



WORKSHOP – CIBERSEGURANÇA E A SUA CRITICIDADE EM EMPRESAS E CIDADÃOS



INSTITUTO DO EMPREGO
E FORMAÇÃO PROFISSIONAL

STARTUP
PORTUGAL

- <https://twitter.com/MiguelSantareno>
- <https://www.linkedin.com/in/miguelsantareno/>
- <https://miguelsantareno.github.io/>
- miguel.santareno@my.istec.pt

RECEPÇÃO E CONTEXTUALIZAÇÃO

Cibersegurança é a prática de proteger sistemas, redes, dispositivos e dados de ataques digitais maliciosos. O seu objetivo é proteger informações pessoais, financeiras e empresariais contra ameaças como hacking, malware e acesso não autorizado, utilizando tecnologias, processos e melhores práticas. [🔗](#)

INFOSEC (INFORMATION SECURITY)

A segurança da informação protege informações sensíveis contra atividades não autorizadas, incluindo inspeção, modificação, gravação e qualquer interrupção ou destruição. O objetivo é garantir a segurança e a privacidade de dados críticos, como detalhes de contas de clientes, dados financeiros ou propriedade intelectual.

<https://www.imperva.com/learn/data-security/information-security-infosec/>

CIA TRIANGLE



CIBERSEGURANÇA COMO ATIVO ESTRATÉGICO

- Aplicações de terceiros
- Redes e sistemas
- Firewalls
- Telemóveis
- Impressoras
- Resumindo em tudo ligado à internet e mesmo na vida pessoal (exemplo engenharia social)

TOP 5 CIBERAMEAÇAS MAIS RELEVANTES



<https://www.cncs.gov.pt/docs/rel-riscosconflitos2025-obciberencncs.pdf>


PHISHING E SMISHING

O QUE SÃO

O phishing é um tipo de ataque em que se usam técnicas de engenharia social para capturar informação sensível de uma vítima através de *email*. Um agente de ameaça que utilize este tipo de ataque procura enganar os recetores de *emails* para que estes disponibilizem informação sensível através do clique em anexos e/ou URL maliciosos ou da partilha de dados em páginas fraudulentas. Para o efeito, o atacante simula uma marca credível ou personifica alguém de confiança. Quando esta técnica é utilizada através de SMS, dá pelo nome de smishing e, por telefone (voz), de vishing. Esta técnica também pode ser usada através de mensagens instantâneas em aplicações de redes sociais.

<https://www.cncs.gov.pt/pt/boas-praticas-contr-o-phishing-o-smishing-e-o-vishing/#oquesao>

PHISHING E SMISHING

- **2021:** Phishing/smishing representaram 40% dos incidentes registados pelo CERT.PT, sendo o tipo de incidente mais comum.
- **2020:** Subiram para 43% dos incidentes registados pelo CERT.PT, com um aumento absoluto de 160% em relação a 2019, impulsionado pela pandemia de COVID-19.
- **2024:** Continuaram a ser os ataques mais comuns, com um aumento de 13% face a 2023, segundo o [Público](#). 

RANSOMWARE

1. Enquadramento

Verifica-se uma tendência de crescimento dos casos de ransomware a afetar organizações no país. O ransomware é um tipo de software malicioso que, depois de instalado nos sistemas das vítimas, furta e/ou cifra dados considerados relevantes, tornando este sistema inoperacional.

De seguida, os atacantes exigem um resgate, normalmente em criptomoedas, em troca da chave que decifra estes dados. Os criminosos ameaçam a vítima com a perda desses dados ou com a sua divulgação ao público no caso do valor exigido não ser pago. Este tipo de ataques pode ocorrer de forma indiscriminada ou dirigida a vítimas de elevado valor económico.

Para proteger uma organização deste tipo de ameaça é importante conhecer o contexto e as ações de mitigação. O Centro Nacional de Cibersegurança (CNCS) chama a atenção para as seguintes metodologias de ataque e boas práticas de prevenção associadas.

<https://www.cncs.gov.pt/pt/contexto-atual-ransomware/#enquadramento2>

RANSOMWARE

Ataques de 'ransomware' em Portugal dispararam 250% no primeiro semestre

Os ciberataques concentram-se, sobretudo, no setor industrial, indica um estudo do grupo Thales. Nos primeiros seis meses do ano registaram-se 14 ataques.

Sónia Santos Pereira

Publicado a: 22 Out 2025, 12:26

Atualizado a: 22 Out 2025, 12:26

<https://www.dn.pt/economia/ataques-de-ransomware-em-portugal-dispararam-250-no-primeiro-semester>

EXPLORAÇÃO DE VULNERABILIDADES

Known Exploited Vulnerabilities Catalog



For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

EXPLORAÇÃO DE VULNERABILIDADES

GRAFANA LABS | GRAFANA

 [CVE-2021-43798](#) 

Grafana Path Traversal Vulnerability: *Grafana contains a path traversal vulnerability that could allow access to local files.*

Related CWE: [CWE-22](#) 

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

■ **Date Added:** 2025-10-09

■ **Due Date:** 2025-10-30

[Additional Notes +](#)

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog?page=1>

NEGAÇÃO DE SERVIÇOS DISTRIBUIDA (DDoS)

O que é o DDoS?

É um ataque distribuído de negação de serviço (DDoS), uma forma maliciosa de interromper o tráfego de um servidor, serviço ou rede, através da sobrecarga do mesmo.

<http://cncs.gov.pt/pt/intercop-ddos/>

NEGAÇÃO DE SERVIÇOS DISTRIBUIDA (DDOS)

7.3 terabits per second

In mid-May 2025, Cloudflare blocked the largest DDoS attack ever recorded: a staggering **7.3 terabits per second** (Tbps). This comes shortly after the publication of our DDoS threat report for 2025 Q1 on April 27, 2025, where we highlighted attacks reaching 6.5 Tbps and 4.8 billion packets per second (pps). 19/06/2025

AMEAÇA CRESCENTE 2025 – INFO STEALERS

Centro Nacional de Cibersegurança alerta para ameaça de roubo de dados sensíveis

O Centro Nacional de Cibersegurança (CNCS) alertou para a ameaça crescente dos `infostealers`, que roubam dados sensíveis, e apelou para a implementação de medidas preventivas, segundo um comunicado hoje divulgado.

Lusa / 4 Novembro 2025, 20:03

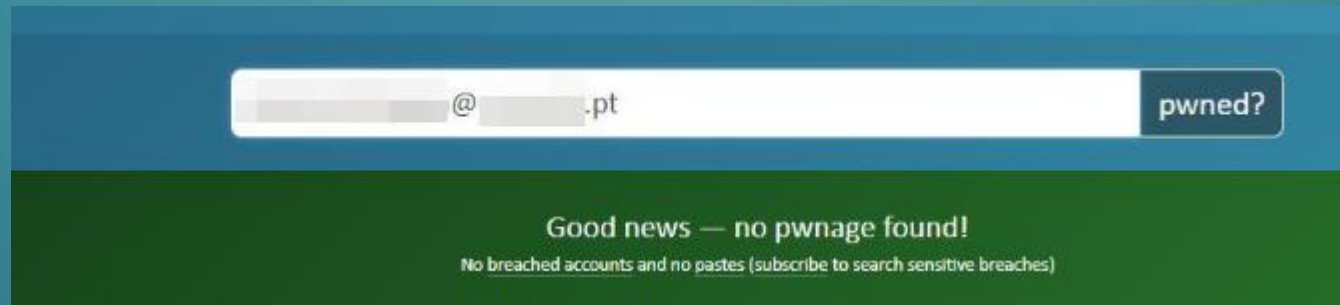
AMEAÇA CRESCENTE 2025 – INFO STEALERS

Os *infostealers* são um tipo de código malicioso desenvolvido para recolher dados sensíveis em dispositivos informáticos (p. ex. computadores, telemóveis), incluindo credenciais de acesso a contas pessoais ou profissionais (p. ex. credenciais de acesso a serviços de *homebanking*, serviços de governo eletrónico ou mesmo credenciais de acesso a contas profissionais), dados armazenados nos *browsers* (p. ex. *cookies*, *tokens*, histórico de navegação do utilizador), mas também *emails* e outros documentos.

Este tipo de código malicioso representa um desafio considerável, pois a sua utilização reduz significativamente o custo inicial de intrusão na infraestrutura da vítima para posterior realização de ataques mais rentáveis para o criminoso, como por exemplo o *ransomware*. Uma vez obtidas as credenciais de acesso a uma conta de uma potencial vítima, os atacantes não necessitam de utilizar outras metodologias de ataque, mais complexas ou morosas, para obterem o acesso inicial a um sistema.

Esta crescente ameaça é suportada por um vasto ecossistema comercial composto por fóruns *online* que operam como mercados. Aqui encontramos atores criminosos a venderem o acesso aos dados recolhidos por estes *infostealers* (*Malware-as-a-service*), bem como atores criminosos a curarem e venderem na *darkweb* os dados recolhidos por este *malware*.

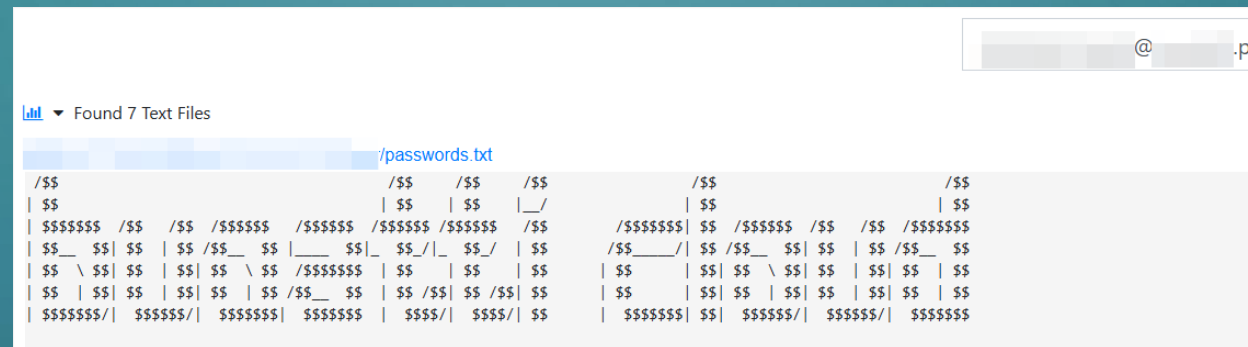
?AM I SAFE?



A screenshot of the Have I Been Pwned website interface. At the top, there is a search bar with a light blue background. Inside the search bar, the text "@.pt" is visible. To the right of the search bar is a button labeled "pwned?". Below the search bar is a green banner with white text that reads "Good news — no pwnage found!". Underneath the banner, in smaller white text, it says "No [breached accounts](#) and no [pastes](#) ([subscribe](#) to search sensitive breaches)".

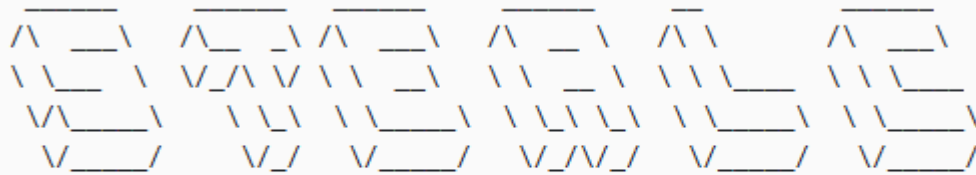
<https://haveibeenpwned.com/>

?AM I SAFE?



<https://intelx.io/>

?AM I SAFE?



stealc stealer

powerful native stealer based on C lang

<https://intelx.io/>

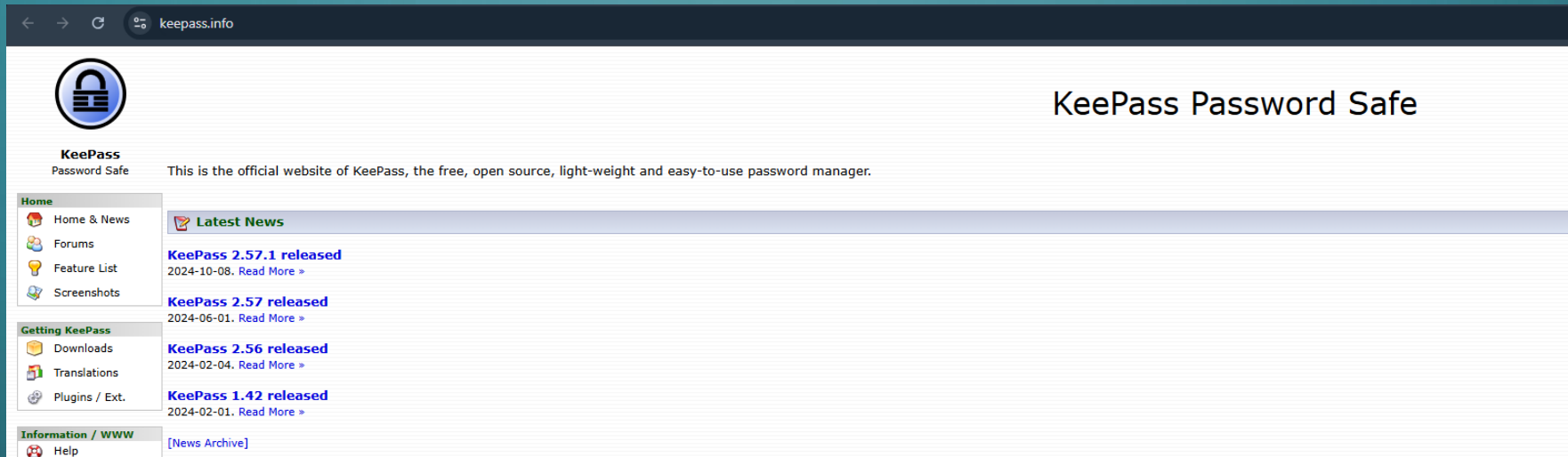
MEDIDAS BÁSICAS DE PROTEÇÃO E BOAS PRÁTICAS DE SEGURANÇA DIGITAL



PASSWORD MANAGERS

- <https://keepass.info/>
- <https://1password.com/>
- <https://bitwarden.com/>
- Among others.

KEEPASS









<https://keepass.info/>

1PASSWORD

Escolha um plano

☒ Anual ☐ Mensal EUR

Todos os planos **Business** **Pessoal**

 Individual Assuma o controle da sua segurança online. €2.65 EUR <small>por mês. Pago anualmente.</small> Experimente GRÁTIS por 14 dias <ul style="list-style-type: none">Gerador de senhasPreenchimento automático de login e compartilhamentoUse em todos os seus dispositivosVerificador de violação de segurança Watchtower <small>• Suporta iOS e 34 horas por dia 7</small>	 Famílias Paz de espírito para toda a sua família. €4.75 EUR <small>por mês. Pago anualmente.</small> Experimente GRÁTIS por 14 dias <p>Tudo do plano individual mais:</p> <ul style="list-style-type: none">5 membros da famíliaControles administrativos simples	 Pacote básico Teams Proteja até 10 membros da equipe. €16.95 EUR <small>até 10 usuários por mês. Pago anualmente.</small> Experimente GRÁTIS por 14 dias <p>Proteja sua pequena equipe com:</p> <ul style="list-style-type: none">Compartilhamento simples e seguroAlertas de segurança acionáveis1Password Developer <small>• Recursos de integração e</small>	 Business Segurança que se adapta à sua empresa. €6.99 EUR <small>por usuário, por mês. Pago anualmente.</small> Fale com o departamento de vendas Experimente GRÁTIS por 14 dias <p>Tudo do Pacote básico Teams, além de:</p> <ul style="list-style-type: none">Integração com Okta, Entra ID, OneLogin, Duo e muito maisRelatórios avançados, controles administrativos granulares, criptografia de ponta a ponta <small>• Suporta iOS e 34 horas por dia 7</small>	 Enterprise Proteja todos da sua organização com segurança de nível corporativo.  <small>Entre em contato com a equipe de vendas para saber preços especiais.</small> Fazer orçamento <p>Tudo do plano Business, mais:</p> <ul style="list-style-type: none">Gerente de conta dedicado, gerente de integração e sucesso do cliente para contas com mais de 75 usuáriosIntegração e treinamento personalizados <small>• Suporta iOS e 34 horas por dia 7</small>
--	--	---	--	---

<https://1password.com/pt/pricing>

BITWARDEN

Get powerful, trusted password security now. Pick your plan.

Personal Business

Teams
Resilient protection for growing teams

\$4
per month / per user billed annually

- ✓ Secure data sharing
- ✓ Event log monitoring
- ✓ Directory integration

Includes premium features for all users

Start a Trial

Enterprise
Advanced capabilities for larger organizations

\$6
per month / per user billed annually

- ✓ Enterprise policies
- ✓ Passwordless SSO
- ✓ Account recovery

Includes premium features and complimentary families plan for all users

Start a Trial

Get a quote
For companies with hundreds or thousands of employees contact sales for a custom quote and see how Bitwarden can:

- ✓ Reduce cybersecurity risk
- ✓ Boost productivity
- ✓ Integrate seamlessly

Bitwarden scales with any sized business to bring password security to your organization

Contact Sales

Pricing shown in USD and based on an annual subscription

<https://bitwarden.com/pricing/business/>

VPNS


- <https://protonvpn.com/pricing>
- <https://mullvad.net/pt/pricing>
- Among others.


PROTONVPN


Proton VPN Plus


Proton Unlimited


All premium Proton services. One easy subscription.


 Proton Mail

 Proton Calendar

 Proton Drive

 Proton VPN

 Proton Pass

 Proton Wallet

0% OFF

1-month plan

€12.99 /month

Get 1-month plan

30-day money-back guarantee

Billed at €12.99 every month

BEST DEAL

38% OFF

2-year plan

€12.99

€7.99 /month

Save €120

Get 2-year plan

30-day money-back guarantee

Billed at €191.76 for the first 24 months

23% OFF

1-year plan

€12.99

€9.99 /month

Save €36

Get 1-year plan

30-day money-back guarantee

Billed at €119.88 for the first 12 months

<https://protonvpn.com/pricing>

MULLVAD

Um modelo de preços justo

Não é ilusão de ótica. É uma taxa mensal fixa para garantir a máxima flexibilidade. Incluindo IVA.

1 mês

€ 5
por mês

1 ano

€ 5
por mês

1 década

€ 5
por mês

€5 é equivalente a



US\$ 5,28



£ 4,17



SEK 57,66



AU\$ 8,13



CA\$ 7,41

<https://mullvad.net/pt/pricing>

SECURE CHANNELS

- Signal.
- Telemóveis e cartões descartáveis.
- Protonmail.
- Utilização de PGP.

EXPOSED INFORMATION AND TAKEDOWNS

- Submeter pedido de remoção da informação à entidade em questão justificando abrangência do RGPD.
- Depois remover a informação via formulário da google.
- <https://search.google.com/search-console/remove-outdated-content>

EXPOSED INFORMATION AND TAKEDOWNS



<https://search.google.com/search-console/remove-outdated-content>

EXPOSED INFORMATION AND TAKEDOWNS

Nova solicitação

Qual é o principal motivo para usar a ferramenta "Remover conteúdo desatualizado"?

- ☒ Atualizar o resultado do Google referente a uma página da Web que mudou
- ☐ Remover informações desatualizadas ou obsoletas de uma página da Web
- ☐ Remover permanentemente um conteúdo do Google

<https://search.google.com/search-console/remove-outdated-content>

DOXING

Doxxing (também escrito "doxing") é o ato de revelar as informações pessoais de alguém online. Doxxing é uma forma de assédio online que significa expor publicamente o nome real, endereço, emprego ou outras informações de identificação sem o consentimento da pessoa. O objetivo do doxxing é humilhar, intimidar, assediar ou prejudicar a vítima de alguma forma.

<https://www.avast.com/pt-br/c-what-is-doxxing>

DOXING E PII

Remove personally identifiable info or doxxing content from Google Search

You can request to remove select personally identifiable information (PII) from Google Search results. This information includes:

- Address, phone number, and/or email address
- Confidential government identification (ID) numbers (for example, Social Security or Tax ID number, Resident Registration or Resident Identity Card number)
- Bank account or credit card number
- Images of a handwritten signature or an ID doc
- Highly personal, restricted, and official records (for example, medical records)
- Confidential login credentials
- Other types of personal information

We may also consider the removal of the above and other types of personal info if it is being shared maliciously (this practice is sometimes known as doxxing). [Learn more about the factors we consider when we evaluate for doxxing.](#)

Request to remove select info from Google Search

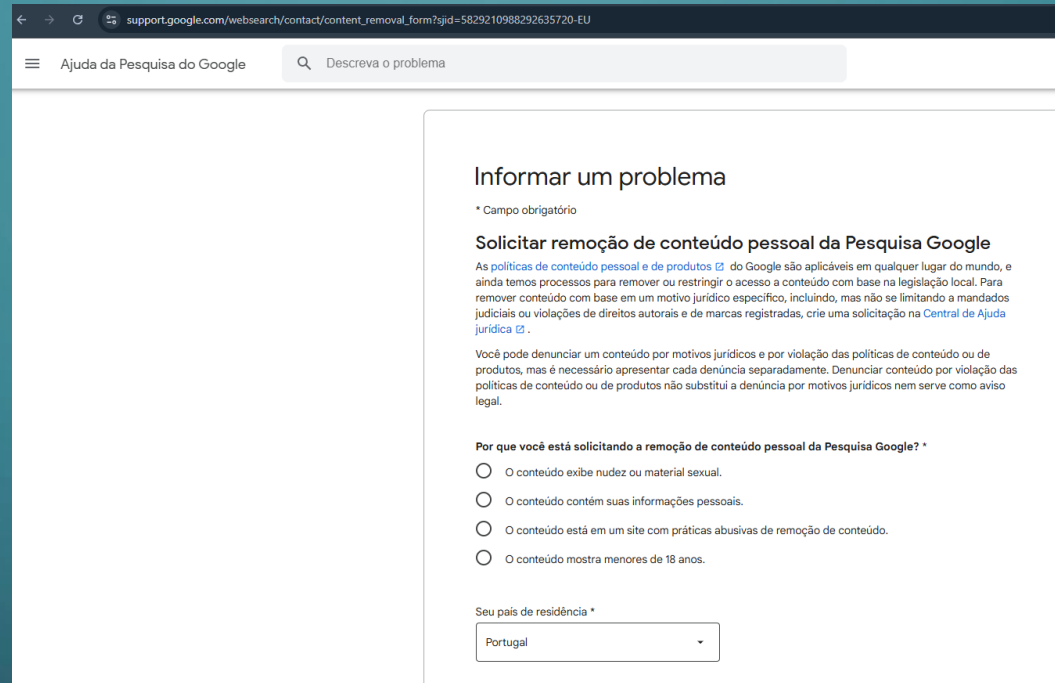
You or your authorized representative can submit a request to remove links to the content from Google Search results. Any authorized representative must explain how they have the authority to act on your behalf.

Important: We only review the URLs that you or your authorized representative submit in the form.

[Start removal request](#)

<https://support.google.com/websearch/answer/9673730?hl=en>

DOXING E PII



A screenshot of the Google Content Removal Request form. The browser address bar shows the URL: support.google.com/websearch/contact/content_removal_form?sjid=5829210988292635720-EU. The page header includes 'Ajuda da Pesquisa do Google' and a search bar with the placeholder text 'Descreva o problema'. The main heading is 'Informar um problema'. Below it, a note states '* Campo obrigatório'. The section is titled 'Solicitar remoção de conteúdo pessoal da Pesquisa Google'. The text explains that Google's policies on personal content and products are applicable worldwide, and that users can request removal based on local legislation, specific legal reasons, or trademark violations. It provides links to 'políticas de conteúdo pessoal e de produtos' and 'Central de Ajuda jurídica'. A paragraph states that users can report content for legal reasons or policy violations, but each report must be separate. Below this, a question asks 'Por que você está solicitando a remoção de conteúdo pessoal da Pesquisa Google? *' with four radio button options: 'O conteúdo exibe nudez ou material sexual.', 'O conteúdo contém suas informações pessoais.', 'O conteúdo está em um site com práticas abusivas de remoção de conteúdo.', and 'O conteúdo mostra menores de 18 anos.'. At the bottom, there is a field for 'Seu país de residência *' with a dropdown menu currently showing 'Portugal'.

support.google.com/websearch/contact/content_removal_form?sjid=5829210988292635720-EU

Ajuda da Pesquisa do Google

Descreva o problema

Informar um problema

* Campo obrigatório

Solicitar remoção de conteúdo pessoal da Pesquisa Google

As [políticas de conteúdo pessoal e de produtos](#) do Google são aplicáveis em qualquer lugar do mundo, e ainda temos processos para remover ou restringir o acesso a conteúdo com base na legislação local. Para remover conteúdo com base em um motivo jurídico específico, incluindo, mas não se limitando a mandados judiciais ou violações de direitos autorais e de marcas registradas, crie uma solicitação na [Central de Ajuda jurídica](#).

Você pode denunciar um conteúdo por motivos jurídicos e por violação das políticas de conteúdo ou de produtos, mas é necessário apresentar cada denúncia separadamente. Denunciar conteúdo por violação das políticas de conteúdo ou de produtos não substitui a denúncia por motivos jurídicos nem serve como aviso legal.

Por que você está solicitando a remoção de conteúdo pessoal da Pesquisa Google? *

- ☐ O conteúdo exibe nudez ou material sexual.
- ☐ O conteúdo contém suas informações pessoais.
- ☐ O conteúdo está em um site com práticas abusivas de remoção de conteúdo.
- ☐ O conteúdo mostra menores de 18 anos.

Seu país de residência *

Portugal

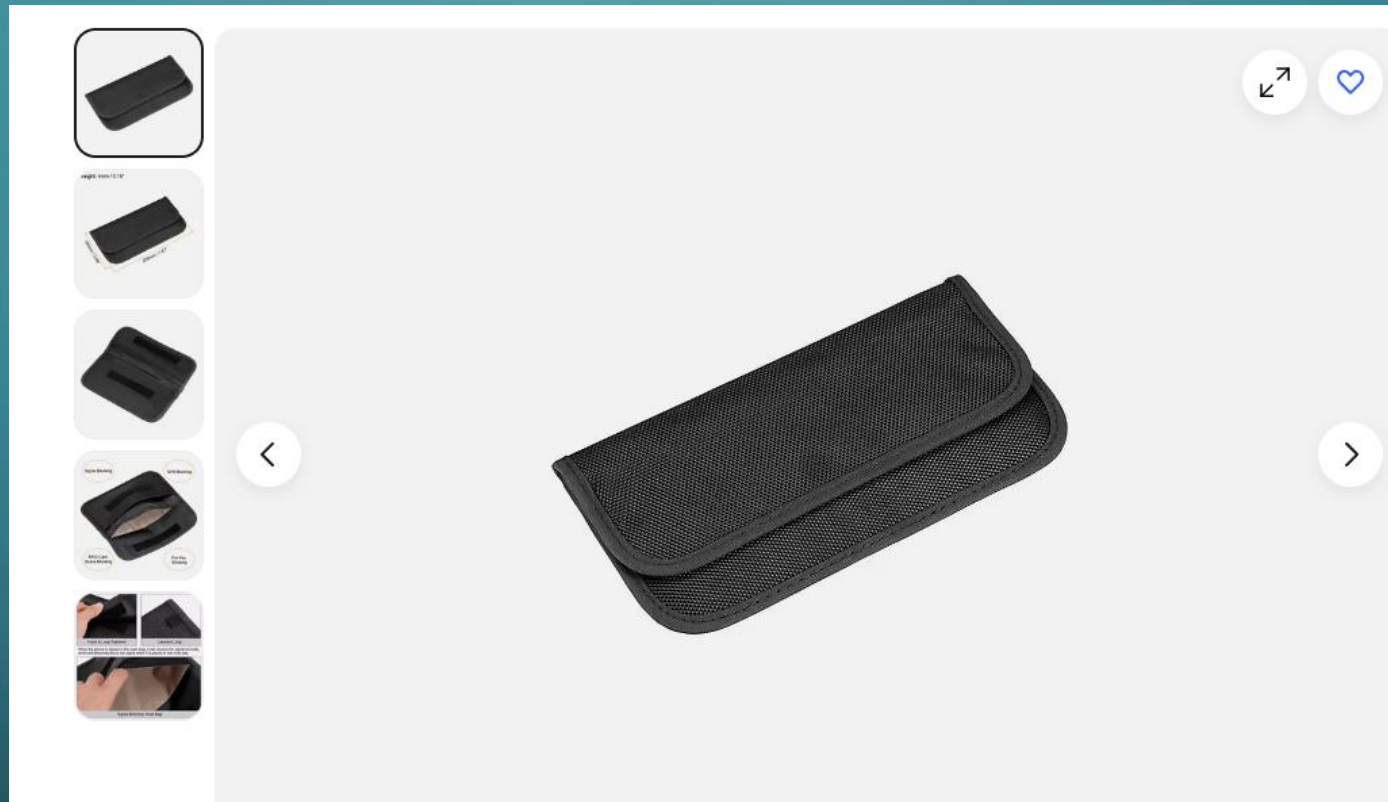
https://support.google.com/websearch/contact/content_removal_form?sjid=5829210988292635720-EU

SOCIAL MEDIA

Social Media "Closure" - Validar informação tua ou de terceiros em redes sociais e fechar tudo o que seja sensível.

Exemplo: Uma foto nossa num terceiro que pode expor a nossa localização.

FARADAY BAGS



<https://www.ebay.co.uk/itm/185921071582>

RFID BLOCKERS

BANKING

- Validar os terminais de pagamento bem como os ATMs antes de usar o cartão.
- Utilizar cartões bancários de uma só compra com valor fixo.
- Não utilizar redes desconhecidas para online banking.



PAUSA



CIBERSEGURANÇA ORGANIZACIONAL: POLITICA, CULTURA E FORMAÇÃO

- Formações gratuitas do Centro Nacional de cibersegurança (cidadão ciberseguro) entre outros providers
- Políticas de governance, risk and Compliance atualizadas
- Realização de testes de intrusão e emulação de ameaças recorrentes
- Realização de backups e storage em cold e hot site
- Procedimentos de resposta a incidentes e análise forense se caso
- Cultura não discriminatória a quem comete erros porque errar é humano

