

# Site report for www.fernandopedroza.rn.gov.br



#### Netcraft Extension

Home
Download Now!
Report a Phish
Site Report
Top Reporters
Incentives for reporters
Phishiest TLDs
Phishiest Countries
Phishiest Hosters
Phishiest Certificate Authorities
Phishing Map
Takedown Map
Most Popular Websites
Branded Extensions

# Phishing & Fraud

Tell a Friend

Phishing Site Feed
Hosting Phishing Alerts
SSL CA Phishing Alerts
Protection for TLDs against
Phishing and Malware
Deceptive Domain Score
Bank Fraud Detection
Phishing Site Countermeasures

## **Extension Support**

FAQ	
Glossary	
Contact Us	
Report a Bug	
Report a Bug	

### Tutorials

Installing the Extension	
Using the Extension	
Getting the Most	
Reporting a Phish	

# About Netcraft

Netcraft Home
About Netcraft
Website Terms of Use
Phishing Site Feed
Security Services
Contact Us

Lookup anoth	er URL:	Sh	are:	
Enter a U	er a URL here			
Backg	round			
Site title	Not Acceptable!	Date first seen	June 2006	
Site rank		Primary Ianguage	English	
Description	Not Present			
Keywords	Not Present			
Netcraft Risk Rating [FAQ]	1/10			

#### Network

Site	https://www.fernandopedroza.rn.gov.br	Netblock Owner	WEBSITEWELCOME.COM
Domain	rn.gov.br	Nameserver	ns1.rn.gov.br
IP address	108.179.252.149 (VirusTotal)	DNS admin	suporte@rn.gov.br
IPv6 address	Not Present	Reverse DNS	srv166-ip05.prodns.com.br
Domain registrar	nic.br	Nameserver organisation	whois.nic.br
Organisation	Governo do Estado do Rio Grande do Norte, Brazil	Hosting company	unknown
Top Level Domain	Brazil (.gov.br)	DNS Security Extensions	unknown
Hosting country	<b>■</b> US		

## SSL/TLS

SSLv3/POODLE	This site does not support the SSL version 3 protocol.					
	More information about SSL version 3 and the POOL	More information about SSL version 3 and the POODLE vulnerability.				
Heartbleed	The site did not offer the Heartbeat T	LS extension	prior to the Heartbleed			
	disclosure, and so was not exploitable	e.				
	This test does not exploit the Heartbleed vulnerability information about Heartbleed detection.	This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection.				
Assurance	Domain validation	Domain validation				
Organisation	Not Present Common fernandopedroza.rn.gov.br name					
State	Not Present	Country	Not Present			
Organisational unit	Not Present	Subject Alternative Name	autodiscover.fernandopedroza.rn.gov.br, cpanel.fernandopedroza.rn.gov.br, fernandopedroza.rn.gov.br, mail.fernandopedroza.rn.gov.br, webdisk.fernandopedroza.rn.gov.br, webmail.fernandopedroza.rn.gov.br, whm.fernandopedroza.rn.gov.br, www.fernandopedroza.rn.gov.br			

Not   Present   Not   Prese	Site report for www.fernandopedroza.rn.gov.br					
Protocol version	Validity period	·				
Version   Version   Version   Version   Version number	Server	Apache		•	rsaEncryption	
Check         algorithm           Serial number         0x047d16al7/5e0096351b91e376620396cb1         Cipher Cipher         ECDHE-RSA-AES128-GCM-SHA256           Version number         0x02         Perfect Forward Secrecy         Yes           Next Protocol Negotiation         Not Present TLS encrypt Session ticket         Supported TLS encrypt Intention formats, RFC5746         RFC4366 server name, RFC5746           Issuing organisation         Let's Encrypt Session ticket         Issuer country Issuer Common name         Let's Encrypt Authority X3           Issuer unit         Not Present Session ticket         Issuer Not Present Issuer State         Not Present Session ticket           Certificate Revocation Lists         Not Present Session Se		TLSv1.2		•	2048	
Next Protocol Negotiation   Not Present   Supported Secrecy   Supported Secrecy   RFC4366 server name, RFC5746   renegotiation   TLS renegotiation info, RFC4492 EC point Extensions   Supported Extensions   Supported Secrecy   RFC4366 server name, RFC5746   renegotiation info, RFC4492 EC point Extensions   Supported Secrecy   Supported Secrecy   Supported Secrecy   RFC4366 server name, RFC5746   renegotiation info, RFC4492 EC point Extensions   Supported Secrecy   Supported Secrec		ok		•	sha256WithRSA	AEncryption
Next Protocol Negotiation	Serial number	0x047d16af	7f5e0096351b91e376620396cb1c	Cipher	ECDHE-RSA-A	ES128-GCM-SHA256
Negotiation    TLS	Version number	0x02		Forward	Yes	
common name         Issuer unit       Not Present location         Issuer country       US       Issuer location         Lists       Certificate state       Not Present state         Revocation Lists       Certificate Public Key       Hash         OCSP servers       http://ocsp.int-x3.letsencrypt.org - 100% uptime in the past 24 hours         OCSP stapling response       Not response received         Certificate Signed Certificate Timestamps (SCTs)         Timestamp       Signature Verification         Verification         Certificate       DigiCert Yeti 2019       2019-07-04       Success         Certificate       Gignature Verification         Verification		Not Present		TLS	renegotiation inf	o, RFC4492 EC point
Issuer country	_	common		nthority X3		
Certificate Revocation Lists  Public Key Hash  OCSP servers OCSP stapling response  Certificate Signed Certificate Timestamps (SCTs)  transparency  Source Log Log Hall-ribo6UAJ6IYbt jud1D77n/nSI+6SPKJMBnd3x2/4= O2:47:42  Certificate Google Icarus  State  Certificate rt0G590KLwWYjklBxXeik/EDYe8  Hash  Certificate rt0G590KLwWYjklBxXeik/EDYe8  Hash  Timestamp Signature Verification  Signature Verification  Success	Issuer unit	Not Present			Not Present	
Revocation Lists  Public Key Hash  OCSP servers OCSP stapling response  Certificate transparency  Source  Certificate  DigiCert Yeti 2019 4mlLribo6UAJ6IYbt jub1D7n/nSI+6SPKJMBnd3x2/4=  Certificate C	Issuer country	US			Not Present	
Hash  OCSP servers http://ocsp.int-x3.letsencrypt.org - 100% uptime in the past 24 hours  OCSP stapling response  Certificate Signed Certificate Timestamps (SCTs)  transparency  Source Log Timestamp Signature Verification  Certificate DigiCert Yeti 2019 2019-07-04 Success  Certificate Google Icarus 2019-07-04 Success	Revocation	Not Present		,		jklBxXeik/EDYe8
OCSP stapling response  Certificate transparency  Source Log  Timestamp Signature Verification  Certificate DigiCert Yeti 2019 4mlLribo6UAJ6IYbt juD1D7n/nSI+6SPKJMBnd3x2/4= 02:47:42  Certificate Google Icarus 2019-07-04 Success		e23cedc43be58cdbda7bc99dc70bb9adbd19851bc0fc83d0393bd493a3ec3022			2	
response  Certificate transparency  Source Log Timestamp Signature Verification  Certificate DigiCert Yeti 2019 4mlLribo6UAJ6IYbtjuD1D7n/nSI+6SPKJMBnd3x2/4= Certificate Google Icarus  Certificate Signature Verification Success	OCSP servers	http://ocsp.int-x3.letsencrypt.org - 100% uptime in the past 24 hours			'	
transparency Source Log Timestamp Signature Verification  Certificate DigiCert Yeti 2019 4mlLribo6UAJ6IYbtjuD1D7n/nSI+6SPKJMBnd3x2/4= 02:47:42  Certificate Google Icarus 2019-07-04 Success		No response received				
Source Log Timestamp Signature Verification  Certificate DigiCert Yeti 2019 4mlLribo6UAJ6IYbtjuD1D7n/nSI+6SPKJMBnd3x2/4= 02:47:42  Certificate Google Icarus 2019-07-04 Success		Signed Certificate Timestamps (SCTs)				
4mlLribo6UAJ6IYbtjuD1D7n/nSI+6SPKJMBnd3x2/4= 02:47:42  Certificate Google Icarus 2019-07-04 Success	transparency	Source	Log		Timestamp	· ·
		Certificate	9	MBnd3x2/4=		Success
		Certificate		z05UVH9Hg=		Success

#### **SSL Certificate Chain**

# **Hosting History**

Netblock owner	IP address	os	Web server	Last seen Refresh
WEBSITEWELCOME.COM 5005 Mitchelldale Suite 100 Houston TX US 77092	108.179.252.149	Linux	Apache	12- Jul- 2019

# **Sender Policy Framework**

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Qualifier	Mechanism	Argument
+ (Pass)	a	
+ (Pass)	mx	
+ (Pass)	include	websitewelcome.com
~ (SoftFail)	all	

Modifiers extend the functionality of SPF records. The most common one is the redirect which indicates another host contains the SPF record being searched for.

Modifier	Argument
----------	----------

#### **DMARC**

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

This host does not have a DMARC record.

#### **Web Trackers**

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

No known trackers were identified.

COPYRIGHT © NETCRAFT LTD. 2019