Credits: CSI Piemonte & Risk Solver
Info: segreteria@assintel.it

10 domande per le Aziende per capire se si stanno difendo dal Phishing

		Si	No	In corso	Previsto
1. Hai previsto dei corsi di formazione e sensibilizzazione dei Dipendenti?	Una delle misure più efficaci per prevenire il phishing è garantire che tutti i dipendenti siano adeguatamente formati e consapevoli dei rischi associati. Organizza regolarmente sessioni di formazione per insegnare ai dipendenti a riconoscere e segnalare tentativi di phishing				
2. Hai definito delle Politiche di Sicurezza per l'uso delle E-mail	Implementa politiche di sicurezza delle email rigorose. Utilizza filtri antispam per bloccare le email sospette e istruisci i dipendenti a non aprire allegati o cliccare su link provenienti da mittenti sconosciuti.				
3. Hai adottato l'autenticazione a Due Fattori (2FA)?	L'autenticazione a due fattori aggiunge un ulteriore livello di sicurezza. Anche se i cybercriminali riescono a ottenere le credenziali di accesso, avrebbero comunque bisogno di un secondo fattore, come un codice inviato al telefono del dipendente, per accedere ai sistemi aziendali				
4. Hai adottato Software Antivirus e Anti-malware su tutte le postazioni?	Assicurati che tutti i computer e i dispositivi mobili aziendali siano protetti da software antivirus e anti-malware aggiornati. Questo software può rilevare e bloccare molti tentativi di phishing prima che raggiungano gli utenti.				
5. Hai definito una politica di Controllo degli Accessi?	Limita l'accesso ai dati sensibili solo ai dipendenti che ne hanno realmente bisogno per svolgere il loro lavoro. Utilizza sistemi di gestione degli accessi per monitorare e controllare chi può accedere a quali informazioni.				
6. Hai definito delle attività di monitoraggio e analisi del Traffico di Rete?	Implementa sistemi di monitoraggio e analisi del traffico di rete per rilevare attività sospette. Condividi con il personale dipendente e le rappresentanze sindacali i controlli di sicurezza. Questo può aiutare a identificare e bloccare tentativi di phishing in tempo reale				
7. Effettui aggiornamenti Regolari del software?	Mantieni tutti i software aziendali, inclusi i sistemi operativi, i browser e le applicazioni, aggiornati con le ultime patch di sicurezza. Le vulnerabilità non risolte possono essere sfruttate dai cybercriminali per condurre attacchi di phishing				

8. Organizzi delle simulazioni di Phishing?	Esegui periodicamente simulazioni di phishing per testare la preparazione dei dipendenti. Questo può aiutarti a identificare aree di miglioramento e a fornire una formazione mirata.				
9. Hai implementato una politica di Backup dei Dati? Ne verifichi periodicamente l'efficacia?	Implementa una politica di backup dei dati efficace. In caso di successo di un attacco di phishing, avere backup recenti e sicuri può aiutarti a recuperare rapidamente i dati.				
10. Hai predisposto un piano di Risposta agli Incidenti?	Sviluppa e mantieni un piano di risposta agli incidenti che includa procedure specifiche per gestire i tentativi di phishing. Questo piano dovrebbe includere istruzioni su come isolare i sistemi compromessi, notificare gli utenti interessati e riportare l'incidente alle autorità competenti.				