Employee Security Training Guide

Every employee is a potential target. Cybercriminals exploit people more often than systems, using phishing, social engineering, and malware to gain access to company data. A well-trained team is the strongest defense against attacks.

Recognizing Phishing & Social Engineering

- Be suspicious of urgent requests (e.g., “Act now!” or “Your account will be closed”).
- Check sender addresses carefully — small typos or unusual domains are red flags.
- Never click unknown links or open unexpected attachments.
- Report suspicious emails immediately using your company’s reporting tool or IT helpdesk.

Password & Authentication Best Practices

- Use unique, strong passwords (preferably through a password manager).
- Never reuse work passwords for personal accounts.
- Enable Multi-Factor Authentication (MFA) wherever possible.
- Do not share login credentials with anyone — even colleagues.

Device Security

- Lock your computer when away from your desk (Ctrl+Alt+Del or Windows+L / ⌘+Control+Q).
- Keep devices updated with security patches.
- Report lost or stolen devices immediately.
- Only use approved company devices for work tasks.

Data Protection & Cloud Usage

- Store files only in company-approved platforms (e.g., Egnyte, Office 365).
- Do not send sensitive information via personal email or unencrypted channels.
- Avoid uploading confidential data into unauthorized AI tools or third-party apps.
- Follow company policies for data classification and retention.

Please scan the QR code to book an appointment with our expert to learn more or visit: calendly.com/methodologyit/intro

800-270-0016
hello@methodologyit.tech

Employee Security Training Guide

Safe Internet & Remote Work Practices

- Be cautious when using public Wi-Fi — connect through a company VPN.
- Avoid downloading unapproved software or browser extensions.
- Keep work and personal browsing separate.
- Never plug in unknown USB drives or devices.

Incident Response & Reporting

- If you suspect something unusual (phishing, malware, data loss):
- Stop what you're doing immediately (disconnect from Wi-Fi if necessary).
- Do not try to fix it yourself — contact IT support.
- Report quickly — the faster an incident is reported, the less damage occurs.

Ongoing Security Awareness

- Complete assigned Security Awareness Training (SAT) modules.
- Participate in phishing simulations and learn from results.
- Join in tabletop exercises to practice response scenarios.
- Stay updated — cyber threats evolve constantly.

Daily Cybersecurity Best Practices

- Pause and verify before clicking links or opening attachments
- Use strong, unique passwords and enable MFA everywhere possible
- Lock devices when unattended, keep them updated, and report if lost or stolen
- Store and share data only with approved company tools
- Connect securely (VPN on public Wi-Fi, never use unknown USBs)
- Report suspicious activity immediately — no exceptions
- Stay current by completing required training and simulations

Remember: Security is a team effort. By staying alert and following these guidelines, you protect not only yourself but also your coworkers, clients, and the company's reputation.

800-270-0016
hello@methodologyit.tech