Employee Security Awareness Checklist 2024

Employee Security Awareness Checklist for 2024, incorporating the latest cybersecurity trends:
This checklist covers essential cybersecurity practices for employees working in office or remotely.

Password Protection	
Use passwords at least 16 characters long with a mix of uppercase, lowercase, numbers, and special characters	□
Implement passwordless authentication methods where possible (e.g., biometrics, security keys)	□
Use a reputable password manager for generating and storing unique passwords	□
Enable password breach monitoring services	□
Multi-Factor Authentication (MFA)	
Enable MFA on all accounts that offer it, especially email and financial accounts	□
Prioritize using authenticator apps or hardware tokens over SMS-based MFA	□
Consider adaptive MFA that adjusts based on user behavior and risk levels	□
Email Security	
Verify sender email addresses and domain names carefully	□
Be cautious of urgent requests or threats in emails	□
Hover over links to preview URLs before clicking	□
Use email filtering and anti-phishing tools	□
Report suspicious emails to IT security team	□
Software Updates	
Enable automatic updates for operating systems and applications	□
Promptly install security patches when released	□
Keep browsers and browser extensions up-to-date	□
Safe Browsing	
Use HTTPS-enabled websites, especially for sensitive transactions	□
Be wary of browser extensions and only install from trusted sources	□
Use privacy-focused browsers and search engines	□
Remote Work Security	

Use a company-provided VPN when working remotely	□
Secure home Wi-Fi networks with strong encryption (WPA3 if available)	□
Avoid using public Wi-Fi for work-related tasks	□
Use a separate, dedicated device for work if possible	□
Device Security	
Use endpoint detection and response (EDR) solutions	□
Enable full-disk encryption on all devices	□
Use biometric authentication (e.g., fingerprint, facial recognition) where available	□
Keep work and personal activities separate on devices	□
AI and Machine Learning Awareness	
Be cautious of AI-generated phishing attempts and deepfakes	□
Understand the basics of AI-related security risks	□
Follow company policies on AI tool usage	□
Cloud Security	
Use company-approved cloud storage and file-sharing services	□
Enable MFA for all cloud service accounts	□
Be cautious when granting permissions to third-party apps	□
Social Engineering Awareness	
Be vigilant of vishing (voice phishing) and smishing (SMS phishing) attempts	□
Verify requests for sensitive information through official channels	□
Be wary of impersonation attempts in video calls or chat applications	□
Incident Reporting	
Know the proper channels for reporting security incidents	□
Report any suspicious activities or potential breaches immediately	□
Familiarize yourself with the company's incident response plan	□
Continuous Learning	
Participate in regular security awareness training sessions	□
Stay informed about the latest cybersecurity threats and best practices	□
Engage in cybersecurity drills and simulations when offered	□