WORKSHOP – CIBERSEGURANÇA E A SUA CRITICIDADE EM EMPRESAS E CIDADÃOS

- 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-obcibercncs.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-contra-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-semestre

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.

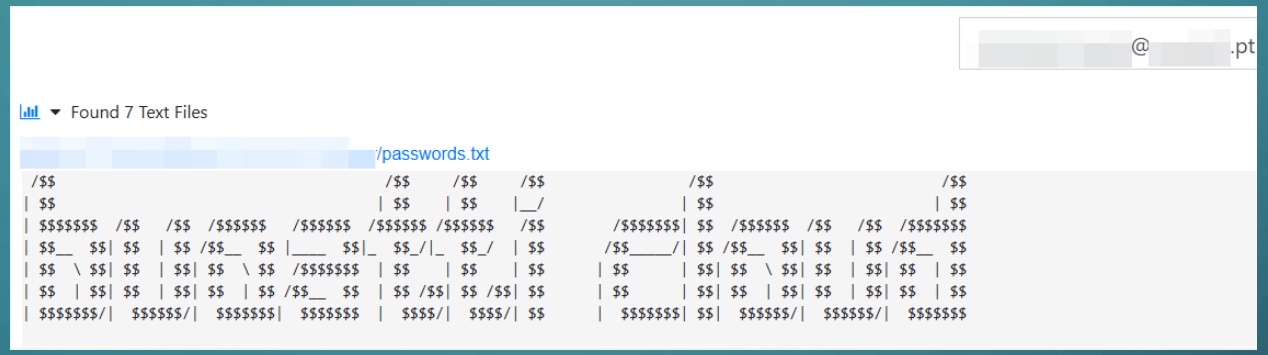
Este tipo de código malicioso representa um desafio considerável, pois a sua utilização reduz significativamente o custo inicial de intrusão na infraestrutura da vítima para posterior realização de ataques mais rentáveis para o criminoso, como por exemplo o *ransomware*. Uma vez obtidas as credenciais 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?

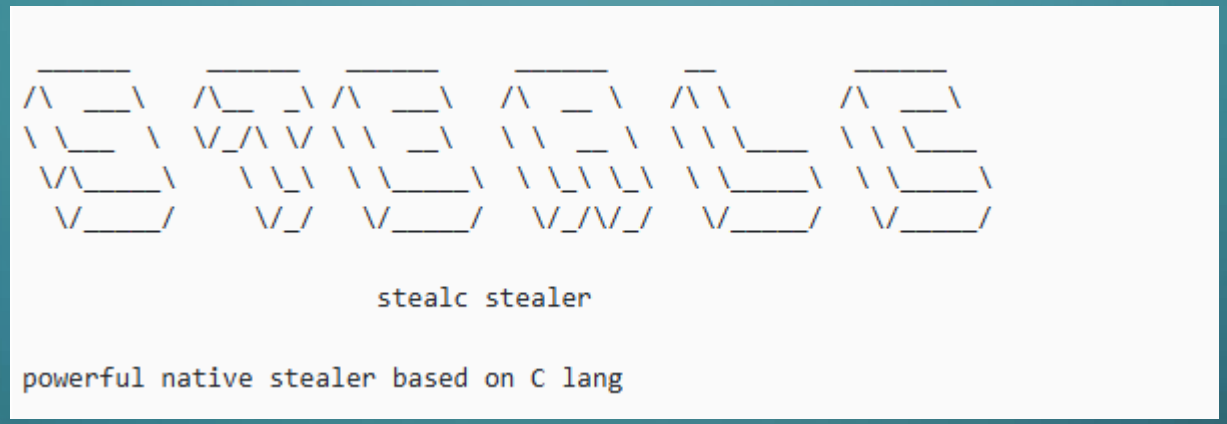
https://haveibeenpwned.com/

?AM I SAFE?



https://intelx.io/

?AM I SAFE?



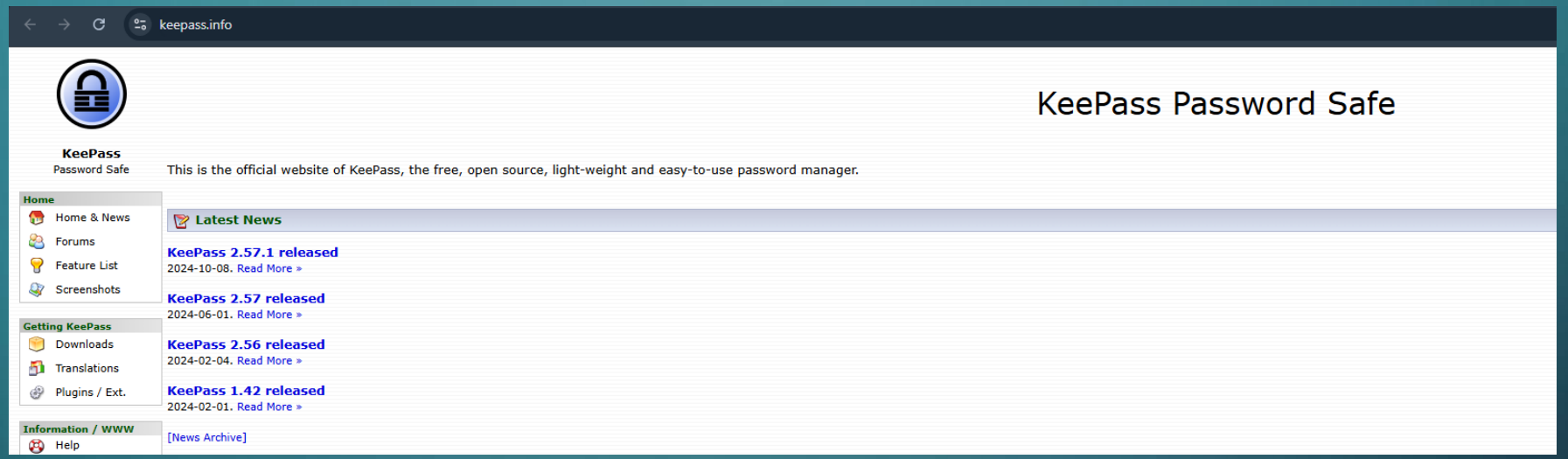
https://intelx.io/

MEDIDAS BÁSICAS DE PROTEÇÃO E BOAS PRÁTICAS DE SEGURANÇA DIGITAL

PASSWORD MANAGERS

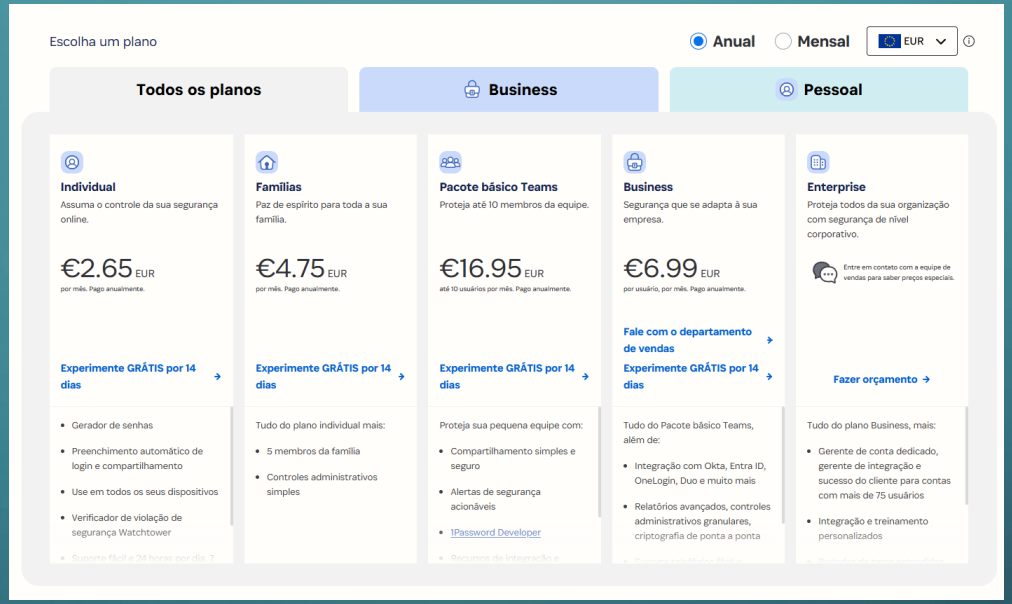
- https://keepass.info/
- https://1password.com/
- https://bitwarden.com/
- Among others.

KEEPASS



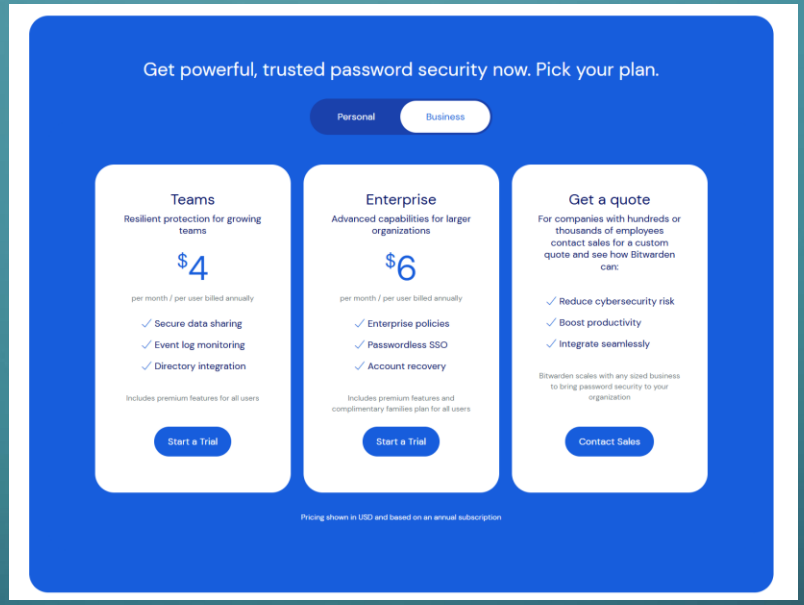
https://keepass.info/

1PASSWORD



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

BITWARDEN

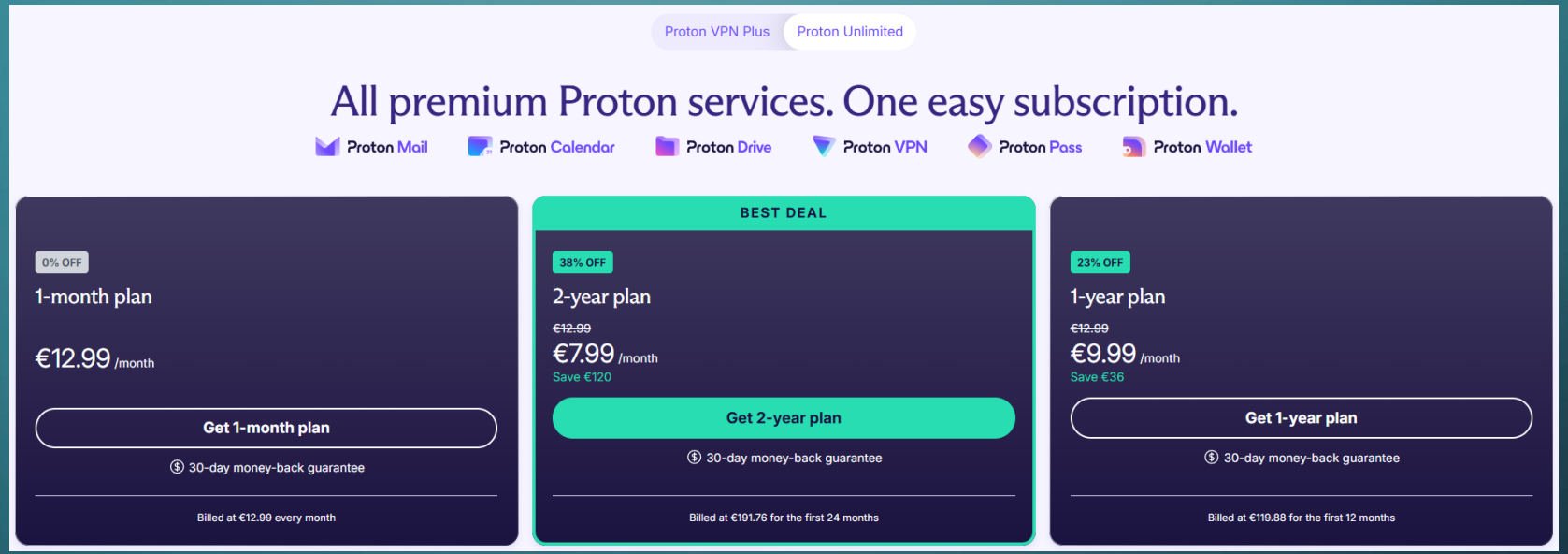


https://bitwarden.com/pricing/business/

VPNS

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

PROTONVPN



https://protonvpn.com/pricing

MULLVAD

https://mullvad.net/pt/pricing

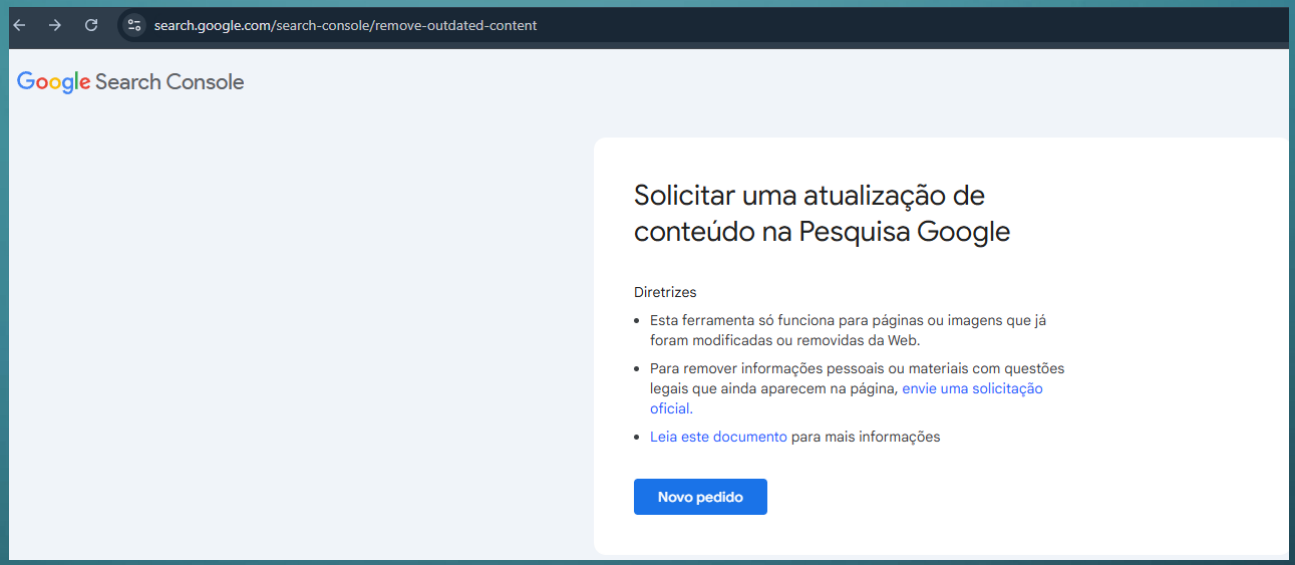
SECURE CHANNELS

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

EXPOSED INFORMATION AND TAKEDOWNS

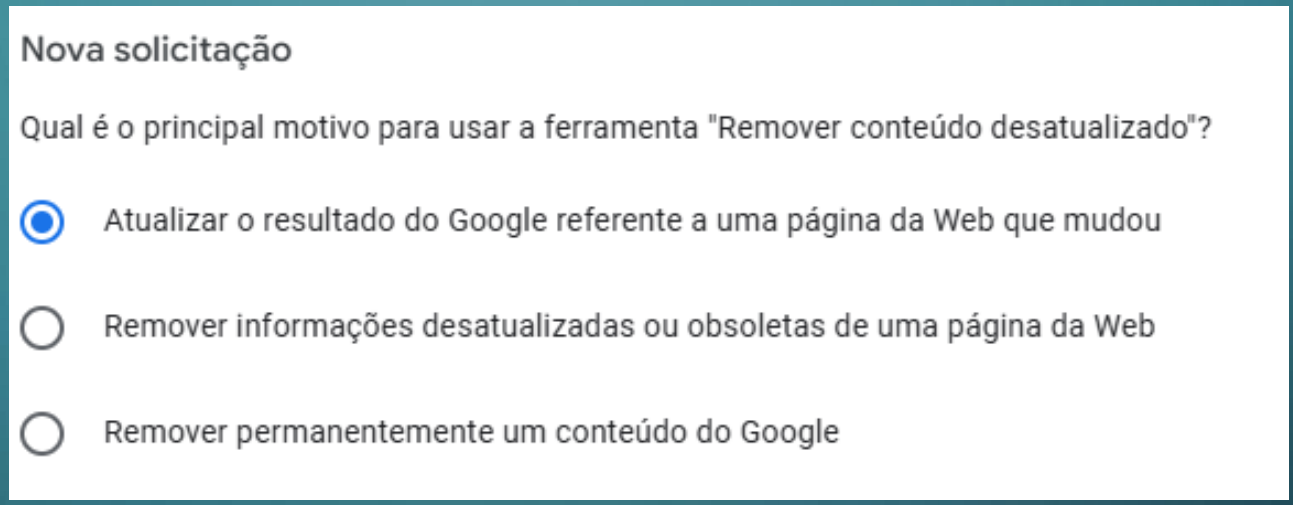
- Submeter pedido de remoção da informação à entidade em questão justificando abrangência do RGPD.
- Depois remover a informação via formulário da google.
- https://search.google.com/search-console/remove-outdated-content

EXPOSED INFORMATION AND TAKEDOWNS



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

EXPOSED INFORMATION AND TAKEDOWNS



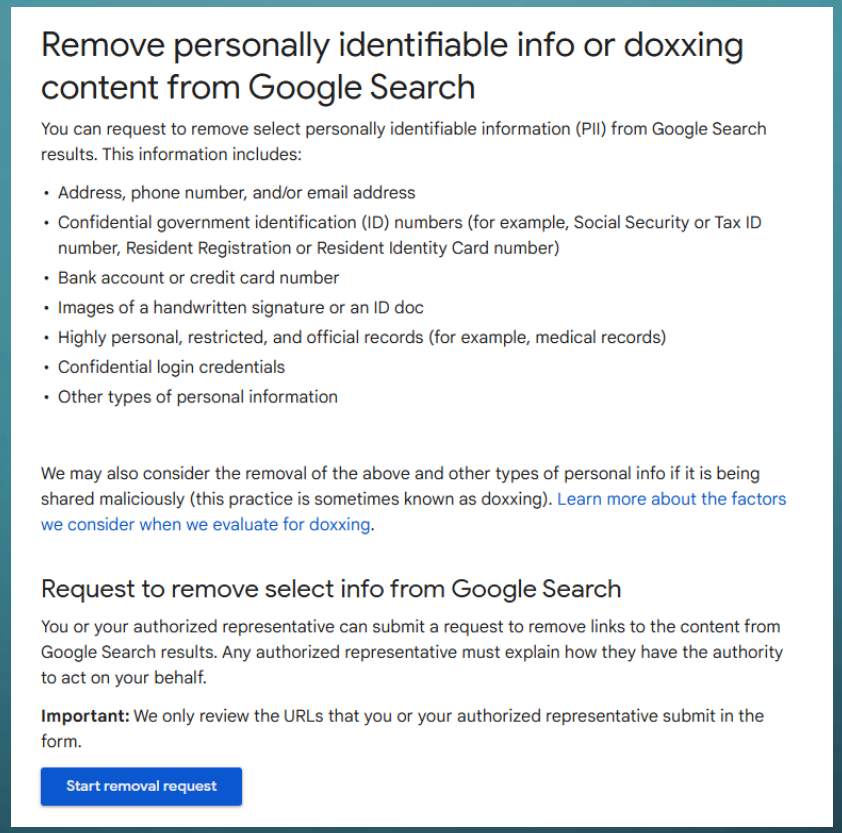
https://search.google.com/search-console/remove-outdated-content

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

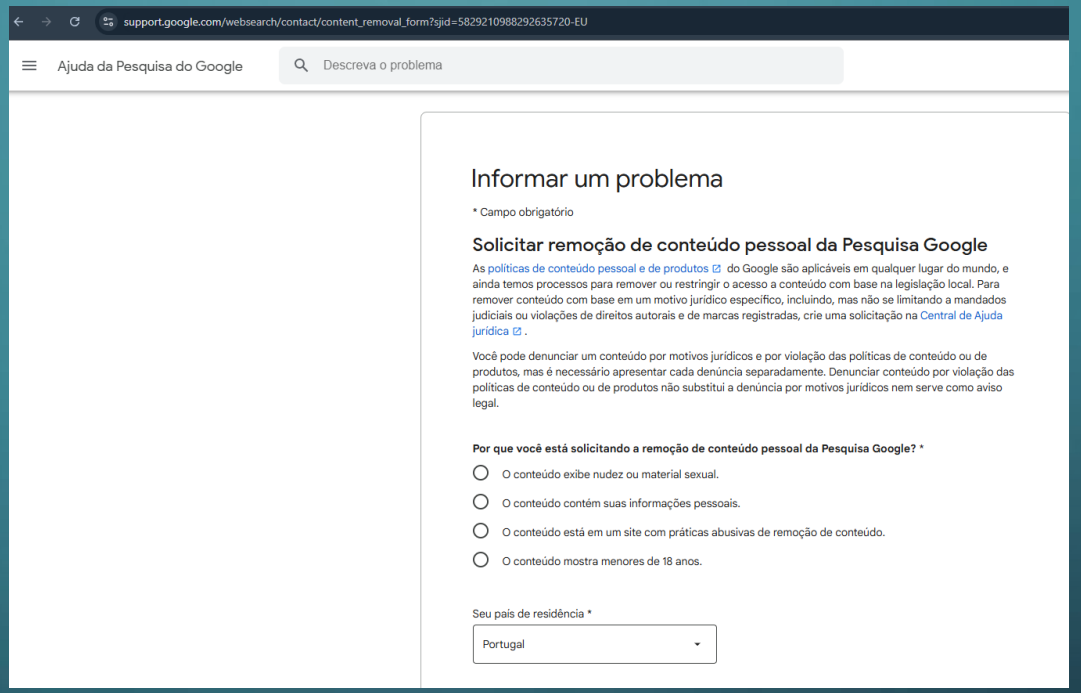
You or your authorized representative can submit a request to remove links to the content from Google Search results. Any authorized representative must explain how they have the authority to act on your behalf.

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



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
- Politicas 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 anáise forense se caso
- Cultura não descriminatória a quem comete erros porque errar é humano


That's all Folks!