Castle
TECHNOLOGY PARTNERS

ANNUAL SECURITY ANALYSIS

GULF COAST REGION | 1,000 BUSINESSES SCANNED

GULF COAST CYBERSECURITY INDEX

Mobile & Baldwin County, Alabama

CASTLE TECHNOLOGY PARTNERS

2026

ABOUT THIS REPORT

Who We Are & Why We Built This

Castle Technology Partners is a cybersecurity and managed IT team helping businesses reduce risk, improve reliability, and make stronger technology decisions with confidence.

We created the **Gulf Coast Cybersecurity Index** as a service project for our community so business owners can understand risk in plain language and act on the gaps that matter most.

WHAT WE ANALYZED

We reviewed **1,000 businesses** (500 in Mobile County and 500 in Baldwin County) using publicly observable indicators only. No private systems were accessed. Every data point used in this report is internet-facing information that can be seen externally.

SSL/TLS Encryption	If customer info sent through your website is protected.
SPF Record	If scammers can pretend to send email as your business.
DMARC Policy	If fake email attempts are only monitored or actively blocked.
Security Headers	If your site has key browser safety controls enabled.
Dark Web Exposure	If business-linked credentials appear in breach datasets.

WHY THIS MATTERS

Most attacks begin with email impersonation, exposed credentials, or missing web protections. This report helps prioritize the fixes that reduce real-world risk fastest.

Benchmark Method: Local metrics come from this 1,000-business scan. U.S. and Global values are directional reference baselines from public transparency and domain-security adoption reports.

KEY FINDINGS

Executive Summary

The data is clear: Gulf Coast businesses are significantly underprotected. Most businesses in this dataset still have multiple visible control gaps across email authentication, web hardening, and credential exposure. These are widespread patterns that attackers actively exploit.

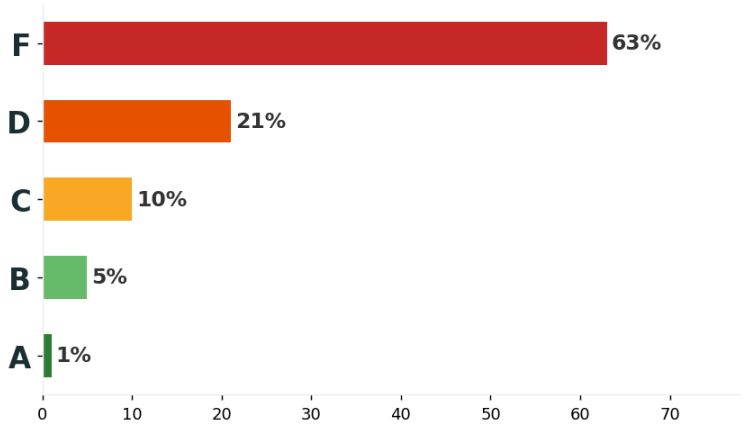
84%
SCORED D OR F

1%
SCORED A

23%
DARK WEB EXPOSURE

24%
NO DMARC

Overall Grade Distribution



Five Critical Findings

1. **Most businesses carry serious cybersecurity risk**
   84% of Gulf Coast businesses scored D or F — indicating multiple unaddressed vulnerabilities.

2. **Email fraud doors are wide open**
   24% have no DMARC policy. Anyone can impersonate their email domain.

3. **Top grades are extremely rare**
   Only 1% earned an A. The median score was 11/21.

4. **Dark web exposure is common**
   23% have credentials or data found in known breach databases.

5. **Basic protections are widely ignored**
   46% have zero web security headers — standard protections remain unconfigured.

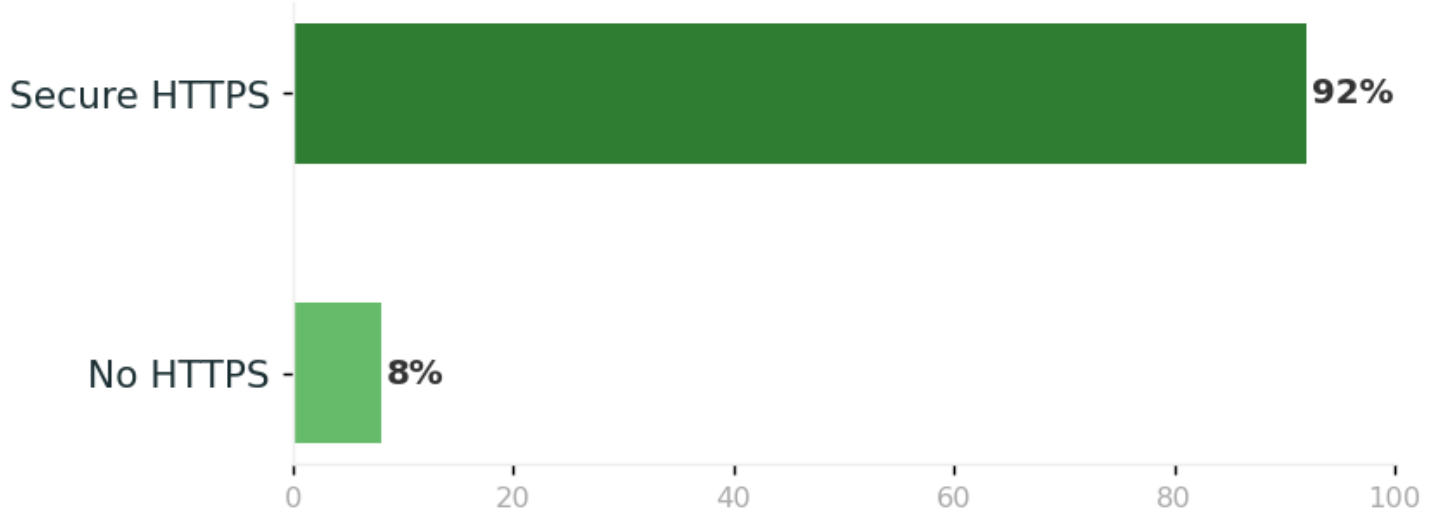
FINDING 1 OF 4

SSL/TLS Encryption

OVERALL
A

SSL/TLS protects website traffic in transit. When missing, browser warnings reduce trust and increase exposure risk. It also weakens customer confidence during key actions like contact forms, account logins, and payments. For businesses taking payments online, weak transport security increases both fraud and reputational risk.

Why it matters: Businesses accepting online payments over weakly protected web sessions face higher fraud, chargeback, and trust-loss risk after incidents.



No HTTPS
Unencrypted traffic and visible browser trust warnings.

Redirects to HTTPS
Improved state, but should enforce strict transport policy.

Secure HTTPS
Valid certificate. Traffic is encrypted and trusted.

Did you know? Outdated certificates and weak TLS configs are common indicators attackers look for first.

BENCHMARK SNAPSHOT
Local 92% | U.S. 95% | Global 93%

FINDING 2 OF 4

Email Authentication: SPF & DMARC

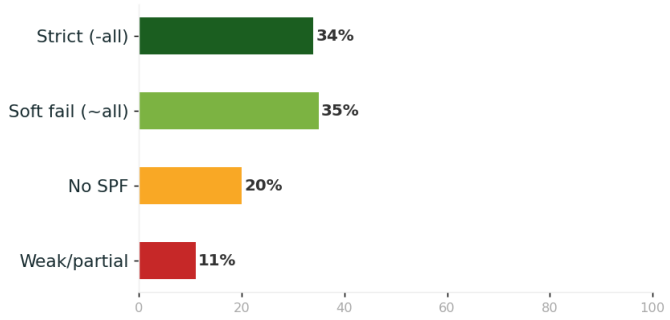
OVERALL
F

Without SPF and DMARC, anyone on the internet can send an email that appears to come from your domain. This is how business email compromise (BEC) and phishing attacks begin — and it remains one of the most common attack paths for businesses.

Did you know? In 2023, organizations reported about **$2.9 billion** in exposed losses tied to Business Email Compromise (BEC).

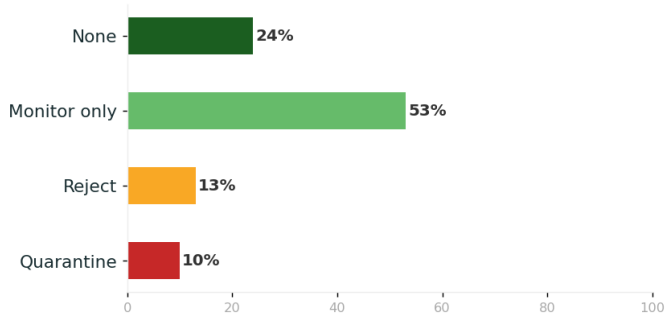
SPF — WHO CAN SEND ON YOUR BEHALF

SPF tells receiving mail servers which IP addresses are authorized to send email from your domain.



DMARC — ENFORCEMENT & REPORTING

DMARC tells receiving servers what to do when an email fails authentication and sends abuse reports.



20%
HAVE NO SPF RECORD
Anyone can send email claiming to be from their domain.

24%
HAVE NO DMARC
No visibility into impersonation and no automated enforcement.

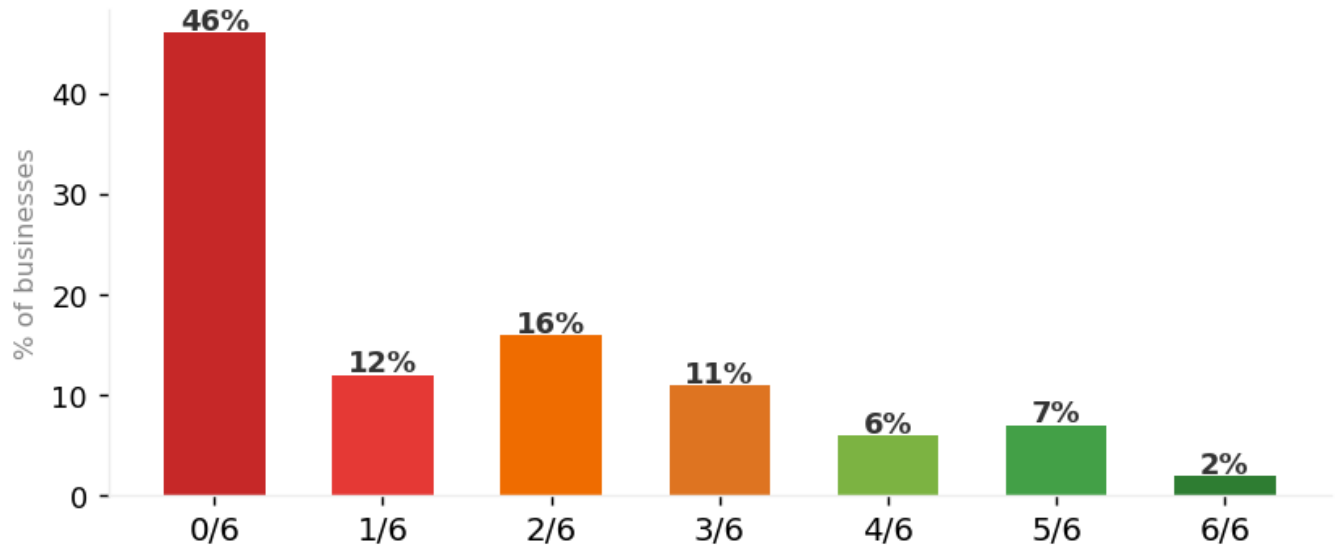
BENCHMARK SNAPSHOT
SPF: Local 34% / US 70% / Global 58%
DMARC: Local 23% / US 35% / Global 15%

FINDING 3 OF 4

Web Security Headers

OVERALL
F

Web security headers are browser-side guardrails that reduce common attack paths such as script injection and clickjacking. These controls are often overlooked because they are invisible to users, but attackers actively scan for their absence. Properly configured headers improve resilience without changing your site's user experience.



The 6 Critical Headers

`Content-Security-Policy`
Prevents cross-site scripting (XSS) and data injection attacks

`Strict-Transport-Security`
Enforces HTTPS; prevents protocol downgrade attacks

`X-Frame-Options`
Blocks clickjacking

`X-Content-Type-Options`
Prevents MIME-type sniffing attacks

`Referrer-Policy`
Controls what referrer data is shared

`Permissions-Policy`
Restricts browser feature access

46%
HAVE ZERO SECURITY HEADERS
Average across all businesses: 3/6.

BENCHMARK SNAPSHOT
Local 28% | U.S. 42% | Global 30%

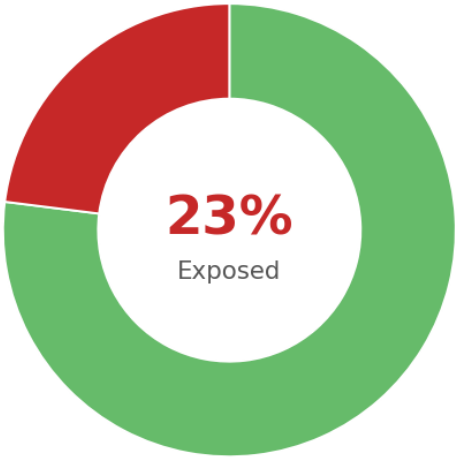
FINDING 4 OF 4

Dark Web Exposure

OVERALL
C

Dark web exposure means business-linked credentials have surfaced in breach ecosystems where attackers actively search for reusable access. Exposure does not guarantee a breach, but it materially increases the chance of phishing success, account takeover, and follow-on intrusion.

Did you know? Over 90% of cyberattacks begin with phishing or stolen credentials.



WHY IT MATTERS

Credential Stuffing
Exposed passwords are tested across banking, email, and cloud platforms automatically by bots.

Business Email Compromise
Access to one email account can enable vendor impersonation and payment fraud.

Ransomware Entry Point
A single compromised credential is a common initial foothold in ransomware incidents.

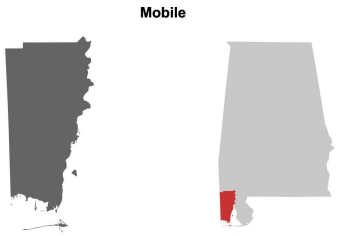
BENCHMARK SNAPSHOT
Local 23% | U.S. 28% | Global 35%

REGIONAL ANALYSIS

County by County Comparison

Cybersecurity posture varies across the Gulf Coast region. This comparison uses an even sample of 500 businesses per county and shows how both counties perform against regional and external benchmarks.

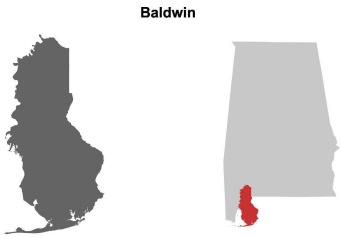
MOBILE COUNTY



F

11.9/21

BALDWIN COUNTY



F

10.6/21

HOW WE COMPARE

Mobile and Baldwin counties show similar overall cybersecurity maturity, with both landing in high-risk territory. Mobile holds a slight edge in average score, but the difference is narrow and does not change the overall risk profile. In both counties, the same patterns appear: weak email authentication enforcement, inconsistent web security headers, and meaningful credential exposure risk. The data suggests this is a regional control-gap issue rather than a single-county outlier.

WHY THIS MATTERS

Because these weaknesses are regional, incidents can ripple across local vendor relationships, shared service providers, and client trust networks. Improving control maturity in one business helps, but raising standards across both counties strengthens the entire Gulf Coast business ecosystem.

MOBILE COUNTY

Businesses Analyzed	500
Average Score	11.9 / 21
Overall Grade	F

BALDWIN COUNTY

Businesses Analyzed	500
Average Score	10.6 / 21
Overall Grade	F

INDUSTRY ANALYSIS

Industry Performance Snapshot

Industry differences exist, but the broader signal is consistent: many sectors remain below strong security maturity. When this happens, threat actors can scale attacks by repeating the same phishing, impersonation, and credential-abuse playbooks across multiple organizations in the same vertical.

ALL INDUSTRIES (RANKED)

Legal	13.3/21	D
Technology	13.2/21	D
Healthcare	12.5/21	F
Education	12.3/21	F
Manufacturing	12.2/21	F
Other	12.1/21	F
Marketing & Media	11.8/21	F
Finance & Insurance	11.7/21	F
Food & Beverage	11.6/21	F
Construction	11.6/21	F
Professional Services	11.2/21	F
Retail	11.2/21	F
Real Estate	11.2/21	F
Nonprofit	10.9/21	F
Hospitality	9.6/21	F

Did you know? The average data breach takes 200+ days to identify and contain.

YOUR ROADMAP

The Path to an A Grade

Use this checklist to help your business achieve an A-grade posture.

Security Improvement Checklist

☐ Enforce HTTPS across all public web properties and verify certificate health.	+3 points
☐ Harden SPF to strict policy and validate authorized senders.	+3 points
☐ Set DMARC to enforcement mode (quarantine/reject) and monitor reports.	+3 points
☐ Implement all six recommended security headers consistently.	+6 points
☐ Review dark web exposure and reset/rotate affected credentials promptly.	+3 points
☐ Harden business email infrastructure (mail gateway/MX security controls).	+3 points
☐ Establish recurring security reviews to keep controls current.	BONUS POINTS
☐ Enable MFA for email and admin access across all critical systems.	BONUS POINTS
☐ Document a tested incident response process with clear owner roles.	BONUS POINTS

Castle Technology Partners helps businesses translate findings into practical action through a proactive, consultative approach. We prioritize the highest-risk gaps first, align fixes to business operations, and validate improvements over time so security becomes a repeatable management discipline instead of a one-time project. Our approach includes recurring leadership-level reviews so progress stays visible and aligned to business priorities. We also help leadership teams understand which risks are urgent now versus which can be phased into a quarterly roadmap. That clarity helps businesses invest confidently, avoid wasted spend, and build security momentum that lasts.

Did you know? 60% of small businesses close their doors within 6 months of a major cyberattack, including ransomware events.

NEXT STEP

See how your business scored

What would be most costly to your business: fraud, downtime, or lost trust? Let's align your cybersecurity priorities before it happens.

Scan to book your review

castletechnologypartners.com

251.313.0411