YesGov

GOVERNMENT DOMAIN SECURITY REPORT

orangecountygov.com

Town of Palm Tree, New York · Population 41,857

Checked September 22, 2026 at 10:16 PM UTC · Check ID d616193e-2784-4987-9ecd-e15ae3a93a83

F

3 of 16 checks passed **Residents are exposed**

Basic protections recommended by CISA are missing. Each fix below is a standard setting, listed in order of risk to residents.



● 3 passed ● 1 needs attention ● 12 missing

Website	Email	DNS and domain
0 of 8	2 of 5	1 of 3

Not on a .gov domain

orangecountygov.com is not a .gov address. Anyone can register a look-alike .com or .org, so residents cannot tell from the address alone that this is the official site.

CISA and DHS advise that .gov is a requirement for secure government, trusted communication and public trust. Every day on a non-.gov address is a day residents can be fooled by an impostor site or email.

What to fix first

In order of risk to residents. Each is a one-time setting that then needs to be watched.

1. **Fix the HTTPS certificate** — HIGH RISK
   Browsers warn residents that the site is not secure, and anything they type, such as a payment or a permit form, can be read by others on the same network.
   Fixed by: Your web host

2. **Send every visitor to HTTPS** — HIGH RISK
   Residents who type the plain address or follow an old link get an unencrypted page that can be read or changed on public Wi-Fi.
   Fixed by: Your web host

3. **Repair the certificate** — HIGH RISK
   The certificate chain, signature or name does not check out. That teaches residents to click past browser warnings, which is exactly what fake sites rely on.
   Fixed by: Your web host

4 **Repair the SPF record** — HIGH RISK
Receiving mail systems cannot tell the agency's real email from a forgery, so residents can receive fake notices in its name.
Fixed by: Your email or DNS provider

5 **Turn on DNSSEC** — HIGH RISK
DNS answers are not signed. A forged answer can send residents to a fake payment page, or redirect the agency's email, with no visible sign.
Fixed by: Your DNS host and domain registrar

6 **Turn on HSTS** — MEDIUM
On public Wi-Fi, a resident's visit can be pushed to an unencrypted copy of the site.
Fixed by: Your web host

7 **Require encrypted mail delivery (MTA-STS)** — MEDIUM
Mail sent to agency staff can be forced onto an unencrypted connection and read in transit.
Fixed by: Your email or DNS provider

8 **Turn on mail encryption reports (TLS-RPT)** — MEDIUM
Nobody is told when encrypted mail delivery to the agency fails or is tampered with.
Fixed by: Your DNS provider

9 **Add framing protection** — MEDIUM
The site can be hidden inside a hostile page to trick residents into clicking buttons they cannot see.
Fixed by: Your web host

10 **Add a CAA record** — MEDIUM
Any certificate authority in the world may issue a certificate for this domain, which makes impersonating the site easier.
Fixed by: Your DNS provider

11 **Add file type protection** — MEDIUM
Browsers may guess file types, which can let an uploaded file run as code against visitors.
Fixed by: Your web host

12 **Publish a security contact (security.txt)** — MEDIUM
People who find a security problem have no standard way to tell the agency before it is misused.
Fixed by: Your web host

13 **Add IPv6 support** — MEDIUM
Networks that only use IPv6, including some mobile carriers, cannot reach the site directly.
Fixed by: Your web host

All results in detail

Every record and value we saw, grouped by area. Written for your IT team, readable by anyone.

Website — 0 of 8 passed

HTTPS certificate — MISSING

What this means: Browsers warn residents that the site is not secure, and anything they type, such as a payment or a permit form, can be read by others on the same network.

How to fix: Install a certificate from a trusted authority (Let's Encrypt is free) and set it to renew automatically. (Your web host)

Redirect to HTTPS — MISSING

HTTPS available	No
Plain address redirects to HTTPS	No

What this means: Residents who type the plain address or follow an old link get an unencrypted page that can be read or changed on public Wi-Fi.

How to fix: Redirect every http:// request to https:// with a permanent (301) redirect. (Your web host)

HSTS — MISSING

HSTS header	Not sent

What this means: On public Wi-Fi, a resident's visit can be pushed to an unencrypted copy of the site.

How to fix: Send the Strict-Transport-Security header with a max-age of at least one year. (Your web host)

Certificate trust and match — MISSING

Trusted chain	No
Strong public key	No
Valid signature	No
Name matches domain	No

What this means: The certificate chain, signature or name does not check out. That teaches residents to click past browser warnings, which is exactly what fake sites rely on.

How to fix: Reissue the certificate for this exact domain and install the full certificate chain. (Your web host)

CAA record — MISSING

CAA record	Not found

What this means: Any certificate authority in the world may issue a certificate for this domain, which makes impersonating the site easier.

How to fix: Publish a CAA record naming the authority you use, for example 0 issue "letsencrypt.org". (Your DNS provider)

Framing protection — MISSING

X-Frame-Options	Not sent

What this means: The site can be hidden inside a hostile page to trick residents into clicking buttons they cannot see.

How to fix: Send the header X-Frame-Options: SAMEORIGIN, or a Content-Security-Policy with frame-ancestors 'self'. (Your web host)

File type protection — MISSING

X-Content-Type-Options	Not sent

What this means: Browsers may guess file types, which can let an uploaded file run as code against visitors.

How to fix: Send the header X-Content-Type-Options: nosniff. (Your web host)

Security contact (security.txt) — MISSING

/.well-known/security.txt	Not found

What this means: People who find a security problem have no standard way to tell the agency before it is misused.

How to fix: Publish /.well-known/security.txt with a contact address and an expiry date. (Your web host)

Email — 2 of 5 passed

SPF — NEEDS ATTENTION

Record	`v=spf1 ip4:74.43.125.0/24 include:_spf_useast2.prod.hydra.sophos.com include:spf.protection.outlook.com include:spf.mandrillapp.com include:_pm.spf.spectrumretailnet.com include:_spf.fortimailcloud.com ~all`
Ending	Soft fail (~all)

What this means: Receiving mail systems cannot tell the agency's real email from a forgery, so residents can receive fake notices in its name.

How to fix: Publish one TXT record that lists every service sending mail for the domain and ends in -all. (Your email or DNS provider)

DKIM — PASS

Selectors found	k2, mandrill

DMARC — PASS

Policy	quarantine
Record	`v=DMARC1;  p=quarantine`

MTA-STS — MISSING

DNS record	Not found
Policy file	Not found
Enforced	No

What this means: Mail sent to agency staff can be forced onto an unencrypted connection and read in transit.

How to fix: Publish an _mta-sts TXT record and a policy file at mta-sts.(domain)/.well-known/mta-sts.txt. (Your email or DNS provider)

TLS-RPT — MISSING

TLS-RPT record	Not found

What this means: Nobody is told when encrypted mail delivery to the agency fails or is tampered with.

How to fix: Publish a TXT record at _smtp._tls with an address to receive reports. (Your DNS provider)

DNS and domain 1 of 3 passed

DNSSEC MISSING

Zone signed	No
Result	No DNSSEC records found. DNSSEC may not be enabled for this domain.

What this means: DNS answers are not signed. A forged answer can send residents to a fake payment page, or redirect the agency's email, with no visible sign.

How to fix: Turn on DNSSEC signing at the DNS host, then add the DS record at the registrar. (Your DNS host and domain registrar)

IPv6 MISSING

Website reachable over IPv6	No
Name servers reachable over IPv6	Yes

What this means: Networks that only use IPv6, including some mobile carriers, cannot reach the site directly.

How to fix: Ask the host for an IPv6 address and publish an AAAA record for the site. (Your web host)

RPKI route protection PASS

Website route signed	Yes
Website route valid	Yes
Name server route valid	Yes

.gov domain NOT SCORED

Ends in .gov	No

What this means: Anyone can register a look-alike .com or .org, so residents have no way to confirm this is the official site. Every .gov request is verified by CISA.

Hosting and platform

Informational, not scored

Website server	16.15.254.163
Mail server	orangecountygov-com-1.fortimailcloud.com
Website server reputation	Not on abuse lists
Mail server blocklists	Not listed
WordPress	Not detected
Email addresses published on the site	0
Broken links found	0
Referrer policy header	No

Progress over time

Checks passed at each scan, oldest to newest. Highest possible is 16.



If these basics were missed, what else has been missed?

These are published CISA standards that any IT department or provider can check in seconds. YesGov can fix all 13 in under 24 hours, re-run this check to prove it, and keep watching every day. The move to .gov takes 1 to 2 weeks because CISA verifies each request; security fixes on the current domain do not wait for it.

yesgov.com/contact · (888) 777-0017 · info@yesgov.com

How we check

We only check settings that any computer on the internet can see: DNS records, certificates, web headers and mail policies. We never log in to, scan or probe any agency system. The 16 checks build on CISA Binding Operational Directive 18-01 and other published internet standards. Full method: yesgov.com/open-data#how-we-grade.

Verify this report online

Scan the code or visit the address below to see these results, check the domain again and get alerts when anything changes.

https://yesgov.com/check/orangecountygov--com?check=d616193e-2784-4987-9ecd-e15ae3a93a83

YesGov PBC is a Public Benefit Corporation that works only with U.S. government agencies. 1639 Medical Center Parkway, Murfreesboro, TN 37129. This report reflects public settings at the time of the check and is not a full security audit.