Identificação

Título: cliqueaquiparaperder.pt

Área temática: História Digital / Literacia Digital / Cibersegurança

Candidata: Ingra Gonçalves Barreto

E-mail: barretoingra.17@gmail.com

Descrição do Trabalho

Clique Aqui Para Perder é um projeto de investigação histórica publicado em https://cliqueaquiparaperder.pt, que resgata, classifica e analisa as primeiras burlas e esquemas que circularam na internet portuguesa entre 2000–2012. O horizonte temporal vai do colapso da bolha «dot.com», em março de 2000, ao momento em que o Facebook atingiu os mil milhões de utilizadores, em setembro de 2012: transição de uma internet experimental para uma internet comercial e o momento em que a fraude digital em língua portuguesa ganhou forma e escala. O Arquivo.pt é a fonte primária insubstituível, sem a qual fóruns extintos, notícias arquivadas, os textos e as denúncias das fraudes seriam irrecuperáveis.

O projeto materializa-se em quatro componentes articulados por uma taxonomia simplificada autoral: cinco classes que agrupam as burlas pela promessa central à vítima e nove espécies que descrevem o mecanismo operativo concreto.

(1) O Bestiário: 100 casos em fichas normalizadas com estrutura invariante, cada uma com excerto literal do Arquivo.pt, captura de ecrã e URL verificável, garantindo rastreabilidade e replicabilidade. O formato bestiário, tradição presente em língua portuguesa desde o «Livro das Aves» (séc. XII) e retomada por Jorge Luis Borges no «O Livro dos Seres Imaginários», trata cada burla como uma criatura classificada, tornando os padrões de manipulação reconhecíveis e transferíveis para o presente.

(2) O Observatório analisa 23.498 registos em domínios (.pt), extraídos de um corpus bruto de 32.245 registos obtidos através de 2.600 consultas à API do Arquivo.pt (200 palavras-chave × 13 anos), após remoção de duplicados e filtros de qualidade documentados.

(3) O Glossário reúne 86 termos especializados em linguagem acessível ao cidadão comum.

(4) Os Recursos de Literacia Digital incluem um guia de resposta a fraude por tipo de incidente, ferramentas de verificação e formações gratuitas em português.

Objetivos

Preservar e tornar acessível a memória histórica da fraude digital na internet portuguesa entre 2000–2012, através de metodologia documentada, como contributo científico e ferramenta de literacia digital cidadã.

1) Documentar 100 casos em fichas normalizadas com estrutura invariante, critérios de inclusão e exclusão explícitos e ligação direta ao URL no Arquivo.pt, garantindo que a memória preservada seja rastreável, verificável e replicável.
2) Mapear dinâmicas linguísticas e de volume entre 2000–2012, identificando anos de maior incidência e correlacionando a evolução da linguagem de manipulação com momentos de transformação tecnológica.
3) Democratizar o acesso à literacia digital preventiva através de um arquivo que transforma a memória histórica da fraude numa ferramenta de defesa cidadã, transferível para o reconhecimento de esquemas de engenharia social contemporâneos.

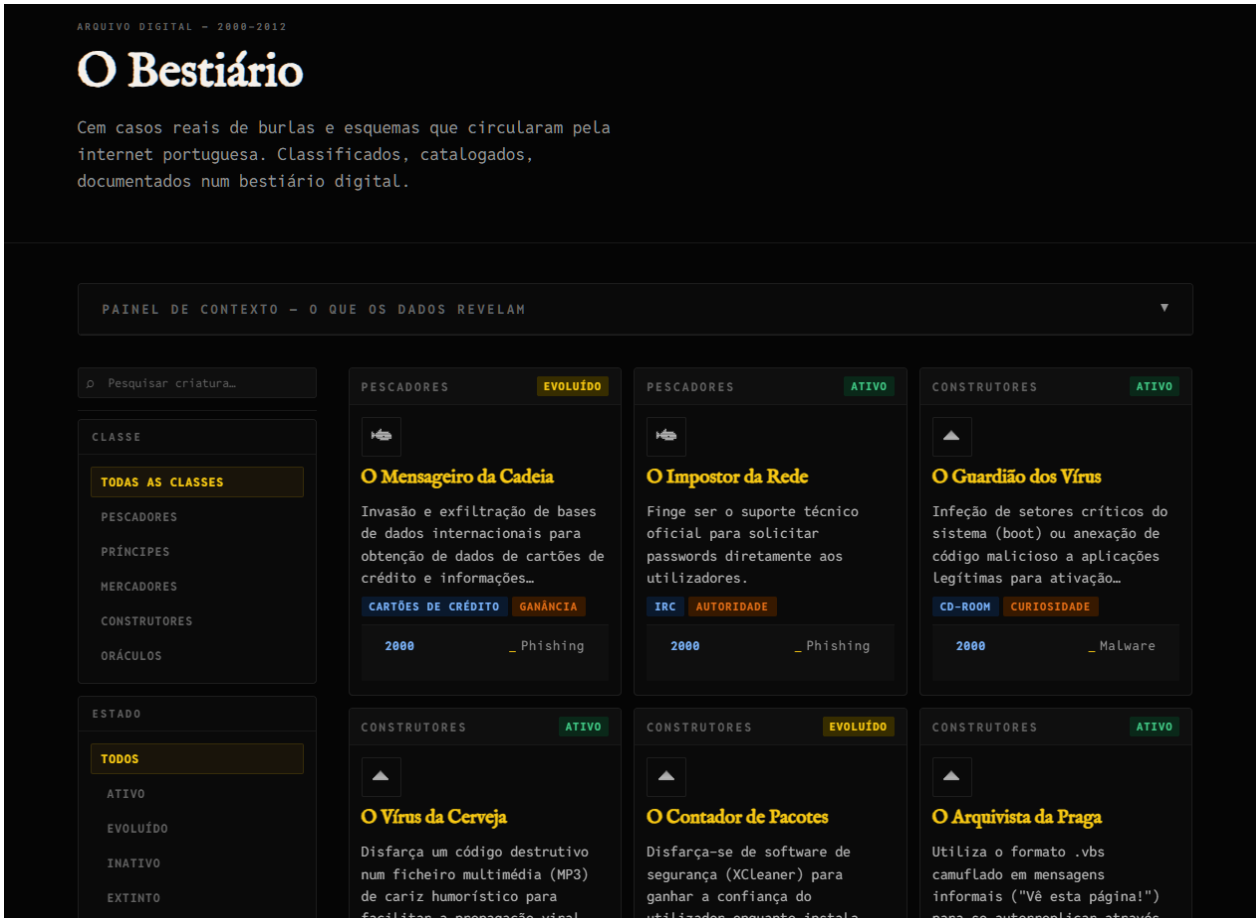
Resultados Atingidos

O Bestiário é um corpus de 100 casos de fraude digital recuperados do Arquivo.pt: 99 em domínios portugueses e um brasileiro (caso paradigmático *"O Thriller de Dados"*), selecionados de um universo de 32.245 registos brutos reduzido a 1.578 após filtros automáticos documentados, por amostragem intencional com critérios explícitos de cobertura temporal, tipológica e de qualidade do excerto. Cada caso é inscrito numa ficha com os seguintes campos obrigatórios:

Nome da criatura	Nomenclatura lúdica baseada na burla (até 3 palavras, estilo RPG de mesa)
Data de captura	*Timestamp* do Arquivo.pt
Tipo de fonte	Jornal / Fórum / Blogue / Marketplace / Classificado / Site institucional / Site da fraude / PDF

Classes	Mercadores / Construtores / Oráculos / Príncipes / Pescadores
Espécies	Armadilha de recrutamento / Phishing / Vishing / Esquema de Investimento / Burla Transacional / Extorsão / Falso prémio / Charlatanismo / Malware
Habitat tecnológico	E-mail / SMS / Ligação / Homebanking / Fóruns / Marketplaces
Gatilho psicológico	Ganância / Urgência / Medo / Autoridade / Pertença / Curiosidade / Reciprocidade / Escassez
Comportamento	Como se apresenta a burla
Excerto literal	Transcrição direta da fonte, sem edição
Estado atual	Ativo / Evoluído / Inativo / Extinto
URL Arquivo.pt	Link direto para a página arquivada
Captura de ecrã	Captura da página

A estrutura invariante garante replicabilidade: qualquer investigador que siga os mesmos critérios obtém fichas comparáveis.



Por dentro do Bestiário

A taxonomia é autoral e organiza-se em dois níveis complementares:

O primeiro nível é a **classe**, definida pela promessa central que a burla faz à vítima. Responde à pergunta: o que é esta burla na sua essência? É o nível mais estável da taxonomia: a mesma classe pode ocorrer em períodos e plataformas distintas.

Dessa sistematização surgem **cinco classes** principais de fraude:

Mercadores	Esquemas de ganho rápido: SMS fraudulentos, correntes de dinheiro, burla transacional
Construtores	Software malicioso distribuído por ficheiros, links ou downloads

Oráculos	Vidência, cura e guias espirituais que exploram medo ou fé para pagamentos
Príncipes	Heranças bloqueadas, inclui variantes lusófonas e simulação de autoridades como PSP e tribunais
Pescadores	Simulação de bancos e instituições para captar credenciais; inclui páginas clonadas de homebanking

O segundo nível é a **espécie**, que descreve o mecanismo operativo concreto. Responde à pergunta: como é que este esquema opera? A classificação segue a promessa dominante percebida pela vítima (voz da "denúncia") ou através do anúncio do burlão, documentada no excerto literal.

Dessa sistematização surgem **nove espécies** correspondentes aos mecanismos operacionais identificados:

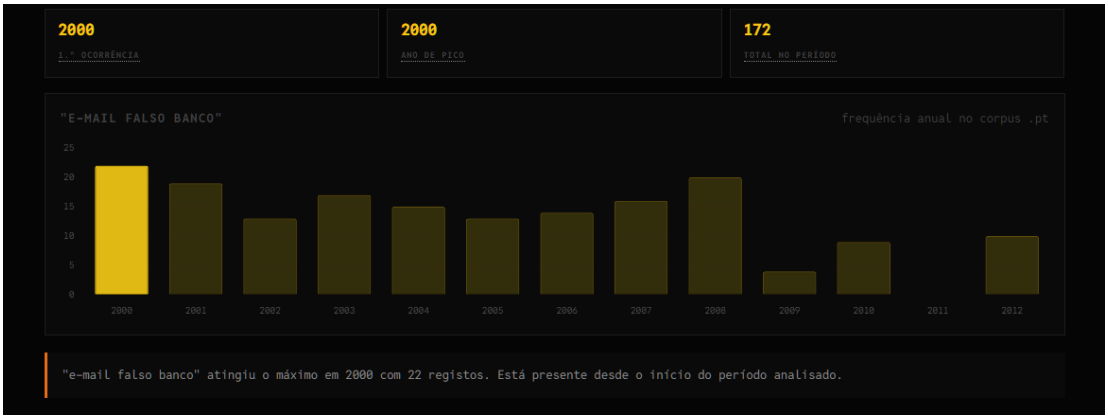
Armadilha de recrutamento	Oferta falsa de emprego ou oportunidade, usada para captar dados ou pagamentos antecipados
Burla transacional	Simulação de transação legítima sem intenção de cumprir
Charlatanismo	Cobrança por capacidades não verificáveis: vidência, cura, proteção espiritual
Esquema de investimento	Promessa de retorno acima do mercado mediante entrega de capital; inclui pirâmides
Extorsão	Pagamento exigido sob ameaça de exposição, dano ou bloqueio de acesso
Falso prémio	Ganho fictício condicionado a ação prévia; o prémio nunca existe

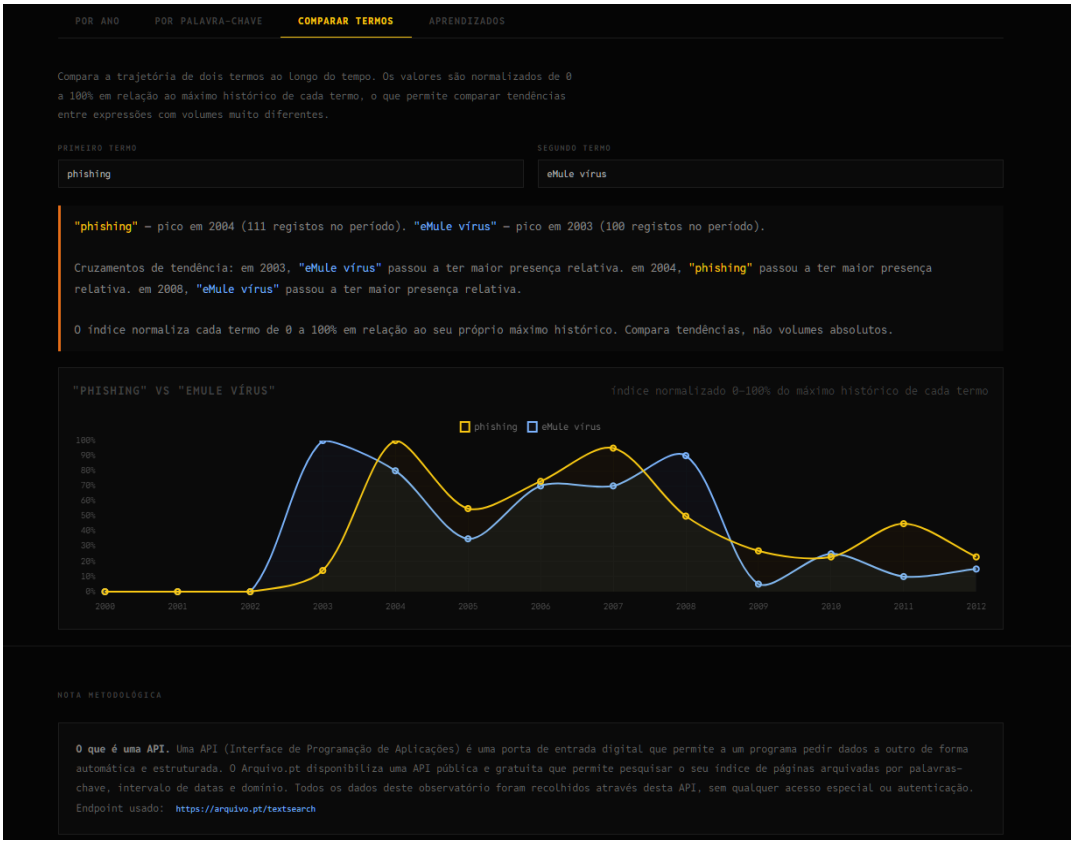
Malware	Software malicioso instalado no dispositivo do alvo
Phishing	Simulação de entidade legítima para obter credenciais ou acesso a contas
Vishing	Chamada telefónica fraudulenta simulando banco, seguradora ou serviço público

O Observatório é o componente analítico de larga escala do projeto. Foram executadas **2.600 consultas à API do Arquivo.pt** (200 palavras-chave × 13 anos). O corpus real obtido foi de **23.498 registos validados** em domínios (.pt), após aplicação de critérios de inclusão e exclusão documentados: relevância temática, integridade dos metadados, contexto verificável e restrição a domínios portugueses. A cobertura temporal é desigual por razões estruturais do próprio arquivo: o período 2000–2003 apresenta densidade de indexação inferior ao período 2008–2012.

O Observatório produz dois tipos de análises:

1) Quantitativa: gráficos de volume por ano e por termo, com identificação de picos de atividade (2007 como ano de maior volume no corpus do Observatório; 2009 como o ano com mais casos curados no Bestiário, métricas distintas que se complementam).
2) Qualitativa: painéis interativos por ano, por palavra-chave e por comparação de termos, que rastreiam a mutação terminológica.





Por dentro do Observatório

Originalidade e caráter inovador

Não existe em Portugal nenhum projeto que combine, num único ecossistema, arquivo histórico de fraude digital, taxonomia autoral, análise linguística de larga escala por via de API e formato de mediação pública acessível a públicos não especializados.

Os contributos inovadores são três:
(1) o uso sistemático do Arquivo.pt como fonte primária de investigação histórica sobre fraude digital, num período em que esse conteúdo não existe em nenhum outro repositório acessível.
(2) uma taxonomia autoral de dois níveis que separa o que a burla é, definido pela promessa que faz à vítima, de como opera, descrito pelo mecanismo concreto, permitindo comparar casos de épocas e canais diferentes. A escolha de dois níveis é intencional: num corpus de 100 casos, mais granularidade criaria categorias com representação insuficiente para análise.
3) a escolha do bestiário como dispositivo de mediação deliberado, não apenas como formato, mas como estratégia de acesso: cada nomenclatura é uma chave de reconhecimento. A forma lúdica não concede ao rigor, é a condição para que o corpus chegue a quem mais precisa dele.

Impacto social (aplicação e utilidade social)

A ANACOM (2024) documenta que apenas 29,9% da população portuguesa entre 16 e 74 anos apresenta literacia digital acima do nível básico e que 14,2% não utiliza a internet, colocando Portugal no 4.º lugar da UE27 na taxa de não utilização, por falta de competências digitais. A maioria das campanhas de sensibilização responde com instrução direta. Este projeto busca responder com memória histórica documentada: expõe a anatomia de burlas reais, os seus gatilhos psicológicos e sequências de manipulação, construindo uma capacidade de reconhecimento transferível para o presente.

Os padrões identificados entre 2000–2012 persistem com mutações de canal, não de lógica. O Gabinete Cibercrime da Procuradoria-Geral da República alertou em março de 2025 para esquemas de investimento em criptomoedas que replicam os esquemas de pirâmide a partir de 2003: promessa de rentabilidade elevada, captação por anúncio, taxas fictícias para levantar ganhos inexistentes.

O CNCS documenta que phishing foi considerado a ameaça mais relevante por 84% dos profissionais de cibersegurança em Portugal em 2024, tipologia presente no corpus deste projeto desde 2000. A PSP (2026) documenta aumento de burlas em plataformas de compra e venda online, variante direta das burlas transacionais em classificados portugueses desde 2001 (mais evidente a partir de 2008). O mecanismo é o mesmo. Quem reconhece o padrão histórico está preparado para o identificar na sua forma atual.

Impacto científico (aplicação e utilidade científica)

O projeto disponibiliza três recursos para investigadores:
(1) um corpus de 100 casos com estrutura invariante, excertos originais, capturas de ecrã e URLs verificáveis no Arquivo.pt, cobrindo um período sem equivalente disponível publicamente em português.
(2) os registos completos das 2.600 consultas à API do Arquivo.pt, com critérios de inclusão e exclusão documentados, permitem que qualquer investigador reproduza o processo e aplique o mesmo método a outros fenómenos no arquivo.
(3) o mapeamento de como a linguagem da fraude evoluiu entre 2000-2012, em paralelo com a adoção de novas plataformas tecnológicas, constitui um recurso para estudos de linguística, criminologia digital e história da internet em português.

Relevância da utilização do Arquivo.pt

O Arquivo.pt não é um recurso auxiliar neste projeto: é a condição da sua existência. A maioria dos conteúdos analisados, fóruns de discussão, plataformas de classificados, páginas pessoais, alertas de consumidores, desapareceu da web acessível. Sem o Arquivo.pt, esses registos seriam irrecuperáveis por qualquer outro meio.

A dependência é concreta e documentável. O corpus inclui, entre outros: um alerta dos anos 2000 sobre pedidos fraudulentos de passwords em canais de IRC em nome da Telepac (***O Impostor da Rede***, **CASO_02**), página extinta sem qualquer outro registo online; anúncios de classificados do SAPO de 2003 com propostas de esquemas de pirâmide financeira ***(O Grão-Mestre da Pirâmide, CASO_10)***; e uma notícia de jornal regional de 2001 sobre burla na compra de equipamento informático via internet (***A Coletora de Contos***, **CASO_08**), cujo arquivo digital próprio não mantém cobertura desse período. Em todos estes casos, o URL do Arquivo.pt é o único ponto de acesso verificável ao documento original. É essa unicidade que torna o Arquivo.pt insubstituível e que justifica a centralidade da utilização neste projeto.

Comentários adicionais

O projeto está disponível online https://cliqueaquiparaperder.pt e é integralmente acessível ao público, sem registo ou *paywall*. Toda a metodologia, incluindo os critérios de inclusão e exclusão do corpus, o script de extração e os dados completos das 2.600 consultas à API do Arquivo.pt, está disponível em repositório público: github.com/barretoingra/clique-aqui-para-perder,permitindo o escrutínio e replicação por qualquer investigador. Este trabalho é também uma demonstração prática do que se pode construir com infraestrutura de arquivo aberto.

Recursos complementares

ANACOM (2024). Competências digitais da população e das empresas 2024: https://www.anacom.pt/streaming/Competencias_digitais_populacao_e_empresas_2024.pdf?contentId=1801487&field=ATTACHED_FILE: indicadores de literacia digital da população portuguesa por área, incluindo segurança digital.

Arquivo.pt. API pública. https://arquivo.pt/api: infraestrutura de dados primária do projeto; permite pesquisa full-text em páginas arquivadas da web portuguesa entre 2000-2012.

Centro Nacional de Cibersegurança (2024). Relatório de Cibersegurança: Riscos e Conflitos 2024, https://www.cncs.gov.pt: demonstra a persistência das tipologias de fraude no panorama atual.

Cialdini, R. B. (1984). Influência: a psicologia da persuasão. Harper Collins, https://www.harpercollins.com: base teórica para os gatilhos psicológicos identificados e classificados em cada caso do bestiário.

Diário de Notícias (abril 2026), https://www.dnoticias.pt/2026/4/8/487582-psp-alerta-para-aumento-de-burlas-na-compra-e-venda-online: notícia sobre alerta da PSP para o aumento de burlas em plataformas de compra e venda online.

Filipe Adão Gomes (2023). A Digitalização no Setor Bancário e a Satisfação dos Usuários no Ambiente Digital: https://repositorium.uminho.pt/server/api/core/bitstreams/e2654a39-87c8-448f-a48b-1c91079c9259/content.

Gabinete Cibercrime, Procuradoria-Geral da República (2025). https://cibercrime.ministeriopublico.pt/sites/default/files/editor-files/2025.03.25-alerta-burlas-cripto.pdf**:** alerta oficial sobre esquemas fraudulentos de investimento em criptomoedas.

Livro das Aves (séc. XII), Mosteiro do Lorvão. Arquivo Nacional da Torre do Tombo. Disponível em: https://digitarq.arquivos.pt/documentDetails/c72e54ef34e74aceb8ded52aad827b37: Manuscrito didático em latim que utiliza descrições de aves e animais para transmitir lições morais.

Polícia Judiciária. Alertas públicos sobre fraude, https://www.policiajudiciaria.pt/alertas-2: verificação da recorrência dos padrões históricos identificados no corpus em contexto contemporâneo.