# CliqueAqui_ ParaPerder



Ingra Barreto

1,º PRÉMIO ARQUIVO.PT 2026

“solicitavam, em nome da [redacted], que os clientes enviassem a sua identificação e respectiva **«password»**.”

“caso não fornecessem […], a sua conta seria cancelada.”

# Daria a sua password?_

## DARIA A SUA PASSWORD?

**CASO 2 – O IMPOSTOR DA REDE**

**captura de 5 out. 2000**



Utilizando indevidamente o nome da Telepac, alguns frequentadores dos canais de IRC da PT-net (a rede portuguesa de IRC) solicitavam, em nome da empresa, que os clientes enviassem a sua identificação e respectiva «password». Ameaçavam ainda que, caso não fornecessem os dados sigilosos que haviam sido pedidos, a sua conta seria cancelada. Este tipo de abordagem - desmascarado a tempo pela Telepac, que informou os seus clientes - não é mais do que um acto de pirataria informática, configurando um crime de burla. O caso, ocorrido no dia 23 de Junho, foi entregue à Polícia Judiciária e o alerta foi lançado: o «username» e a «password» são pessoais e intransmissíveis.

https://arquivo.pt/wayback/20001005055436/http://www.ciberfest.pt/telepac/net/5/4.html

**https://cliqueaquiparaperder.pt/bestiario.html#CASO_02**

# 358 casos

De burlas registadas pela Linha Internet Segura em 2025

# um aumento de 44%

Face a 2024

> “O crime que mais nos chega [...] mantém-se, são situações de burla”, apontou Carolina Soares, que somou 358 situações em 2025, um aumento de 44% face aos 247 do ano anterior. “Dentro da burla temos vários tipos de métodos”, sublinhou, a que se segue, em segundo lugar, a extorsão, com 167 situações, um aumento de 90% face a 2024 (88).

https://www.publico.pt/2026/02/10/sociedade/noticia/linha-internet-segura-casos-cibercrime-aumento-70-denuncias-conteudo-ilegal-2164258

ENQUADRAMENTO

# E se tratarmos a *burla* como um documento social?

O que se desejava

O que se temia

O que não se sabia reconhecer




O engano também é memória, e as burlas continuam a fazer vítimas

Consultas à API do Arquivo.pt e leitura manual

2000–2012

13 anos de internet portuguesa recolhidos num **Observatório** e num **Bestiário** com 100 casos

## PERGUNTA DE INVESTIGAÇÃO

Que padrões de fraude circularam na internet portuguesa entre 2000 e 2012, e quais persistem hoje?

# 32.245

**Páginas recuperadas do Arquivo.pt relacionadas com burlas**

*dados brutos

12 de fevereiro, 2005

https://arquivo.pt/wayback/20050704210658/http://www.lojistas.net/fl/viewtopic.php?t=140

**O Fantasma do Colégio**, caso #27 – Bestiário

| Autor | Mensagem |
|---|---|
| **WebMaster**<br>Administrador<br><br>Registrado em:<br>Sexta-Feira, 3 de Dezembro de 2004<br>Mensagens: 258 | Enviada: 12/02/05 13:38:15 — Responder com Citação |

## 1) Falso atalho em e-mail - Pessoal

IP 200.198.85.9. Neste endereço respondeu o site www.valorservicos.com.br

Veja como saber o remetente do e-mail

Recebemos este e-mail que estamos divulgando para a informação dos nossos leitores.
Previna-se!
Comunicamos ao responsável pelo IP.

O texto do remetente contém um FALSO ATALHO. Quando você coloca o ponteiro do mouse sobre o atalho, SEM CLICAR, você vê, na última linha do MS Outlook Express, que o atalho verdadeiro é outro. Quando a vítima clica sobre o FALSO ATALHO é remetido para o VERDADEIRO ATALHO DO REMETENTE.

### E-mail com o FALSO ATALHO

Olá tudo bem ?

Meu nome é Rafael, e sem querer achei o seu email, meu amigo me disse que esse era o seu email, não tenho certeza se é você mesmo que estudou comigo no colégio e gostaria de fazer uma festa de reencontro do pessoal todo, seria legal reencontrar a turma toda, alguns morreram infelizmente, mas eu estou tentando entrar em contato com o maior numero de amigos possiveis daquela época, e estou te convidando para ir a esta festa, gostaria muito de reencontra-lo.

Para não haver engano eu tenho uma foto minha, se me reeconhecer por favor entre em contato, estou um pouco diferente desde aquela época, mas acho que da para se lembrar de min.

link da minha foto -> http://host940bnx.plugin.com.br/rafael.jpg

Se não for voce realmente, por favor desconsidere este email, e desculpe pelo incomodo.

Atenciosamente Rafael Dante.

# 21 ANOS DEPOIS

24 de junho, 2026



EM DESTAQUE

**24.06.26 - Campanha de phishing em nome da MEO**

4 meses atrás • Última edição: 4 meses atrás • 0 respostas • 152 visualizações

Vanessa_MEO Administrador • 1066 respostas

+26

O **CSIRT MEO** detetou que está em curso uma campanha de phishing/smishing utilizando a imagem corporativa da MEO.

Estão a ser enviados SMS em nome da MEO, com o seguinte texto:

> **MEO: O seu debito direto foi interrompido. Regularize os seus dados ate 25/06 para evitar interrupçoes no servico. Aceda a gestao-telecom.com. Obrigado"**



SMS malicioso

Ao clicar na ligação (gestão-telecom.pt) incluída no SMS é direcionado para um ***site*** que **não é da MEO**, onde é pedido que introduza:

1. As credenciais de acesso ao ID

https://forum.meo.pt/alertas-de-fraude-40/24-06-26-campanha-de-phishing-em-nome-da-meo-167454

A fraude não nasceu com a internet, mas encontrou nela um habitat fértil.
Embora os meios *mudem*, os mecanismos de engano *mantêm-se*,
pois continuam a explorar as *mesmas vulnerabilidades humanas*.

**200**
palavras-chave

**2.600**
consultas

à API pública
do Arquivo.pt

**23.498**
registos

ao longo de
13 anos

100 casos documentados individualmente,
reunidos num bestiário digital de burlas

32.245 páginas devolvidas pela API

23.498 páginas em domínios .pt: Observatório

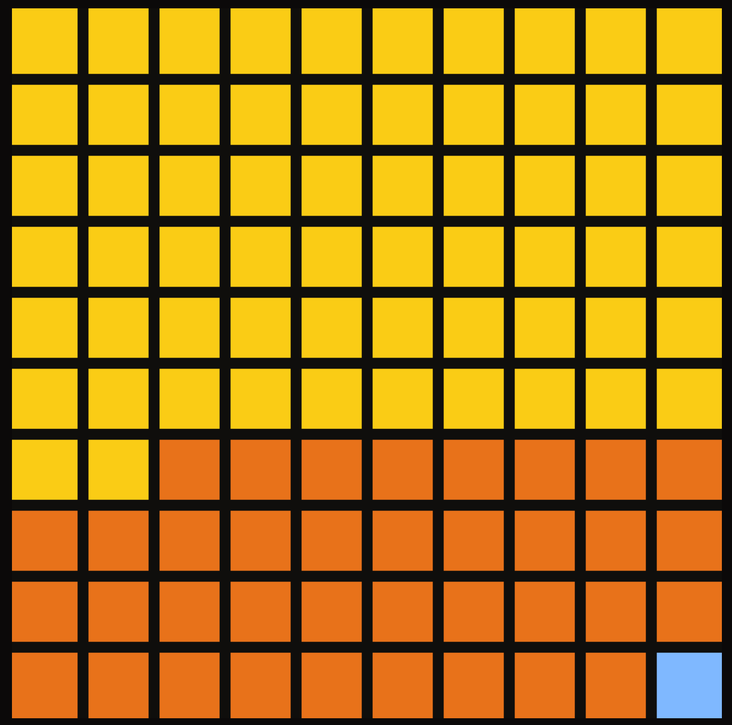
1.578 corpus para leitura manual

100 casos validados: Bestiário

200 palavras-chave × 13 anos = 2.600 consultas

## A API não bastou

# Nem tudo se encontra à primeira pesquisa



**62 casos**
do corpus da API

**37 casos**
pesquisa manual

**1 caso**
exceção paradigmática
“Thriller dos Dados”,
com domínio .br

# TAXONOMIA

## Classes



01/ Construtores



02/ Oráculos



03/ Pescadores



04/ Príncipes



05/ Mercadores

## Espécies

| | |
|---|---|
| /01 | ARMADILHA DE RECRUTAMENTO |
| /02 | BURLA TRANSACIONAL |
| /03 | CHARLATANISMO |
| /04 | ESQUEMA DE INVESTIMENTO |
| /05 | VISHING |
| /06 | EXTORSÃO |
| /07 | FALSO PRÉMIO |
| /08 | MALWARE |
| /09 | PHISHING |

O período de análise vai do colapso da bolha «dot-com», no início dos anos 2000, aos mil milhões de utilizadores do Facebook, em 2012. Começa numa internet mais dispersa e termina numa internet mais centralizada.

## COMO ERA ESTA «INTERNET DE ANTES»?

Uma internet ingénua, artesanal, *menos centralizada.*




https://arquivo.pt/wayback/20030111223852/http://www.terravista.pt:80/portosanto/3785/default.htm




https://arquivo.pt/wayback/20000816063853/https://bvi.clix.pt/




https://arquivo.pt/wayback/19980109034046/http://supragw.supra.pt/futuro.htm

## “PHISHING” ENTRA NO CORPUS EM 2003

# A prática chega antes da palavra

a prática

**2000**

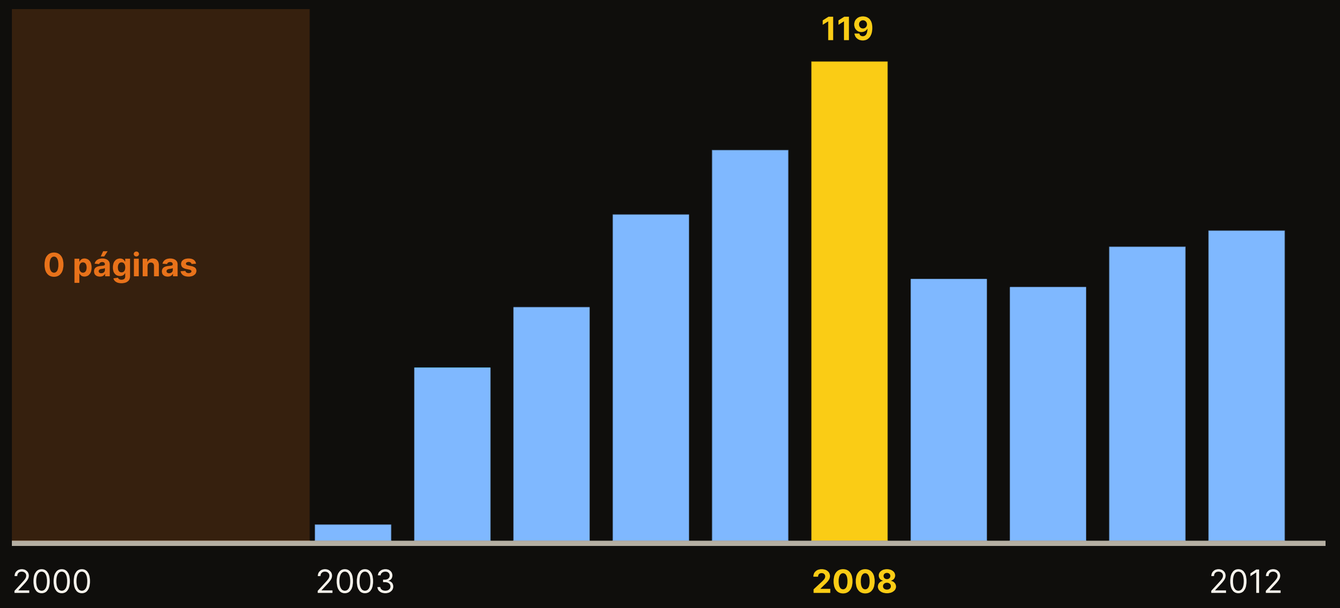
↓

**3 anos sem nome**

**2003**

a palavra

Páginas .pt que mencionam “phishing”, por ano de captura




Fonte: corpus .pt do projeto (título e excerto); primeira ocorrência neste corpus, 13 out. 2003.

COMO LER OS DADOS

 Vestígios, não incidência da fraude

 Cobertura desigual do arquivo

 .pt não é toda a internet portuguesa

**PRÓXIMOS PASSOS**

# Levar os casos do arquivo para a sala de aula, num jogo de investigação com burlas reais.

Analisar um caso real | Desmontar o “truque” | Verificar a fonte

---

**Está previsto um piloto em março de 2027 para o 3.º ciclo.**

# VAMOS DAR UMA VISTA DE OLHOS NA PÁGINA?

cliqueaquiparaperder.pt

Não reconhecemos
o que não guardámos.




_isto é para todos

# Perguntas?

Porque arquivar a web é também arquivar
a forma como aprendemos a confiar,
a clicar e a perder.

Ingra Gonçalves Barreto
github.com/barretoingra/clique-aqui-para-perder
info@cliqueaquiparaperder.pt
cliqueaquiparaperder.pt

CliqueAqui_
ParaPerder