

Employee-Facing Security Awareness Survey

Purpose

This survey helps us understand how you experience security awareness in your role. Your feedback will help shape a stronger, more relevant, and more engaging security program.

Note: All questions are anonymous. Please answer honestly.

Section 1: About You

(Informational only — optional demographic questions)

1. **What department do you work in?**
[Multiple Choice / Dropdown]
 2. **How long have you worked at the company?**
[Multiple Choice]
 - ☐ Less than 6 months
 - ☐ 6–12 months
 - ☐ 1–3 years
 - ☐ 3–5 years
 - ☐ 5+ years
 3. **How would you describe your level of technical knowledge?**
[Multiple Choice]
 - ☐ Low – I mostly use standard apps (email, browser, etc.)
 - ☐ Medium – I use systems and tools specific to my job
 - ☐ High – I work with code, infrastructure, or security tools
-

Section 2: Strategy & Leadership (Perceived Support)

(Likert Scale: Strongly Disagree → Strongly Agree)

1. Leadership in my department takes cybersecurity seriously.
 2. I believe cybersecurity is a priority for the company.
 3. I understand how cybersecurity helps protect our business and customers.
-

Section 3: Content & Communication

(Likert Scale)

1. I receive regular security reminders or training.
 2. The security tips or training I receive are clear and easy to understand.
 3. I know where to go to find security information or guidance.
 4. Security messages or trainings are delivered in ways that are easy to access (e.g., email, videos, short modules).
-

Section 4: Behavior & Culture

(Likert Scale)

1. I know how to report a suspicious email or potential security issue.
2. I think before clicking links or downloading attachments in emails.
3. I take steps to protect sensitive information in my day-to-day work.
4. People around me generally follow good security practices.
5. I believe secure behavior is part of everyone's responsibility, not just IT's.

Open Text (optional):

What's one thing you've learned from our security training that you now use regularly?

Section 5: Measurement & Optimization (Perceived Effectiveness)

(Likert Scale)

1. The security training I've received helps me do my job more securely.
2. I've become more aware of potential threats (like phishing or data loss) because of the awareness program.
3. I feel more confident handling a suspicious email or incident now than I did before.

Open Text (optional):

What type of security content would be most helpful to you? (e.g., quick tips, videos, simulations, how-to guides)

Section 6: Engagement & Enablement

(Likert Scale)

1. I've participated in a security campaign, training, or simulation in the past 6 months.

2. The security training was interactive and engaging.
3. I would be interested in participating in security activities like games, challenges, or competitions.
4. I would feel comfortable helping a coworker with a basic security question.

Open Text (optional):

What would make our security awareness efforts more helpful or engaging?

 Final Thoughts

(Likert Scale)

1. Overall, I believe the company is doing a good job promoting security awareness.
 2. I feel personally responsible for helping keep the company secure.
-

 Scoring (for Analyst Use)

- **Likert Scale Responses:** Scored 0–4
- Group questions under the 5 categories:
 - Strategy & Leadership → Section 2
 - Content & Communication → Section 3
 - Behavior & Culture → Section 4
 - Measurement & Optimization → Section 5
 - Engagement & Enablement → Section 6
- **Category Score = Average of responses in that section**

Average Score Maturity Level

0.0–0.9	Level 1 – Ad Hoc
1.0–1.9	Level 2 – Foundational
2.0–2.9	Level 3 – Behavioral
3.0–3.4	Level 4 – Embedded
3.5–4.0	Level 5 – Optimized