BUSINESS IMPACT SUMMARY

Security findings and their business impact for Harbour Street Bakery

harbourstreetbakery.example · October 9, 2026 · Prepared for Harbour Street Bakery (Sam Okafor, Owner) by Frontage Security

Two issues present a material risk of financial loss, customer impact or data exposure and should be addressed promptly. Two further issues should be scheduled for remediation over the coming months. The remaining items are routine maintenance.

35 / 100

At risk

At least one issue offers a credible route for an attacker and should be addressed within days.

Immediate attention

These items should be addressed promptly: critical items immediately, and all others within two weeks.

Your email domain can be impersonated

FINDING

The domain lacks one or more of the DNS records (SPF, DKIM and DMARC) that allow receiving mail servers to verify which servers may send email on its behalf. Without them, messages that falsely display your address can be delivered to recipients' inboxes as though they were genuine.

BUSINESS IMPACT

This is the technique most commonly used in invoice and payment-redirection fraud, in which a customer or supplier receives an apparently legitimate request to change bank details. The same technique can be used to target staff with messages that appear to come from colleagues or senior management.

AFFECTED PARTIES	RESPONSIBLE PARTY	ESTIMATED EFFORT
Customers, suppliers and staff	Your email provider or IT support provider	Typically a few hours of work, phased over two to four weeks so that legitimate email is not disrupted.

Affected systems: `harbourstreetbakery.example`.

Technical reference: Missing DMARC record; No DKIM record found at common selectors.

Visitors may be shown a security warning in place of your website

FINDING

Browsers verify a website's security certificate on every visit. A certificate that has expired, is close to expiry or is not trusted causes the browser to display a full-page warning instead of the site.

BUSINESS IMPACT

Most visitors do not proceed past such a warning, so inquiries and online sales are likely to stop until it is resolved. Payment and login functions may also fail, and the warning can undermine customers' confidence in the business.

AFFECTED PARTIES	RESPONSIBLE PARTY	ESTIMATED EFFORT
Customers and prospective customers	Your website developer or hosting provider	Usually under an hour. Automatic renewal should be enabled at the same time to prevent a recurrence.

Affected systems: `shop.harbourstreetbakery.example`.

Technical reference: TLS certificate expires in 9 days.

Planned remediation

These items should be scheduled for remediation over the coming months.

Your website and email are at risk of an outage

FINDING

The DNS configuration that directs internet traffic to your website and email has a weakness, such as an unresponsive name server, no redundancy if a server fails, or settings that are capable of failing outright.

BUSINESS IMPACT

If this configuration fails, your website and email can become unavailable to everyone at once, often without a clear error, until the cause is identified and corrected.

AFFECTED PARTIES	RESPONSIBLE PARTY	ESTIMATED EFFORT
Anyone attempting to reach the organization	Your DNS provider or IT support provider	Usually one to two hours.

Affected systems: `harbourstreetbakery.example`.

Technical reference: Only one working nameserver is published for this domain.

Data sent to your website could be intercepted or altered

FINDING

Your website accepts outdated encryption methods, or does not require an encrypted connection.

BUSINESS IMPACT

On shared networks such as public Wi-Fi, an attacker nearby could read or modify information exchanged with the site, including form submissions and login details. Businesses that accept card payments should also note that the card industry's security standard (PCI DSS) prohibits the oldest of these methods.

AFFECTED PARTIES	RESPONSIBLE PARTY	ESTIMATED EFFORT
Customers and other site users	Your website developer or hosting provider	Usually under an hour.

Affected systems: `shop.harbourstreetbakery.example`.

Technical reference: Obsolete protocol supported: TLS 1.0.

Changes since the previous assessment

RESOLVED

✓ Email impersonation: 1 issue resolved

✓ Exposed services: 1 issue resolved

NEW

+ Website certificate: 1 new issue

Routine maintenance

Lower-priority improvements that present no immediate risk. These are best addressed alongside other planned work. Details are provided in the technical report.

Website safeguards: 2 minor items

General hardening: 2 minor items

Recommended next steps

1. Share the accompanying technical report with your IT support provider. Each finding includes guidance written for the person responsible for the fix.
2. Ask them to address the items under “Immediate attention” first and to confirm once each is complete.
3. The next assessment will confirm which issues have been resolved and identify any new ones.

1 item accepted as a known risk or marked as not applicable is excluded from this summary and remains listed in the technical report.