

“Corso base per la gestione del PC in sicurezza”

ABSTRACT:

La sicurezza informatica dei nostri dispositivi riveste un ruolo cruciale per poter lavorare in sicurezza, proteggendo i dati.

A CHI E' RIVOLTO:

A tutto il personale tecnico-amministrativo dell'Ateneo.

OBIETTIVI:

Il corso si propone di innalzare il livello di consapevolezza della sicurezza informatica nell'utilizzo dei dispositivi utilizzati nelle attività lavorative. Il corso sarà suddiviso

CONTENUTI:

- Introduzione alla Sicurezza Informatica
- Costi della sicurezza
- Analisi dei rischi
- Politiche di sicurezza
- Minacce / Vulnerabilità
- Sistemi di sicurezza
- Insidie della rete
- Malware
- Violazione account
- Furto password
- Social Engineering
- Cosa è un sistema operativo e quali sono le versioni da non usare e quali quelle consigliate
- Come vedo quale SO ho. Come vedo quale versione ho.
- Aggiornamenti di sistema.
- Antivirus e firewall integrato: perché Defender può non bastare. Come installo l'antivirus. Come vedo se l'AV è installato. Versioni dell'antivirus (come vedo quale ho)
- Motore e Virus definition. Cosa sono e come li aggiornare. Chi mi dice quando aggiornare.
- I vari browser: quali usare, quando e perché.
- La differenza tra app desktop e app web.
- Password: dove e perché avere una password, perché cambiarla spesso e perché, soprattutto, non usare sempre la stessa.
- Le varie versioni di office. Come vedo quale versione sto usando. Come posso passare ad office365.
- Cosa posso fare con Office365: quali sono i vantaggi dell'avere la suite e come usarla al meglio. Ho 5 licenze.
- Posta elettronica: quali client ci sono e quali usare (e perché).
- Il backup, questo sconosciuto: cosa è, cosa non è, come e dove fare backup e come non farlo e perché.
- Il disaster recovery anche in caso di virus/malware: che tipo di backup bisogna usare?
- Evoluzione delle strategie e possibili scenari odierni.

DURATA:

20 ore di cui 12 in aula e 8 dedicate allo studio individuale