



Tempest

ACADEMY

Conference  
2023

# Um Guia Inicial para análise de URLs de Phishing

---





Tempest

**ACADEMY**

Conference

**01** Introdução

**02** Conhecendo o Adversário

**03** Ambiente de Análise

**04** Análise da Página Falsa



Tempest

ACADEMY

Conference

# Introdução

---



[ACADEMY]

Conference

THIS  
IS WHO  
I AM



Trabalhando na Tempest há quase 10 anos



Praticante e pesquisador de Threat Intelligence



Atuei diretamente no combate a mais de 10 mil campanhas de Phishing



Lidero um time que tem como foco ajudar negócios a tomarem conhecimento sobre as ameaças e se protegerem delas

# Objetivos

- 1. Entender o que é Phishing e a importância de combatê-lo**
- 2. Conhecimentos iniciais para começar a analisar Páginas Maliciosas**
- 3. Dicas para montar seu primeiro laboratório de análise de Phishing**
- 4. Entender técnicas que os atacantes utilizam para dificultar sua análise**



# Phishing

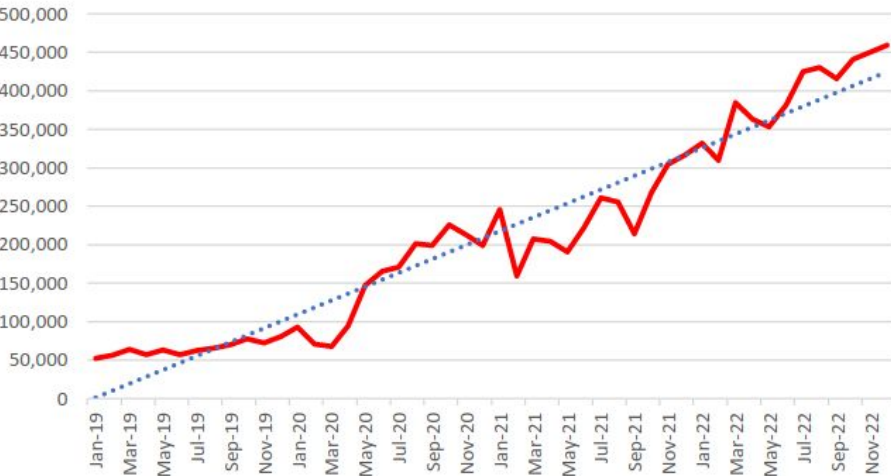
# Phishing

Phishing é um tipo de **ataque** em que criminosos se passam por entidades confiáveis para **enganar** as vítimas e obter **informações pessoais, financeiras ou confidenciais** ou **ganhos financeiros diretos**.

Esse tipo de ataque emprega tanto engenharia social quanto recursos técnicos para enganar suas vítimas.

# Phishing

Phishing Attacks, Jan 2019 to Dec 2022



Campanhas de Phishing  
**cresceram mais de 150%**  
**ao ano** nos últimos 4 anos



# Phishing

## Estudo revela que o Brasil é líder m golpes de phishing

Relatório mostra que um em cada cinco brasileiro menos uma tentativa de ataque em 2020. Já os ci mais de 120% durante a pandemia

Por: Redação | 13/10/2021 às 16h35 - Atualizado em 13/10/2021 às 16h35



2021

## Brasil é líder de phishi na América Latina; sai se proteger

Fácil de ser executado pelos criminosos, o golpe também é bastante simp



Home > Tecnologia > Brasil é líder de phishing na América Latina; saiba se proteger

Por [Dimitria Coutinho](#) | 18/11/2022 06:00

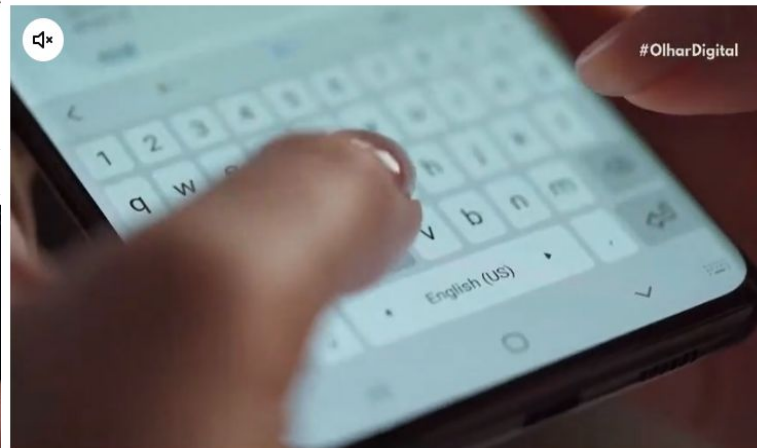


2022

## Brasil é líder em golpes de phishing pelo WhatsApp

Pesquisa da Kaspersky apontou que fraude com link falso foi a mais usada no app em 2022

Tamires Ferreira | 24/03/2023 09h41, atualizada em 24/03/2023 21h02



2023

Tempest

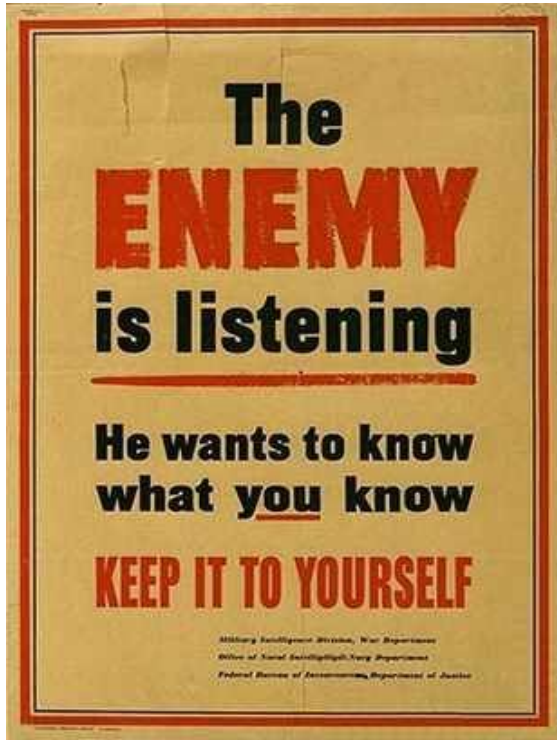
ACADEMY

Conference



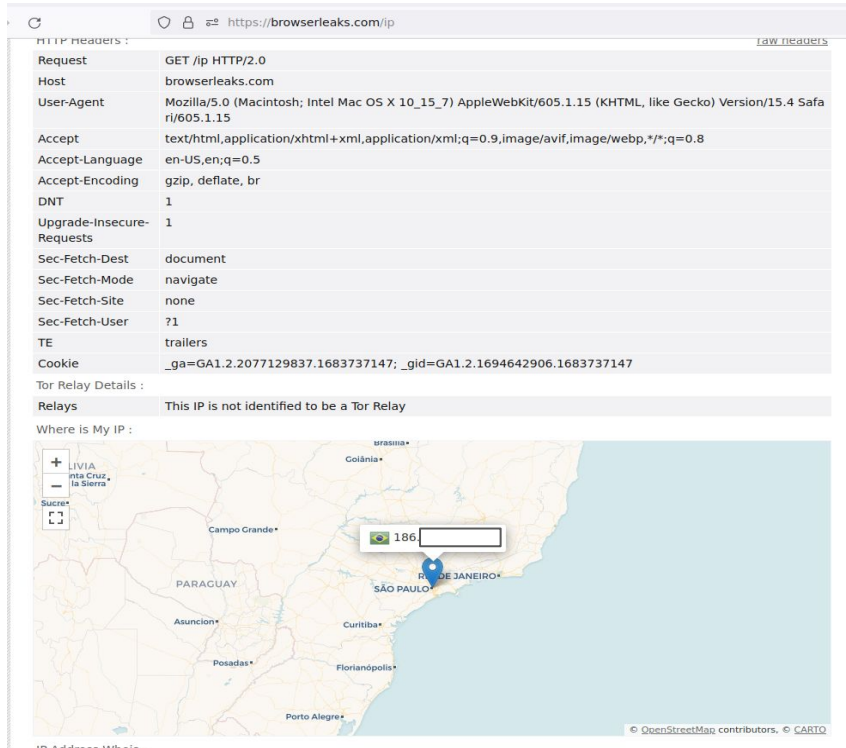
# Segurança Operacional

# Segurança Operacional



OPSEC envolve vários processos e procedimentos usados para proteger informações que podem ser aproveitadas por adversários

# Segurança Operacional



The screenshot shows the 'Network' tab of a browser's developer tools. The selected request is to 'https://browserleaks.com/ip'. The 'Headers' pane is expanded to show 'Request Headers'. Below the headers, the 'Tor Relay Details' section indicates 'This IP is not identified to be a Tor Relay'. The 'Where is My IP' section shows a map of South America with a blue pin over Rio de Janeiro, Brazil. A text box next to the map displays the IP address '186'. The browser's address bar shows the URL 'https://browserleaks.com/ip'.

HTTP headers :	
Request	GET /ip HTTP/2.0
Host	browserleaks.com
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.4 Safari/605.1.15
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate, br
DNT	1
Upgrade-Insecure-Requests	1
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Sec-Fetch-Site	none
Sec-Fetch-User	?1
TE	trailers
Cookie	_ga=GA1.2.2077129837.1683737147; _gid=GA1.2.1694642906.1683737147

Tor Relay Details :

Relays This IP is not identified to be a Tor Relay

Where is My IP :

186

IP Address Whnic

Apenas navegando na Internet vocês entregam informações sobre você:

- Qual sistema Operacional
- Qual o seu endereço IP
- Qual a sua geolocalização
- Qual a versão do seu navegador

HTTP Headers :

[raw headers](#)

Request	GET /ip HTTP/2.0
Host	browserleaks.com
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.4 Safari/605.1.15
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate, br
DNT	1
Upgrade-Insecure-Requests	1
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Sec-Fetch-Site	none
Sec-Fetch-User	?1
TE	trailers
Cookie	_ga=GA1.2.2077129837.1683737147; _gid=GA1.2.1694642906.1683737147

Tor Relay Details :

Relays	This IP is not identified to be a Tor Relay
--------	---

Where is My IP :



# Segurança Operacional

## SWATing: A Prank Where Police Storm Your House

The home of cybersecurity journalist Brian Krebs was flooded by a SWAT team last week pranked into thinking an emergency was happening on his property. He's not alone.



⚠️ OBS:ÓBITO DADO NA BASE DO SUS SE CASO O INDIVÍDUO PISAR EM ALGUM HOSPITAL PARA RESOLVER PROBLEMAS MÉDICOS 🏥, VAI TA FUDIDO E SERÁ O PIOR ATRASO DA VIDA DELE ❌

👤 01 CPF ÓBITO R\$150,00  
👤 04 CPF ÓBITO R\$350,00

✅ todo o procedimento de operação a Óbito em CPF, iniciamos a gravação da Tela 🖥 de execução do serviço do início ao fim, executamos uma nova realização de consulta ao CPF do bico no banco de dados CADSUS pra que assim seja feita a verificação e a checagem da veracidade, no êxito na realização do Óbito ao CPF desejado. ✅



8 de janeiro · 🌐

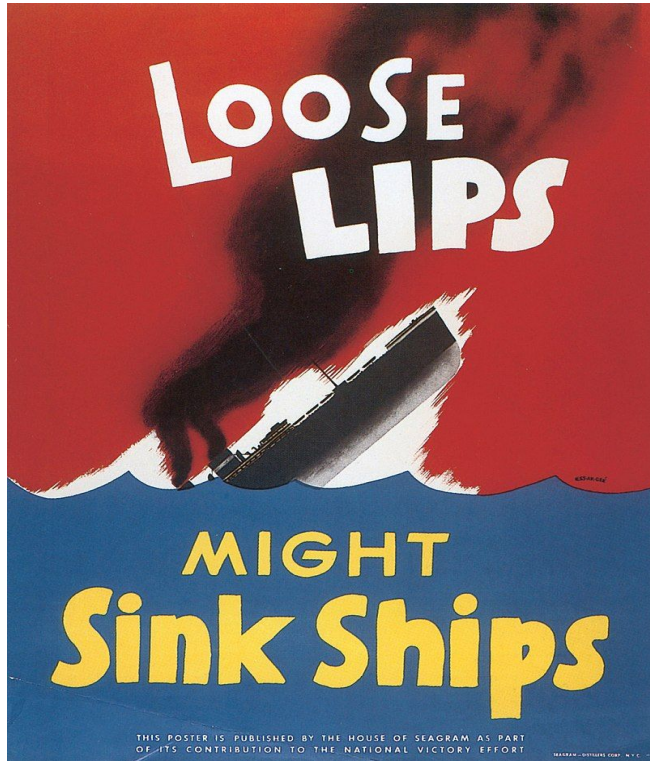
ABRO LARA EM UM BANCO CPF ESPECÍFICO, PIX ATIVO E DEPENDENDO DO SCORE DEPOIS DE UM TEMPO SOLTA UM EMPRÉSTIMO PESSOAL VEM 🧑



1

1 comentário

# Segurança Operacional



Medidas para manter o OPSEC:

- Personas
- Ambiente virtualizado
- Saídas anonimizadas



**ACADEMY**

Conference

# Conhecendo o Adversário

---





**ACADEMY**

Conference



**Conhecimento  
Técnico**



**Motivação**

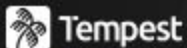


**Entendimento do  
Adversário**



# Exemplos de técnicas de bloqueio de conteúdo

# Bloqueio por Origem



ACADEMY

Conference

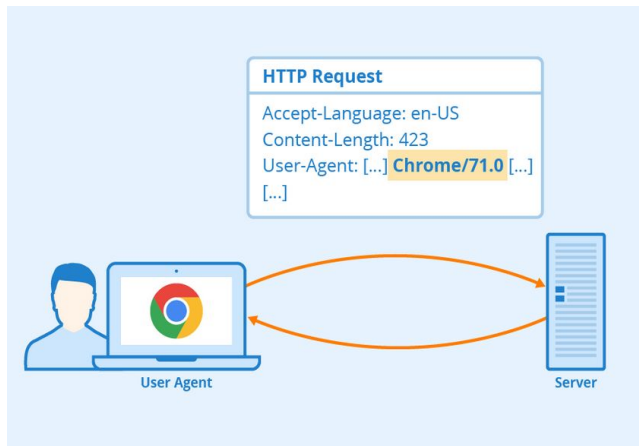
```
<limit GET POST PUT HEAD>
order deny,allow
allow from 179.
allow from 186.
allow from 187.
allow from 189.
allow from 191.
allow from 192.
allow from 198.
allow from 200.
allow from 201.
deny from 150.70.173.
deny from 213.190.193.
deny from 81.161.59.
deny from 70.39.157.
deny from all
</limit>
```

```
$ListaBanidos = array("scotiabank", "letti.", "unisys", "
antivirus1.unisys", "antivirus", "abuse@", "spam@", ".sysms.net
", "easysol.net", "diebold", "cisco.com", "antivirus2.unisys
", "hawking.unisys", "ragingwire.net", "isitphishing.org", "
barracuda", "netcraft", "ebay.", "panda.", "microsoft.", "fbi."
, "google.", "resuelveserver", "bankofamerica", "mozilla.",
"viabcp.", "veritas.", "nod32.", "antipishing.", "kapersky.", "
norton.", "symantec.", "rsasecurity.", "bancopopular.", "
paypal.", "unicaja.", "movistar.", "banesto", "cajamadrid",
"bancopastor", "rsa.", "symantecstore.", "gfihispana.", "
fraudwatchinternational.", "verisign.", "markmonitor.", "
anti-phishing.", "pandasoftware.", "delitosinformaticos.", "
zonealarm", "alerta-antivirus", "vsantivirus", "
nortonsecurityscan", "hauri-la", "cleandir", "trendmicro", "
mcafee", "nod32-es", "pandaantivirus", "free-av", "grisoft"
, "bitdefender-", "sophos", "activescan", "avast", "
bitdefender", "trendmicro-europe", "clamav", "clamwin", "
```

# Bloqueio por Dispositivo



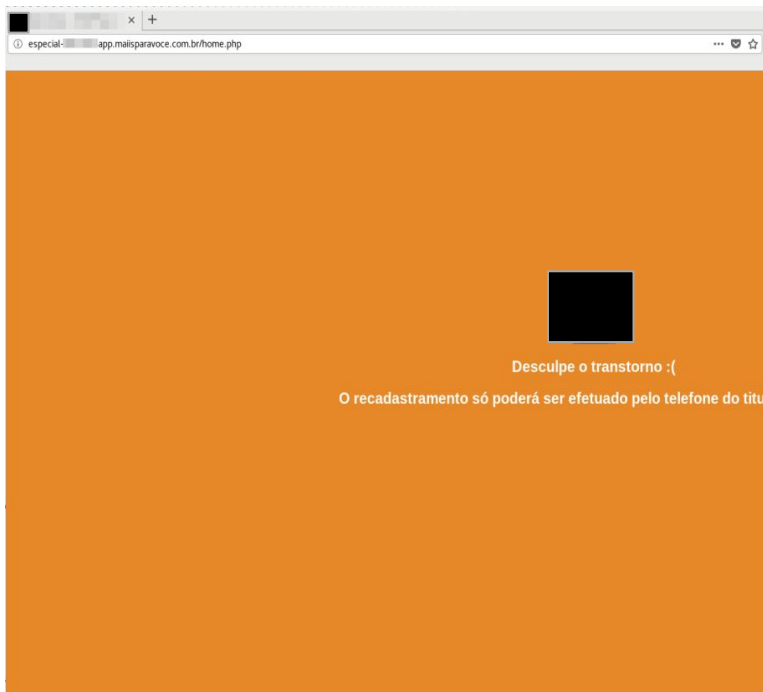
ACADEMY  
Conference



```
<script>
var suamae = navigator.userAgent.toLowerCase();
var uMobile = '';
uMobile += 'iphone;ipod;windows phone;android;iemobile 8';
v_uMobile = uMobile.split(';');
var boolMove1 = false;
for (i=0;i<=v_uMobile.length;i++){
  if (suamae.indexOf(v_uMobile[i]) != -1){
    boolMove1 = true;
  }
}
if (boolMove1 != true){
  location.href='http://xxxx.eu';
}
</script>
```

# Bloqueio por Tela

Tela tamanho desktop



Tela tamanho mobile





**ACADEMY**

Conference

# Ambiente de Análise

---

# Virtualização







# Navegador














# Navegador

 **Header Editor**   





Manage browser's requests, include modify the request headers and response h...

 **HTTP Header Live**   






Show the HTTP header fields. You can edit and resubmit.

 **Image Search Options**    





Customizable Image Search right click context options

 **Mobile simulator**   






Smartphone simulator on computer very realistic with several models to test mo...

 **NoScript**    

Maximum protection for your browser: NoScript allows active content only for tru...

 **Resurrect Pages**   

Resurrect dead pages, by finding their ghosts.

 **User-Agent Switcher and Manager**    

Spoof websites trying to gather information about your web navigation to deliver...

Connection Settings ✕

**Configure Proxy Access to the Internet**

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration

HTTP Proxy  Port

Also use this proxy for HTTPS

HTTPS Proxy  Port

SOCKS Host  Port

SOCKS v4  SOCKS v5

Automatic proxy configuration URL

Reload

No proxy for

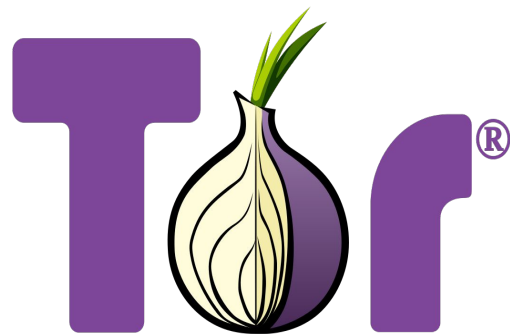
Example: .mozilla.org, .net.nz, 192.168.1.0/24  
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

Do not prompt for authentication if password is saved

Proxy DNS when using SOCKS v5

Cancel OK

# Saída Anonimizada



[TorProject.org](https://torproject.org)



# Setup para começar



+



+





**ACADEMY**

Conference

# Análise da Página Falsa

---



# URL

# Elementos da URL

- **Site Comprometido/ Domínio Malicioso**
- **Informações do Host/Registrar**
- **Parâmetros da URL**

# Elementos da URL

**Submission #8374959** is currently **ONLINE**

Submitted Nov 25th 2023 3:32 AM by [CharisDickinson](#) (Current time: Nov 25th 2023 1:52 PM UTC)

<https://suaspromocoes.com/>



[Sign in](#) or [Register](#) to verify this submission.

This submission needs more votes to be confirmed or denied.

Screenshot of site

View site in frame

View technical details

[View site in new window](#) 

**No screenshot yet.**

We have not yet successfully taken a screenshot of the submitted website.

# Elementos da URL

The screenshot shows the homepage of suaspromocoes.com. At the top, there is a search bar with the text "O que você está procurando?" and a shopping cart icon with a "0" badge. Below the search bar is a navigation menu with categories: INÍCIO, MASCULINO, FEMININO, INFANTIL, CALÇADOS, ROUPAS, SUPLEMENTOS, and EQUIPAMENTOS. A yellow banner below the menu reads "GARANTA +10% OFF NA PRIMEIRA COMPRA, USANDO O CUPOM PRIMEIRA10" with a link to "CONSULTE O REGULAMENTO". The main banner features a pair of blue and red sneakers, the text "BLACK NOVEMBER", and "PRODUTOS COM ATÉ 70% OFF NÃO PERCA >". Below the main banner are four promotional boxes: "2 POR R\$ 99,90", "LEVE 3 POR 2", "2 POR R\$ 129,90", and "4 POR R\$ 99,90". At the bottom, there are three smaller images of different shoe models.



# Elementos da URL

suaspromoco.es.com

Updated 11 hours ago 



## Domain Information

Domain: suaspromoco.es.com

Registrar: GoDaddy.com, LLC

Registered On: 2023-11-24

Expires On: 2024-11-24

Updated On: 2023-11-24

Status: clientDeleteProhibited  
clientRenewProhibited  
clientTransferProhibited  
clientUpdateProhibited

Name Servers: ns07.domaincontrol.com  
ns08.domaincontrol.com

# Elementos da URL

## DNS records for **suaspromocoes.com**

Cloudflare

Google DNS

OpenDNS

Authoritative


Local DNS 

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as they are not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

### A records

IPv4 address

Revalidate in

>  23.227.38.32

1h

# Elementos da URL

- **Site Comprometido/ Domínio Malicioso?**
  - Domínio Malicioso
- **Informações do Host/Registrar**
  - Godaddy
  - CloudFlare
- **Parâmetros da URL**
  - N/A



# Navegar na Página

# Navegar na Página

- **Qual é o fluxo do Phishing?**
- **Quais informações são solicitadas?**
- **Existe algum tipo de bloqueio?**
- **Qual é o público-alvo da campanha?**

# Navegar na Página

https://suaspromocoes.com/products/tenis-adidasbrand-20-frete-gratis-esquenta-bl...  
O que você está procurando?

INÍCIO MASCULINO FEMININO INFANTIL CALÇADOS ROUPAS SUPLEMENTOS EQUIPAMENTOS

Página inicial > Todos os produtos > Tênis Adidas Brand 2.0 - ESQUENTA BLA...



Passe o mouse sobre a foto para ampliar

Diga adeus aos tênis

Lançamento | Pré Black Friday | 7.855 Vendidos

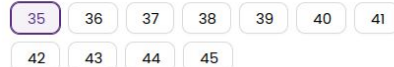
## Tênis Adidas Brand 2.0 - ESQUENTA BLACK FRIDAY NETSHOES

Vendido e entregue por: [Redacted]

Cor: Branco e Laranja



Tamanho: 35



Preço: R\$ 247,90

**R\$ 127,90** ↓ 48%

Em até 10x sem juros de **R\$ 12,96**

R\$ 120 de desconto

https://seguro.nexuscheckout.com.br

### 1 Identificação

Nome completo

Nome e Sobrenome

E-mail

email@email.com

CPF

123.456.789-12

Celular / Whatsapp

(99) 99999-9999

### 2 Entrega

Outra pessoa irá receber o pedido? [Clique aqui](#)

CEP

12345-000

Seu carrinho



Tênis Adidas Brand 2.0 Branco e Laranja

Subtotal


Frete


Tem um cupom?

Código do cupom

Total

# Navegar na Página


https://seguro.nexuscheckout.com.br/pix/kZ7xnjzG? 

 Ambiente seguro


**Falta pouco! Para finalizar a compra, escaneie o QR Code abaixo.**

O beneficiário do PIX é a **NEXUS PAY**.  
Esse é o nome da empresa que intermedia nossos pagamentos.

O código expira em: **28:35**




Se preferir, pague com a opção **PIX Copia e Cola:**




 **COPIAR CÓDIGO**

**Detalhes da compra**

Valor total: **R\$ 127,90**



**Instruções para pagamento**

-  Abra o app do seu banco e entre no ambiente Pix
-  Escolha **Pagar com QR Code** e aponte a câmera para o código ao lado.
-  Confirme as informações e finalize sua compra.

## O que estão falando sobre Nexus Pay

### Reclamações


Últimas

**Não respondidas**

Respondidas


#### Deposito feito

Fiz um depósito de 87. Para fins de devolução de dinheiro perdido conta , Isso ai é um belo de um [Editado pelo Reclame Aqui] daquela devolução do valor no pix tenho comprovante do pagamento da t

 **Não respondida** Há 1 hora

#### Loja não enviou a mercadoria

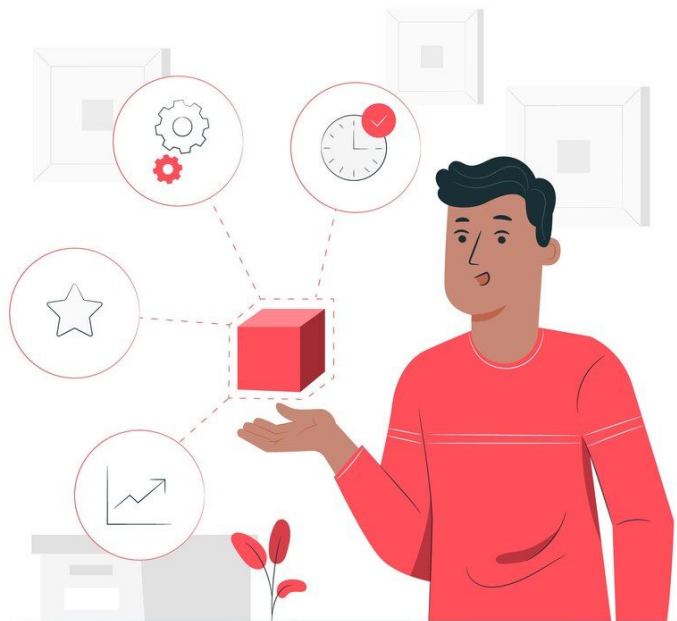
Bom dia, tentei resolver com a loja que vcs colocaram na plataforma vender produtos pra gente, sem sucesso, reputação horrível dessa loja, enrolando a loja pra mim não existe é [Editado pelo Reclame Aqui] a loja não responde nem visualiza nenhuma msg, me passaram m

 **Não respondida** Há 1 hora

#### paguei via pix e não recebi a mercadoria

estava no Instagram, vi a propaganda enganosa sobre a marca us compra paguei via pix, recebi um ctt por wats zapp da [Editado pelo Reclame Aqui] AMANDA PELO N \*\*\*\*\* e até hoje meses depois, não dev dinheiro e muito menos entregaram as compras!!

 **Não respondida** Há 1 hora



# Resumindo



# Resumindo



- Domínio Malicioso recém registrado na Godaddy e site na Cloudflare
- Página sem Bloqueio, focada no público em geral e utilizando processador legítimo de pagamentos.



ACADEMY

Conference

# Considerações Finais

---

# Objetivos

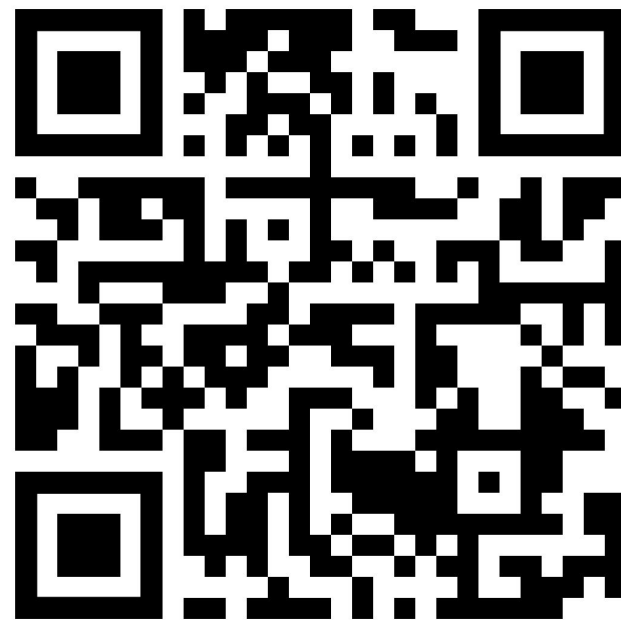
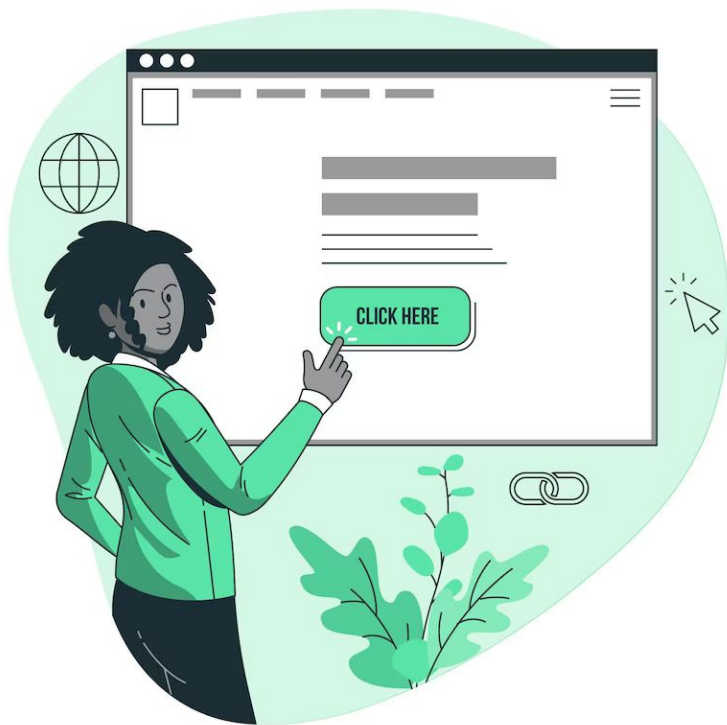
1. Entender o que é Phishing e a importância de combatê-lo ✓
2. Conhecimentos iniciais para começar a analisar Páginas Maliciosas ✓
3. Dicas para montar seu primeiro laboratório de análise de Phishing ✓
4. Entender técnicas que os atacantes utilizam para dificultar sua análise ✓

# Próximos Passos



- Analisar código-fonte da Página
- Analisar requisições executadas pela página Maliciosa

# Links Úteis





Tempest

ACADEMY

Conference

2023

