

CYBER SECURITY E SMART WORKING

Si raccomanda tutto il personale in telelavoro/smartworking di **utilizzare in maniera sicura gli strumenti informatici forniti da FBK.**

Di seguito le **10 regole** che vi raccomandiamo di seguire insieme alle [istruzioni sul corretto trattamento di dati personali](#) fornite da FBK durante la formazione obbligatoria in materia di privacy.

<p>1. POLICY FBK Segui prioritariamente policy raccomandazioni dettate da FBK;</p> <p>3. DISPOSITIVI ESTERNI Utilizza solo dispositivi (chiavette USB, hard disk-esterni, ecc.) di cui conosci la provenienza;</p> <p>5. STRUMENTI Blocca il PC quando ti allontani dalla tua postazione di lavoro;</p> <p>7. SOFTWARE Installa software provenienti solo da fonti o repository ufficiali;</p> <p>9. SISTEMA OPERATIVO AGGIORNATO Aggiorna costantemente il tuo sistema operativo;</p>	<p>2. CONNESSIONI PROTETTE Utilizza connessioni adeguatamente protette (evita reti Wi-Fi gratuite);</p> <p>4. PASSWORD Utilizza sempre password sicure, cambiale periodicamente, mantienile segrete e custodite;</p> <p>6. SERVIZI E PORTALI Disconnettiti sempre dai servizi/portali quando hai concluso la sessione lavorativa;</p> <p>8. E-MAIL SOSPETTE Non cliccare su link o allegati contenuti in email sospette;</p> <p>10. SOFTWARE DI PROTEZIONE Assicurati che i software di protezione (Firewall, Antivirus, ecc) siano abilitati e sempre aggiornati.</p>
---	---

Per ulteriori approfondimenti in tema cybersecurity, vi proponiamo anche i [consigli del Parlamento Europeo](#) e della [Polizia Postale](#).

L'Unità Prevenzione della Corruzione, Trasparenza e Privacy

privacy@fbk.eu

hr.fbk.eu/privacy