Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

ARPAC CAMPANIA

Cyber Security & Data Protection

Newsletter mensile: Maggio 2025

Questo mese parliamo di...

LAVORO DA REMOTO IN SICUREZZA

Il lavoro da remoto offre numerosi vantaggi in termini di flessibilità e produttività, consentendo di svolgere le attività lavorative in base alle esigenze logistiche e lavorative. Tuttavia, **comporta anche una maggiore esposizione a minacce cyber** qualora non si adottino le dovute attenzioni. L'obiettivo della newsletter di questo mese è **fornire una serie di accorgimenti** da adottare per poter **lavorare da remoto in sicurezza** e ridurre il rischio di esposizione accidentale di dati sensibili.

Non consentire l'utilizzo dei dispositivi a utenti non autorizzati

Consentire a utenti non autorizzati di accedere ai dispositivi utilizzati per il lavoro da remoto può portare a gravi conseguenze, come la perdita di dati sensibili e l'esposizione a potenziali attacchi informatici. È fondamentale **mantenere il controllo sui dispositivi, custodirli in sicurezza** e garantire che solo gli utenti autorizzati possano accedervi. Ciò implica non solo **evitare di condividere il computer o lo smartphone utilizzati per lavorare da remoto** con familiari o amici, ma anche **implementare misure di sicurezza** come l'uso di **password robuste**, l'attivazione di sistemi di **autenticazione a due fattori** e il **blocco del dispositivo quando ci si allontana**.

Non connetterti a reti Wi-Fi pubbliche

Le reti Wi-Fi pubbliche risultano poco sicure, in quanto chiunque può accedervi, compresi **i cybercriminali che potrebbero cercare di colpire i dispositivi connessi alla rete**, sottraendo informazioni sensibili e/o installando software dannosi. Quando si lavora da remoto, si consiglia di **connettersi alla propria rete domestica oppure a un hotspot mobile personale** e di assicurarsi di **utilizzare password robuste per proteggere l'accesso alla rete**.

Utilizza esclusivamente i servizi di file-sharing approvati

L'utilizzo di servizi di file-sharing non approvati dall'Agenzia può portare a fughe di dati accidentali. Per evitare accessi indesiderati da parte di utenti non autorizzati a dati sensibili, **utilizza esclusivamente OneDrive, sia per accedere ai documenti dell'Agenzia quando lavori da remoto,** sia per condividerli con colleghi ed enti esterni.

Mantieni aggiornati i dispositivi

Gli aggiornamenti software sono cruciali per la sicurezza dei dispositivi utilizzati per lavorare da remoto, poiché **possono risolvere potenziali vulnerabilità** sfruttabili dai cybercriminali per hackerare i dispositivi. Pertanto, si consiglia di **attivare gli aggiornamenti automatici** sia sul computer che sullo smartphone utilizzati per lavorare da remoto e di **installare regolarmente gli aggiornamenti proposti**.