Ghostly Solutions LLC-FZ
Meydan Grandstand, 6th floor,
Meydan Road, Nad Al Sheba, Dubai
+971 58 534 66 41
general@ghostlysolutions.ae

GhostGuard — Data Collection & Usage Disclosure

Last updated: 05 January 2026

Summary

GhostGuard is designed to provide real-time phishing and impersonation warnings without scanning inbox content and without collecting sensitive user data (except if the user has explicitly enabled this feature). Risk decisions are based primarily on URL/domain signals and on-page security indicators.

What GhostGuard processes (for security analysis)

To generate warnings, GhostGuard processes the following security-relevant technical signals:

Visited URLs and domains, including redirect chains (to detect cloaking, phishing kits, and suspicious navigation patterns).

Domain reputation and infrastructure signals, including domain age and RDAP/WHOIS-derived indicators.

SSL/TLS and basic security indicators (e.g., unsafe HTTP pages, certificate anomalies).

Security verdicts / risk labels (e.g., low/high risk) generated as part of the protection flow.

Webmail link checks

GhostGuard analyzes links shown in supported webmail interfaces and evaluates sender domains as displayed by the webmail UI for phishing/impersonation risk. GhostGuard does not read or store email content or message bodies (except if the user has explicitly enabled a feature that allows email text analysis for security warnings).

Threat intelligence checks

GhostGuard may check URLs/domains against known threat intelligence sources to detect known malicious destinations. When such checks are used, the relevant URL/domain may be queried to complete the lookup.

Data NOT collected

GhostGuard is built to minimize data exposure. We do not collect:

- Email content or message bodies.
- Passwords, login credentials, authentication codes
- Payment card data, bank data, checkout form inputs
- Personal messages or private communications .
- Personal identifiers for advertising or profiling (no tracking)

Data usage

Processed signals are used only to:

Provide real-time security warnings and risk indicators before users proceed to a page or enter sensitive information.

Improve detection logic and maintain security protections (security-only purpose; no advertising).

Data sharing

No advertising / profiling: We do not sell user data or use it for advertising profiling.

Infrastructure providers: If any backend services are used to deliver the Service, they are limited to infrastructure/hosting and operated under contract for service delivery only (not for advertising).

Threat intelligence providers: When threat intelligence checks are used, the relevant URL/domain may be submitted to complete the lookup.

Extension store disclosure

Store listings for GhostGuard indicate that the developer discloses no collection or use of user data and no tracking / no email content access (except if the user has explicitly enabled a feature that allows email text analysis for security warnings) as part of the privacy-first design.

Contact

Ghostly Solutions L.L.C-FZ

Meydan Grandstand, 6th floor, Meydan Road, Nad Al Sheba, Dubai, United Arab Emirates

Phone: +971 58 534 6641

Email: general@ghostlysolutions.ae

Support: ghostguard.support @ghostlysolutions.ae