

The background features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern and dynamic visual effect.

# OSINT

Cuidado, eu sei quem tu és e onde moras!

CDAYS - 2024

# \$whoami

- ▶ Pedro Vieira
- ▶ Engenheiro de Cibersegurança
- ▶ Certified Ethical Hacker
- ▶ Licenciado pela Universidade do Minho



# Aviso Legal & Leis

# Aviso Legal

## Disclaimer - Aborrecido, mas necessário

- ▶ 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 diretamente relacionada** com o meu trabalho ou empregador.



# Aviso Legal

## Disclaimer - Evitem atividades ilegais

- ▶ 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

## Lei Portuguesa e Organizações

### ► Lei

- Diário República Eletrónico ([link](#))
- ANACOM ([link](#))

### ► Organizações

- CNCS - Centro Nacional de Cibersegurança ([link](#))
  - Notificação de Incidentes ([link](#))
  - CERT.PT ([link](#))
- Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) ([link](#))
- Ministério Público ([link](#))

# Consciencialização

# Consciencialização

## A internet sabe e não esquece

- ▶ Informação publicada em modo privado pode ser tornada pública por outra pessoa
- ▶ Quando a informação é publicada
  - ▶ Mostra onde e quando (hábitos e rotinas)
- ▶ A internet tem memória
  - ▶ Arquivo.pt ([link](#))
    - ▶ Exemplo ([link](#)) ➡
  - ▶ Internet Archive - Wayback Machine ([link](#))
    - ▶ Exemplo ([link](#)) ➡



# Consciencialização

## Perfil

- ▶ Telefone/Telemóvel (Longevidade do mesmo número)
  - ▶ Sync.Me ([link](#))
- ▶ Username
  - ▶ WhatsMyName ([link](#)) ➡
- ▶ Email (Reutilização do mesmo username)
  - ▶ Gmail ([link](#))
- ▶ Redes Sociais (Reutilização do mesmo username)
  - ▶ Facebook ([link](#))
  - ▶ LinkedIn ([link](#))
  - ▶ Tinder ([link](#)) ([link](#)) ➡

# Consciencialização

## Mapas

- ▶ Nunca lá estive, mas conheço como a palma da minha mão.
- ▶ Vista de estrada
  - ▶ Google Street View ([link](#)) ➡
- ▶ Mapa/ Vista de Satélite
  - ▶ Google Maps ([link](#))
  - ▶ Overpass Turbo ([link](#)) ➡
    - ▶ Wizard: plant:source=nuclear
  - ▶ World Imagery Wayback example ([link](#)) ➡
- ▶ Tips, Tricks and Techniques ([link](#))

# Consciencialização

## Fotografias

- ▶ Análise da fotografia
  - ▶ Localização
  - ▶ Data em que foi tirada
  - ▶ Elementos identificativos na imagem
- ▶ Pesquisa de imagem
  - ▶ Identificar o castelo ([link](#)) ➡



# Consciencialização

## Fotografias

- ▶ Uma imagem vale mais do que mil palavras.

- ▶ Análise do ficheiro

- ▶ Metadados
- ▶ GPS ([link](#)) →
- ▶ Google Maps ([link](#)) →


- ▶ Ferramentas

- ▶ CleanUp ([link](#))
- ▶ AperiSolve ([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	0 mm
Format	
Scene Capture Type	Standard
Gain Control	Low gain up
ISO	100
Compression	JPEG (old-style)

# Consciencialização

## Quando empresas são atacadas

► Quando as empresas são atacadas os dados privados são expostos. Passam a ser “públicos”.

► Troy Hunt

► HavelBeenPwned ([link](#)) ➡

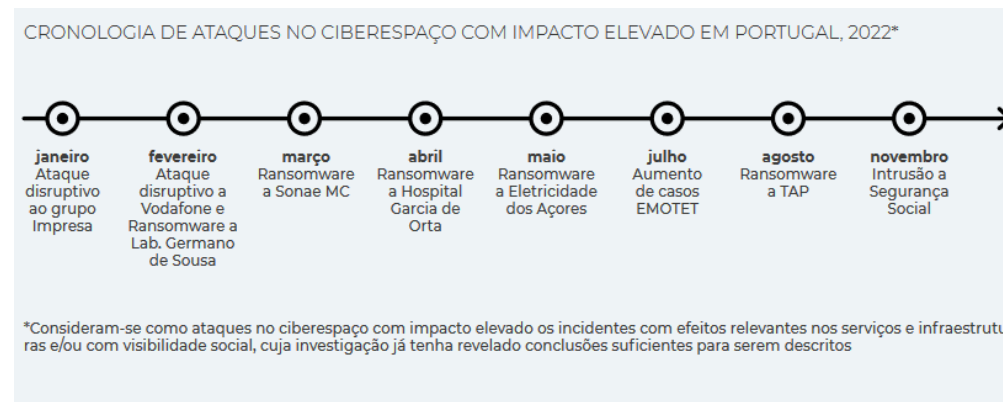
► Pwned websites ([link](#)) ➡

► Domain search ([link](#))

► Relatório CNCS

► Cibersegurança em Portugal 2024 ([link](#))

► Cibersegurança em Portugal 2023 ([link](#))



Fonte: CNCS

# Consciencialização

## Motores de busca para IOT

- ▶ Pastas partilhadas acessíveis a 8 mil milhões de pessoas ([link](#)) ➡

- ▶ Contabilidade - 6
- ▶ Clientes - 3
- ▶ Faturacao - 1
- ▶ Faturacao - 2
- ▶ Primavera - 6
- ▶ SAGE - 13
- ▶ Winrest - 148

Shares			Shares		
Name	Type	Comments	Name	Type	Comments
Web	Shares		ADMIN\$	Disk	Remote Admin
Public	Name	Type	C\$	Disk	Default Share
homes			IPC\$	Printer	
SCAN	Multimedia		IPC\$	IPC	
SERVER	Download	Shares			
Multimedia	Web	Name			
Recordings	Public				
home	homes	Multimedia			
MBPT	TESTE	Download			
PLOUTOS	JOAO	Web			
TGS	DUDA	Public			
MIRUS	SEGMENTO_POPULAR	homes			
USB	SOFTWARE	BackupR			
IPC\$	home	IPC\$			
	IPC\$				

Shares		
Name	Type	Comments
IPC\$	IPC	IPC Service ("")
Carlos	Disk	Carlos Pessoal
TTT	Disk	Todo Tipo Terre
SAIG	Disk	SAIG
Zonesoft	Disk	Clientes Zoneso
FTP	Disk	FTP
Clientes_Sage	Disk	Clientes Sage
Clientes_XD	Disk	Clientes XD
XD Extreme	Disk	XD Extreme
video	Disk	System default
photo	Disk	System default
music	Disk	System default
admin	Disk	...

# Tempo de OSINT

“Information is not knowledge”

Albert Einstein



# OSINT - Open-source intelligence

## Pegada Digital

- ▶ 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 conhecimento.
- ▶ Colecionar dados de:
  - ▶ motores de busca (Google, ...)
  - ▶ redes sociais (Facebook, ...)
  - ▶ sites governamentais
  - ▶ mapas
  - ▶ ...
- ▶ E depois extrair/relacionar/inferir nova informação com maior valor/potencial.



# Quem sou eu?

## Pesquisar, e voltar a pesquisar

- ▶ Começando apenas com um nome
  - ▶ Pedro António Oliveira Vieira
- ▶ Google ([link](#)) ➡
- ▶ Google “Improved Search” ([link](#)) ➡
- ▶ Google “Improved Search” + empresa ([link](#)) ➡
- ▶ LinkedIn ([link](#)) ➡
  - ▶ Perfil público estava a expor demasiada informação
- ▶ Certified Ethical Hacker ([link](#))
- ▶ As minhas notas no github ([link](#))



# Motores de Busca

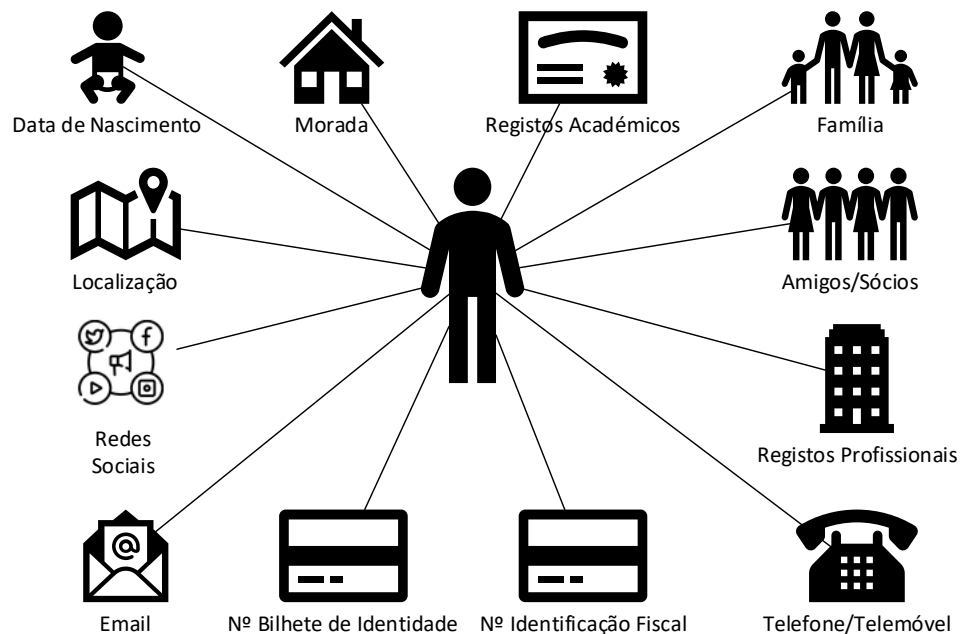
## A internet é mais do que o Google

- ▶ Motores de busca diferentes → regras/crawlers diferentes → resultados diferentes
- ▶ Google ([link](#))
- ▶ Bing ([link](#)) ➡
- ▶ Yahoo ([link](#))
- ▶ DuckDuckGo ([link](#)) ➡
- ▶ Baidu (China) ([link](#))
- ▶ Yandex (Russia) ([link](#))
- ▶ SAPO (Portugal) ([link](#)) ➡
- ▶ Podem pedir para serem removidos de um motor de busca, mas não de todos ☹ ([link](#))

# Quem és tu?

## Pesquisar, e voltar a pesquisar

- ▶ Pesquisem o vosso nome e analisem os resultados
  - ▶ Como viram a pesquisa pode ser melhorada



- ▶ Tipicamente esta informação permite **validar a identidade** numa chamada telefónica.

# Histórias verídicas

# Histórias verídicas

## Portugal

### Crédito de loja

- Como comprar um livro quase sem precisar de dinheiro
- Cartão de cliente de loja
- Informação certa: número de telemóvel e nome completo
- Crédito no cartão

### Dados de clientes

- Pedido de fatura com NIF
  - Nome
  - Morada
- Atualização de dados de cliente no balcão sem documentos

# Histórias verídicas

## Mensagem da Ella do futuro



Deutsche Telekom  
Message from Ella | Without Consent

# OBRIGADO

## Q&A