Primavera ([link](#))
- ▶ Contabilidade ([link](#)) ➡

# Shodan

## Internet of Things - Images



# ONLINE SAFETY

# Helping Tools

## Privacy

- ▶ VPN (Different country, different advertisements, what else ?)
  - ▶ ProtonVPN ([link](#)) ➡
- ▶ Temporary Email (Need to register? Activate software?)
  - ▶ 10 minute email ([link](#)) ➡
  - ▶ 20 minute email ([link](#))
- ▶ Disposable Email
  - ▶ 60 minute email ([link](#))
- ▶ Internet Access (DarkWeb included)
  - ▶ Tor ([link](#)) (internet browser) ➡
  - ▶ Tails ([link](#)) (OS that runs on usb or VM) ➡

# Helping Tools Safety

- ▶ VirusTotal
  - ▶ Check received files ([link](#)) ➡
    - ▶ (**don't upload Personal or Company related information**)
- ▶ Netcraft
  - ▶ Sitereport ([link](#)) (check for suspicious sites)
- ▶ Ransomware
  - ▶ No More Ransom ([link](#)) ➡
- ▶ Virtual Credit Card (online shopping)
  - ▶ Mbnet ([link](#)) ➡
  - ▶ Revolut ([link](#))
  - ▶ PayPal ([link](#))

# Awareness



# Awareness

## True stories - Healthy Meal

- ▶ Someone posted a photo of healthy meal during COVID
  - ▶ Working remotely on in the usual business environment
  - ▶ Company laptop was in the background
    - ▶ Zoomed in and was possible to read emails
    - ▶ Company private information could be leaked
    - ▶ Personal information on other persons was showing
- ▶ Social Media Apps use OCR
  - ▶ Means they also read the emails
  - ▶ And everyone else on that social media could get the same information

# Awareness

## True stories - Quiet vacations

- ▶ Long last deserving vacations
  - ▶ Too many friends at destination
  - ▶ So, warn no one and just relax on vacations
- ▶ I posted a picture on social media
  - ▶ My friends were alerted I was nearby
  - ▶ Friends on that location called me on the phone
  - ▶ Everyone else knew I was not home
    - ▶ Burglars love that kind of information
    - ▶ Not public profile. At least I think it is not (rules change)
    - ▶ Someone could have shared the photo with the world

# Awareness

## True stories - Store Credit

- ▶ Buying a book for almost no money
  - ▶ How I was able to get money just by having the right information
  - ▶ Store clerk asked for store customer card
  - ▶ Gave mobile number and full name
  - ▶ Store clerk asked if I wanted to use balance credit
  - ▶ I accepted and little had to pay
  - ▶ Mobile and full name were not mine 😊