**🔐 Cybersecurity Awareness Month 2025 – Full Campaign Brief**

**📅 Duration:** October 1–31, 2025  
**🏢 Audience:** All Employees (Global)  
**🎯 Theme:** *"Secure Together: Awareness, Action, Accountability"*

**🧠 Overview**

October marks **Cybersecurity Awareness Month**, a company-wide initiative dedicated to strengthening our collective defense against cyber threats. As digital threats continue to evolve, so must our awareness and response. This year’s campaign focuses on empowering every employee to take ownership of cybersecurity through education, vigilance, and proactive behavior.

Participation is **mandatory** for all employees and includes completion of the updated training module, review of phishing simulation results, and engagement in weekly awareness activities.

**📋 Key Objectives**

* Reinforce best practices for digital hygiene and data protection.
* Educate employees on the latest threat vectors, including phishing, social engineering, and credential theft.
* Promote a culture of shared responsibility in cybersecurity.
* Reduce the company’s overall risk exposure through informed behavior.

**🧑‍🏫 Mandatory Training**

All employees are required to complete the **2025 Cybersecurity Awareness Training Module**, which includes:

* Updated threat landscape overview
* Interactive phishing identification exercises
* Secure password and MFA practices
* Remote work and device security protocols
* Case studies of real-world breaches

**Deadline:** October 31, 2025  
**Estimated Time:** 45 minutes  
**Access:** Cybersecurity Training Portal

Completion will be tracked and reported to department heads. Non-compliance may result in restricted access to internal systems.

**🧪 Phishing Simulation Results**

As part of the campaign, the IT Security team conducted a **company-wide phishing simulation** in September. Key findings include:

* **Click Rate:** 12.4% (↓ from 18.7% in 2024)
* **Report Rate:** 41.2% (↑ from 33.5% in 2024)
* **Top Departments by Reporting:** Finance, Legal, and Customer Support
* **Common Mistakes:** Clicking on suspicious links, entering credentials on spoofed login pages

All employees are encouraged to review their individual performance and team metrics via the **Phishing Dashboard** on the intranet.

**📅 Weekly Activities & Events**

| **Week** | **Focus Area** | **Activities** |
| --- | --- | --- |
| Week 1 | Password Security | Password manager tutorials, MFA setup clinics |
| Week 2 | Phishing Awareness | Live phishing quiz, email red flag checklist |
| Week 3 | Device & Data Protection | Secure device configuration guides, USB safety tips |
| Week 4 | Incident Reporting | How to report threats, mock incident response drill |

Each week will feature:

* **Mini challenges** with prizes (e.g., secure password contest)
* **Live webinars** with guest speakers from the cybersecurity industry
* **Daily tips** via Slack and email

**🛡️ Security Champions Program**

We’re launching a new **Security Champions Program** to recognize employees who go above and beyond in promoting cybersecurity awareness. Nominate a colleague who:

* Regularly reports suspicious activity
* Educates peers on safe practices
* Demonstrates leadership in digital safety

Winners will receive:

* A custom Security Champion badge
* Recognition in the company newsletter
* A \$100 gift card

**📣 How to Report Suspicious Activity**

If you receive a suspicious email, message, or notice unusual system behavior:

1. **Do not click** on any links or attachments.
2. **Report immediately** via the “Report Phishing” button in Outlook.
3. **Contact IT Security** through the #security-alerts Slack channel or email security@company.com.

**📊 Metrics & Accountability**

* Departmental compliance rates will be published weekly.
* Managers will receive progress reports for their teams.
* Final participation statistics will be shared in the November All-Hands meeting.

**🧭 FAQs**

**Q: Is the training mandatory for contractors and interns?**  
A: Yes, all individuals with access to company systems must complete the training.

**Q: Can I retake the phishing simulation?**  
A: No, but you can review the simulation breakdown and learn from the results.

**Q: Will there be follow-up simulations?**  
A: Yes, unannounced simulations will occur throughout Q4 to reinforce awareness.

Let’s stay secure—together. Your vigilance is our first line of defense.