

@OFLAVIOC

URGENTE!

NOVO GOLPE POR EMAIL



Você ainda não resgatou o valor de R\$ 2.284,72 do Governo Federal.

O prazo para efetuar o resgate é até 16/02/2024

Solicitamos que acesse agora mesmo para verificar e confirmar seus dados

NÃO CLIQUE!

SEGURANÇA
DESCOMPLICADA

ATENÇÃO

Essa análise técnica revela um esquema de phishing que utiliza informações pessoais da vítima para criar um cenário convincente, encorajando o pagamento de uma taxa de R\$ 68,47 sob a promessa de liberação de um valor fixo de R\$ 2.284,72.

A personalização do ataque com detalhes específicos, como CPF e nome completo, sugere o acesso a bases de dados comprometidas.

Se você recebeu esse e-mail, não clique ou faça qualquer pagamento, é um golpe!

A análise começa com o recebimento de um e-mail de origem desconhecida, com o remetente utilizando um domínio @gmail.com. O e-mail continha meu nome completo e um PDF anexo nomeado com meu CPF.

The screenshot shows an email inbox with a highlighted message from 'GOV-BR - ImportanteG0CpaEX9Et <ellis.lily7647@gmail.com>'. The subject line is 'Ultimo aviso - verifiquePIZIXmuZW1p2'. A red circle with the number 1 points to the recipient's name 'Flávio'. Another red circle with the number 2 points to the sender's name 'GOV-BR'. A red circle with the number 3 points to the text 'Notamos que ainda não solicitou o valor disponível em seu CPF.'. A red circle with the number 4 points to the deadline 'concluir até 16/02/2024'. The email body also contains 'Prezado(a) FLAVIO' and instructions to follow the attached PDF. At the bottom, there are buttons for 'Não sei do que se trata.', 'Feito.', 'Imprimir.', 'Responder', and 'Encaminhar'.

Sinais de phishing

1) E-mail não oficial

2) Autoridade

3) Oportunidade de lucro

4) Senso de urgência

A análise inicial do arquivo PDF e da URL indicada no documento, realizada através do VirusTotal, não identificou indícios de malware conhecidos.

The screenshot shows the VirusTotal analysis interface for the file 'pdf_36931533886_kchklq09.pdf'. The results indicate that 0 security vendors flagged the file as malicious, while 1 sandbox flagged it as malicious. The file hash is 'c9946ecc89d270d2f3c0cc7d174d115d68c52cec747e53e2713a2c5797d3271'. The file size is 47.89 KB and was analyzed a moment ago. There are buttons for 'Reanalyze', 'Similar', 'More', and a PDF icon.

No entanto, a investigação subsequente revelou um esquema de phishing bem elaborado:

Ultimo aviso - verifiquePIZIXmuZW1p2

GI GOV-BR - ImportanteG0CpaEX9Et <ellis.lily7647@gmail.com>
Para: Você Qua, 14/02/2024 12:45

pdf_...kchkLq09... 48 KB

Prezado(a) FLAVIO

Notamos que ainda não tem seu CPF.

Para realizar agora mesmo, anexo.

É fundamental concluir até 16/02/2024.

Protocolo: 27590165

Não sei do que se trata. Feito. Ir

Responder Encaminhar

 GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Você ainda não resgatou o valor de R\$ 2.284,72 do Governo Federal.

O prazo para efetuar o resgate é até 16/02/2024

Solicitamos que acesse agora mesmo para verificar e confirmar seus dados

[CLICANDO AQUI](#)

O documento PDF sugere que há valores a receber do Governo. Há um link para que o suposto resgate possa ser feito até 16/02/2024 (48h da data de recebimento).

O link no documento PDF é:

[https\[:\]//14022024433343\[.\]gatewaypagamentos\[.\]site/?cpf=xxxxxxxxxxxx](https://14022024433343.gatewaypagamentos.site/?cpf=xxxxxxxxxxxx)
IP: 172.67.144.35

A análise em sandbox retornou as seguintes informações:

- O site entrou em contato com 2 IPs em 2 países através de 6 domínios para realizar 3 transações HTTP.
- O principal IP é 172.67.144.35, localizado nos EUA e pertence ao iCloud Private Relay / Cloudflare / Cloudflare Warp / CLOUDFLARE-EU / CLOUDFLARENED, EUA.
- O domínio principal é 14022024433343.gatewaypagamentos.site. Registro DNS A atual: 172.67.144.35 (AS13335)

Temos um redirecionamento do primeiro domínio para um outro endereço com um iframe do site falso para uma página oficial do governo, aparentemente comprometida:

The screenshot shows a browser developer tools Network tab with the Headers tab selected. A request for '?cpf=...' is shown, which has been redirected (Status Code: 301 Moved Permanently) to the URL 'https://portais.sdr.sp.gov.br/xmlrpc.php?cpf=...'. The response headers include Cache-Control: max-age=3600, Cf-Ray: 8557bee3ba95a492-GRU, Date: Wed, 14 Feb 2024 19:33:56 GMT, Expires: Wed, 14 Feb 2024 20:33:56 GMT, Location: https://portais.sdr.sp.gov.br/xmlrpc.php?cpf=..., Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}, and Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?..."}].

Name	Headers	Payload	Preview	Response	Initiator	Timing
?cpf=...	Request URL: https://14022024433343.gatewaypagamentos.site/?cpf=... Request Method: GET Status Code: 301 Moved Permanently Remote Address: 104.21.55.25:443 Referrer Policy: strict-origin-when-cross-origin					
xmlrpc.php?cpf=...	Cache-Control: max-age=3600 Cf-Ray: 8557bee3ba95a492-GRU Date: Wed, 14 Feb 2024 19:33:56 GMT Expires: Wed, 14 Feb 2024 20:33:56 GMT Location: https://portais.sdr.sp.gov.br/xmlrpc.php?cpf=... Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?..."}]}					
govbr?cpf=...						
_ENV.js						
85a3fdb148fb7ccf.css						
webpack-469e484a5...						
framework-7d3b60c...						
main-a16ff636940b...						
_app-52b288c856ec...						
18-93559bfda4d488...						
823-b70e4dd60223...						
%5B%5B...publicId%...						
_buildManifest.js						
_ssgManifest.js						
favicon.ico						
426.bbdbaa83e094e...						

https[:]//14022024433343[.]gatewaypagamentos[.]site/?cpf=xxxxxxxxxxxx
IP: 104.21.55.25:443

Redirecionado para:

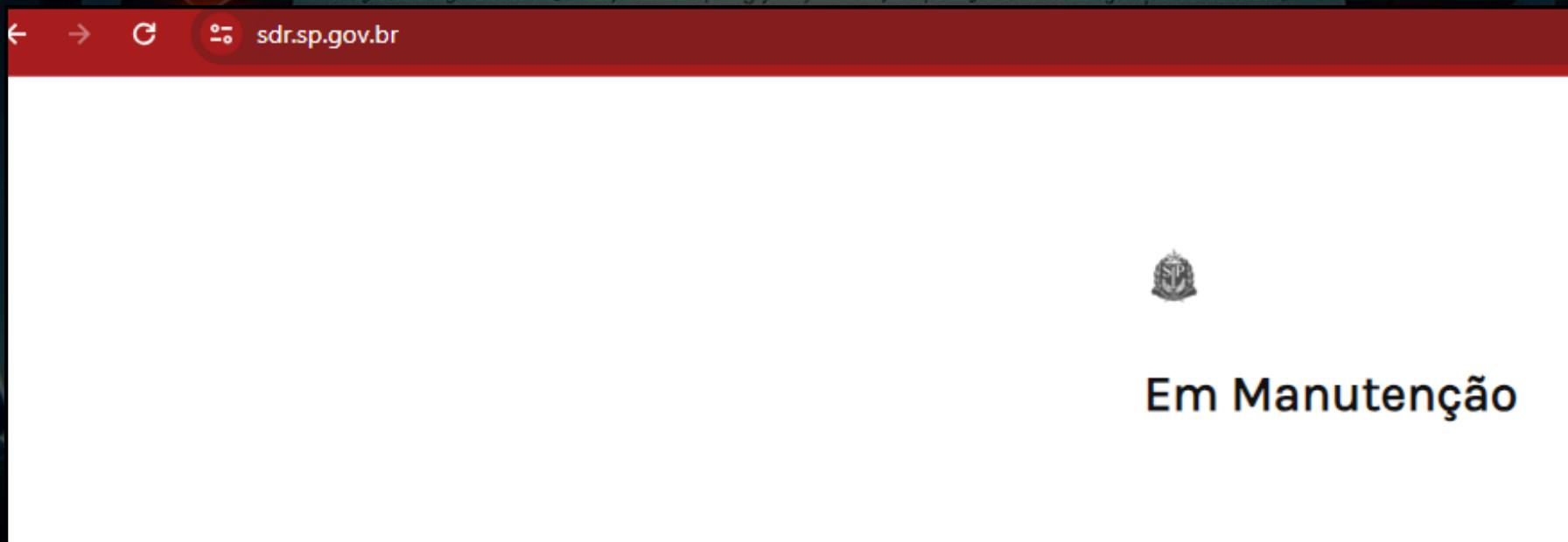
https://portais.sdr.sp.gov.br/xmlrpc.php?cpf=xxxxxxxxxxxx
IP: 200.144.31.50:443



Secretaria de Desenvolvimento Regional

24/03/2014

O site em questão é da **Secretaria de Desenvolvimento Regional do Estado de São Paulo**, e encontra-se indisponível com a mensagem “Em manutenção”:



Não encontrei registros ou notícias de ataque, nem anúncios oficiais sobre qual seria a natureza da manutenção, tampouco sobre os problemas encontrados nos sites oficiais.

Como é possível observar, o link é customizado com o CPF da vítima:

The screenshot shows a web-based chat interface. At the top, the URL is `portais.sdr.sp.gov.br/xmlrpc.php?cpf=[REDACTED]`. The page has a red header bar. Below it, there's a logo for "GOV.BR Atendimento" and a decorative horizontal bar with colored segments (yellow, red, green, blue, grey). A message from the system states: "O Sistema de Valores a Receber (SVR) é um serviço do Banco Central no qual você pode consultar se você, sua empresa ou pessoa falecida tem dinheiro esquecido em algum banco, consórcio ou outra instituição e, caso tenha, saber como solicitar o valor." The chat window shows the following messages:

- Luana entrou no chat!
- Olá, me chamo **Luana** sou assistente virtual do Gov.br.
- Aguarde, estou verificando seus dados...
- Pra sua segurança, **Gov.br** possui regras de validação de dados e estratégias de prevenção de fraudes.
- Olá **Reinor**, tudo certo!
- Antes de prosseguirmos, confirme se seus dados estão corretos:

Below this, there are fields for personal information:

Nome: Reinor [REDACTED]
Identificação (CPF): [REDACTED]
Nascimento: [REDACTED]
Sexo: Masculino

At the bottom right of the chat area are two buttons: "Confirmar" and "Não".

Alterando o valor do CPF para qualquer outro número ele retorna resultados em branco, porém, se usarmos um CPF válido, ele consulta alguma base e retorna as informações daquele CPF, sugerindo o acesso a bases de dados comprometidas.

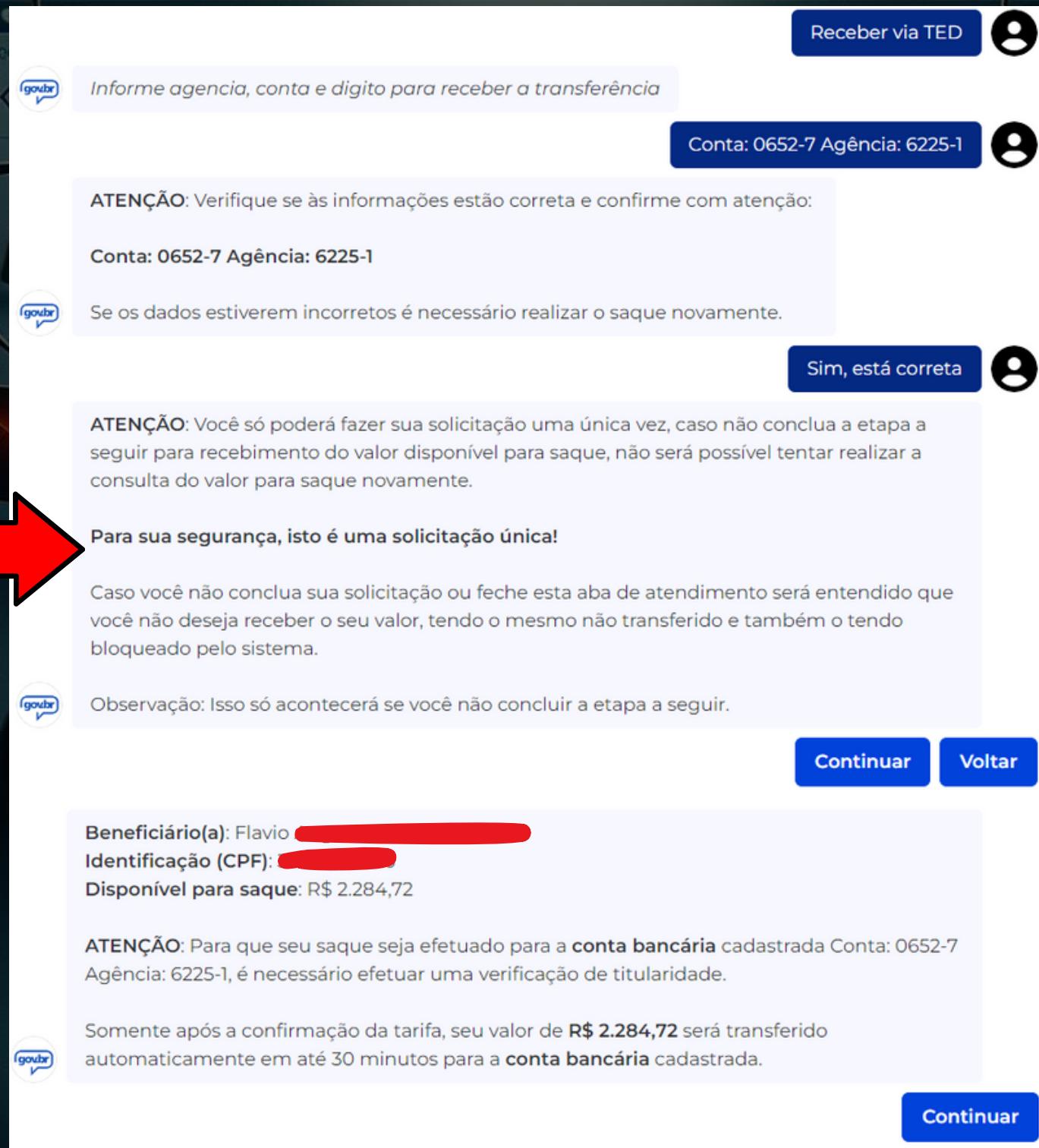
Seguindo as instruções no site falso, depois da confirmação de dados pessoais, o próximo passo seria a escolha de como receber o pagamento, Pix ou TED:

The screenshot shows a web page from a fake government portal (portais.sdr.sp.gov.br/xmlrpc.php?cpf=REDACTED). The page displays personal information (Nome: Flávio, Identificação (CPF): REDACTED, Nascimento: REDACTED, Sexo: Masculino) and a message confirming the amount available for withdrawal (R\$ 2.284,72). It asks if the user wants to withdraw now and provides two options: 'Receber via PIX' and 'Receber via TED'. A browser's developer tools Network tab is overlaid on the page, showing a POST request to <https://app.gatewaypagamentos.site/api/v1/sessions/clsm8ghg7bmc7ox0fy50ebmmo/continueChat> with a status of 200 OK.

Para TED: é solicitado input de agência e conta, e feita uma validação falsa dos dados. Nenhuma comunicação ocorre nesse momento.

Para Pix: é solicitada a chave para onde a suposta transferência seria feita.

Em vários momentos podemos observar o princípio de influência de urgência sendo utilizado:



O golpe consiste na etapa de “verificação de titularidade”

A suposta verificação de titularidade seria feita nesta última instrução: o pagamento de uma guia. Uma tarifa de R\$ 68,47 calculada sobre os valores a receber:

Phishiim 24/03/2014

GUIA DE PAGAMENTO GERADA COM SUCESSO!

O cálculo do valor total da tarifa é feito sobre o valor que você tem disponível para receber (R\$ 2.284,72).

Valor referente a verificação de titularidade da conta bancária

Total da tarifa: R\$ 68,47

Dados do titular:
Beneficiário(a): Flávio [REDACTED]
Mãe: [REDACTED]
Nascimento: [REDACTED]
Identificação (CPF): [REDACTED]

Após o pagamento da tarifa, em até 30 minutos você receberá o valor total de R\$ 2.284,72 na sua conta bancária

O valor é usado apenas para **verificar** sua conta bancária, realize a transferência utilizando uma conta em seu CPF.

Confirmar titularidade e finalizar o saque!

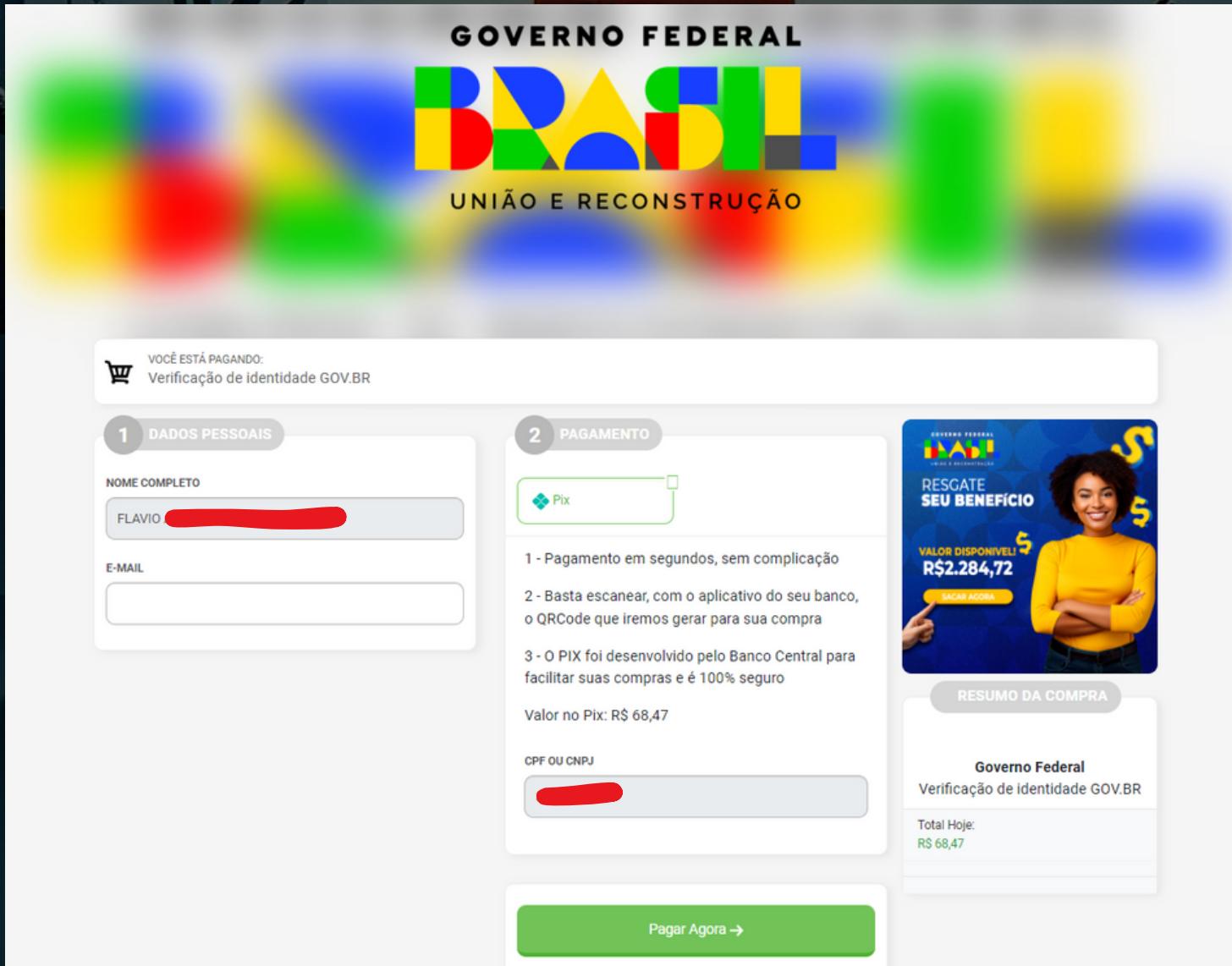
Você será redirecionado(a) para a página de pagamento da tarifa

Caso não efetue o pagamento e saia do site, você perderá todo o dinheiro que está disponível para você.

PREENCHA OS DADOS E EFETUE O PAGAMENTO...

Mais uma vez, uma mensagem reforçando que o usuário deve fazer o pagamento e não sair do site, caso contrário, teria os valores bloqueados.

Dessa vez um novo redirecionamento é feito para pagamento da taxa via Pix. Para aumentar a credibilidade, a URL do site também mostra o CPF e o nome completo da vítima:



O serviço é intermediado pela empresa e também vítima: perfectpay.com.br

Ao selecionar o botão “Pagar Agora” é gerado uma chave Pix Copia e Cola e também um QRCode

Pedido: PPCPMTB5D123124

Valor: R\$ 68,47

1. Copie o código abaixo
2. Cole no seu banco na função
PIX Copia e Cola

00020101021226830014br.gov.bcb.pix2561api.pagseguro.com/pix/v2/80B

Você também pode tentar lendo o nosso QRCode?
1. Abra o aplicativo do seu banco no celular
2. Selecione a opção de pagar com Pix / escanear QR code



Atenção! Verifique os dados enviados:

Com a confirmação do seu pagamento, garantimos um processo eficiente de estorno automático. Priorizamos sua segurança e transparência em cada transação. Estamos aqui para proporcionar uma experiência confiável e descomplicada. Agradecemos a confiança em nossos serviços.

Dados Pessoais:

Nome: FLAVIO [REDACTED]

CPF/CNPJ: [REDACTED]

24/03/2014

pagar QR Code
revise as informações

para

ABMEX PAGAMENTOS INTELIGENTES LTDA
PAGSEGURO INTERNET IP S.A.
58330c46-86dd-4489-a71e-1dcaac3370a8
39.676.137/0001-04

valor

R\$ 68,47

detalhes do pagamento

identificador
20240214174200434479506912996077

valor original
R\$ 68,47

data de expiração
15/02/2024 às 23h59m59s

data de pagamento
hoje, 14/02/2024

saldo em conta

exibir

continuar

Conclusões

Gostaria de ressaltar que todas as denúncias relacionadas a esta campanha de phishing foram devidamente encaminhadas aos serviços envolvidos, incluindo a Secretaria de Desenvolvimento Regional do Estado de São Paulo e os respectivos serviços de CSIRT.

Além disso, a página fraudulenta foi reportada em listas de bloqueio e feeds de inteligência de renomadas instituições, reforçando meu compromisso com a segurança digital e a proteção coletiva contra ameaças cibernéticas.

Compartilhe esse post para que outras pessoas se informem e não sejam vítimas!

Juntos, estamos fortalecendo nossas defesas e promovendo um ambiente digital mais seguro para todos.

@OFLAVIOC

G O S T O U

DESTE CONTEÚDO?



CURTA



COMENTE



COMPARTILHE



SALVE

SEGURANÇA
DESCOMPLICADA