YesGov

GOVERNMENT DOMAIN SECURITY REPORT

facebook.com

Checked July 15, 2026 at 11:26 PM UTC · Check ID d2327fcd-4f3e-485c-b20b-5ec94dd29d2a

B+

12 of 16 checks passed **Needs attention**

The basics are in place, but several standard protections are missing. The list below is in order of risk to residents.



12 passed · 2 need attention · 2 missing

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

Not on a .gov domain

facebook.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. **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

2. **Turn on DKIM signing** — HIGH RISK

   Outgoing mail is not signed, so receivers cannot confirm it came from the agency, and DMARC cannot be fully enforced.

   Fixed by: Your email provider

3. **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

4 **Enforce MTA-STS** MEDIUM

MTA-STS is set up but not enforced, so mail to agency staff can still be forced onto an unencrypted connection.

Fixed by: Your email or DNS provider

All results in detail

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

Website — 8 of 8 passed

HTTPS certificate — PASS

Issued by	**DigiCert Global G2 TLS RSA SHA256 2020 CA1**
Issued to	***.facebook.com**
Expires	**July 23, 2026 (8 days after this check)**
TLS version	**TLSv1.3**

Redirect to HTTPS — PASS

HTTPS available	**Yes**
Plain address redirects to HTTPS	**Yes**

HSTS — PASS

HSTS header	**Sent**
Max age	**15,552,000 seconds**
Includes subdomains	**No**

Certificate trust and match — PASS

Trusted chain	**Yes**
Strong public key	**Yes**
Valid signature	**Yes**
Name matches domain	**Yes**

CAA record — PASS

CAA record	**Found**
Authorities named	**Not captured in this scan**

Framing protection — PASS

X-Frame-Options	**DENY**

File type protection — PASS

X-Content-Type-Options	**nosniff**

Security contact (security.txt) PASS

/.well-known/security.txt	Found

Email 2 of 5 passed

SPF NEEDS ATTENTION

Record	`v=spf1 ip4:66.220.144.128/25 ip4:66.220.155.0/24 ip4:66.220.157.0/25 ip4:69.63.178.128/25 ip4:69.63.181.0/24 ip4:69.63.184.0/25`
Ending	Not strict

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 MISSING

Signing keys	Not found

What this means: Outgoing mail is not signed, so receivers cannot confirm it came from the agency, and DMARC cannot be fully enforced.

How to fix: Turn on DKIM in the mail service (Microsoft 365, Google Workspace and others) and publish the DNS records it gives you. (Your email provider)

DMARC PASS

Policy	reject
Reports sent to	a@dmarc.facebookmail.com
Record	`v=DMARC1; p=reject; rua=mailto:a@dmarc.facebookmail.com; ruf=mailto:fb-dmarc@datafeeds.phishlabs.com; pct=100`

MTA-STS NEEDS ATTENTION

DNS record	Found
Policy file	Found
Mode	testing
Enforced	No

What this means: MTA-STS is set up but not enforced, so mail to agency staff can still be forced onto an unencrypted connection.

How to fix: Fix any problems listed for the policy file, publish the _mta-sts TXT record, and set the policy mode to enforce. (Your email or DNS provider)

TLS-RPT PASS

Record	`v=TLSRPTv1;rua=mailto:sts-reports@facebookmail.com`

DNS and domain 2 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 — PASS

Website reachable over IPv6	Yes
Website IPv6 addresses	2a03:2880:f38a:1:face:b00c:0:25de
Name servers reachable over IPv6	Yes

RPKI route protection — PASS

Website route signed	Yes
Website route valid	Yes
Name server route valid	No

.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.

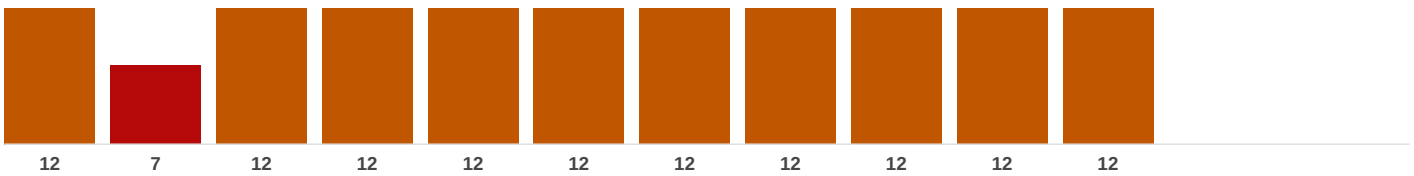
Hosting and platform

Informational, not scored

Website server	57.145.20.1
Mail server	smtpin.vvv.facebook.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 4 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/facebook--com?check=d2327fcd-4f3e-485c-b20b-5ec94dd29d2a

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.