Checktxt
Smishing Awareness Training

Checktxt Smishing Awareness Training teaches employees and customers how to quickly recognize, verify, and avoid SMS-based scams using simple, real-world examples and hands-on guidance.

BENEFITS OF TRAINING

Meets Regulator Expectations
Helps satisfy awareness/training requirements referenced by HIPAA, GLBA, PCI DSS, GDPR, NIST/ISO, etc., when run with proper governance.

Provides Auditable Evidence
Produces DPIAs/risk assessments, approvals, message catalogs, delivery logs, test results and remediation records auditors want.

Reduces Legal & Privacy Risk
Fewer successful scams, stronger defensible evidence after incidents.

Enables Targeted Remediation
Identifies high-risk users/departments so training is focused and cost-effective.

Improves Security Posture
Lowers click/reply rates, increases user reporting, and eases SOC/IR workload.

Protects Brand & Customers
Demonstrates proactive governance and reduces reputational damage.

Key deliverables auditors expect: policy and approvals, DPIA, message catalog, delivery/engagement logs, remediation records, and vendor assurances (DPA/BAA/SOC2).

Bottom Line

With documented governance, safe message design, and robust logging, smishing training becomes an auditable compliance control valuable but not a standalone guarantee of compliance.

Checktxt | Overview & Operations

OVERVIEW

Smishing awareness training is a controlled, educational program that simulates SMS phishing (smishing) to teach people how to recognize, resist and report malicious texts.

Instead of using real attacks, the program delivers realistic but safe SMS messages that mimic common scam vectors (delivery notices, bank alerts, IT password resets) so recipients learn to spot red flags — unexpected links, urgent requests for money or credentials, spoofed senders — and to use the organization's reporting channels.

The goal is behavior change: fewer clicks and replies, faster reporting, and better overall resilience to social-engineering attacks.

A typical program is run from a governed platform and follows a clear process:

- legal/privacy/HR sign-off and, if required, a DPIA;
- careful message design using placeholders or internal training URLs (never live credential harvesters or real PII/PHI);
- audience segmentation and safe delivery; and
- secure vendor controls.

Campaigns record delivery, engagement (clicks/replies), and report rates, then trigger immediate, targeted remediation (short training modules or coaching) for users who fall for simulations. Results are aggregated into auditable reports (purpose, scope, logs, remediation) so compliance teams and auditors can verify the exercise was lawful, proportionate and effective.

OPERATIONALIZE

This service is available to customers with an **Enterprise** or **Partner** account. To enroll, the customer must complete the Check**txt Opt-In** form and obtain documented approvals from Legal, HR, and any other appropriate stakeholders (for example: Compliance, Privacy, Security, or IT). These approvals are required before we activate access to the training configuration form.

Once the Opt-In and approvals are complete, the organization will be granted access to the training form where they will enter the required campaign information:

Attribute	Value
Number of tests to be sent out	?
Start window	$m/d/yr$
End Window (must exceed 72 hours)	$m/d/yr$
List of User that will receive tests	All or designated users
Opt-in information	Upload completed forms

In addition to the training, an online smishing education session (Zoom) will be offered before the training exercise.

RESULTS

Upon completion, administrators will receive a single, auditable results package designed for easy review and for independent attestation by auditors. The package provides a clear record of the exercise and demonstrates the program's effectiveness. It contains:

- **Purpose** – A concise statement of the exercise objectives.
- **Scope** – Target populations, exclusions, and campaign parameters.
- **DPIA / Risk Assessment** – The data-protection impact assessment and any identified mitigations.
- **Test Results** – Aggregate (and where appropriate, de-identified individual) metrics such as delivery, clicks/replies, and remediation outcomes.
- **Proof of Delivery** – Message delivery logs, timestamps, and delivery status.
- **Legal Consents & Compliance Documentation** – Documented in-house legal approvals, consents, and supporting compliance artifacts.
- **Copies of Training Messages** – Exact message text used in the campaign.