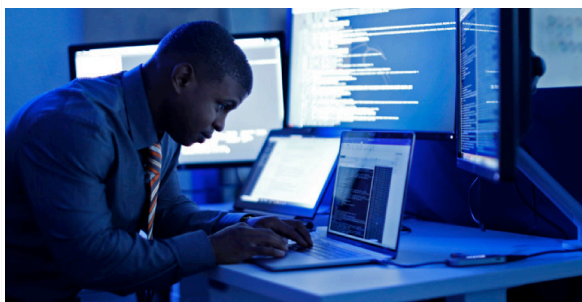


> In generale

Con il passare degli anni i nostri dati in rete sono diventati sempre più preziosi e vulnerabili, eppure non è aumentata di pari passo l'attenzione collettiva e individuale riposta nella protezione dei medesimi dati. Si pensi alla buona norma che ci porta a chiudere porte e finestre uscendo di casa: perché non adoperiamo la stessa premura quando spegniamo il computer, chiudendo con esso anche il wifi? A livello globale, le conseguenze di un attacco cyber sono paragonabili a quelle provocate da una catastrofe naturale. Prima di arrivare però agli attacchi a larga scala, gli hacker si allenano con i singoli. Come possono dunque le persone, ma soprattutto le aziende, rispondere alla minaccia cyber? Con la professionalità. La domanda di professionisti che possano garantire la sicurezza informatica cresce di anno in anno. È questo il motivo che rende quello della **cyber security** uno dei settori in maggiore crescita. Quando parliamo di **cyber security** ci riferiamo ad un settore giovane, con importanti opportunità di impiego. Un settore che si va però strutturando adesso e in cui è ancora difficile trovare i candidati giusti, principalmente perché in Italia sono ancora troppo pochi i laureati in queste discipline.



> Tendenze d'impiego

L'**esperto di cyber security** è ormai una figura chiave per molte imprese e **uno dei ruoli in crescita nelle ricerche di lavoro del settore informatico**. Si tratta dunque di un'interessante opportunità professionale per chi ama sistemi, reti e linguaggi di programmazione.

Cyber Security Expert

Il **Cyber Security Expert** colui che in azienda assicura la protezione di sistemi, reti e dati informatici, rispettando le normative nazionali ed europee.

Essere esperti di cyber security significa saper agire su due livelli: da una parte la **prevenzione**, definendo le strategie per garantire la sicurezza, dall'altra la **soluzione degli eventi critici**, soprattutto nel caso dei *data breach*, le violazioni dei dati che possono mettere a serio rischio non solo l'azienda, ma anche altri soggetti, come gli utenti proprietari delle informazioni sottratte. Il compito primario di un **esperto in cyber security** è quello di **proteggere tutte le risorse digitali dell'impresa da qualunque tipo di minaccia o di attacco**. Tutta l'azienda deve essere costantemente controllata, perché la sicurezza non ammette interruzioni o distrazioni. Un esperto della sicurezza informatica deve saper controllare tutte le fonti, interne ed esterne all'azienda, dalle quali possono derivare rischi di violazione e adottare misure preventive per evitare gli attacchi. È importante anche che sappia confrontarsi con altri esperti e condividere esperienze. Fa parte del lavoro del responsabile della sicurezza informatica aggiornare tutto lo staff sui metodi usati dai criminali informatici per introdursi nei sistemi aziendali e sottrarre dati o provocare danni. La comunicazione deve essere costante e coinvolgere i dipendenti nella prevenzione delle minacce.

> Formazione

Per diventare **esperti in cyber security** è ovviamente necessario essere esperti di informatica e conoscere le formule (password, sistemi di salvataggio). I percorsi formativi possono essere molteplici: se da un lato può accadere che siano gli studenti di Matematica, Statistica ed Economia a convertirsi, dall'altro è anche vero che un esperto non deve necessariamente essere laureato. In questo ambito, le competenze acquisite sul campo diventano più importanti rispetto ad una laurea.

> Per saperne di più

- **A Orientamenti 2019**
 - Via dell'Innovazione Tecnologica - Digitale e Meccatronica, Intelligenza Artificiale e Robotica, Big Data e Internet of Things
 - Laboratori delle Professioni Innovazione Tecnologica
- **Esplora i siti**
 - <https://www.dibris.unige.it>
 - <https://corsi.unige.it/8733/>