

I problemi di sicurezza legati alla didattica a distanza sono molteplici e spaziano dalla security intrinseca offerta dalla piattaforma scelta, ai problemi legati alla privacy e al controllo di chi si collega, passando per i problemi relativi al Copyright dei documenti condivisi su queste piattaforme. Infine, si devono tutelare i minori e le persone che utilizzano la piattaforma.

### **Come utilizzare in maniera sicura queste piattaforme? Ecco dieci consigli pratici dal lato studenti/genitori.**

- Installare un software Antivirus commerciale e abilitare il Controllo parentale sui computer utilizzati, per poter controllare eventuali malware, impostare i tempi di utilizzo del computer stesso, attivare le funzionalità di controllo privacy sui social network e controllare la navigazione web
- Nel caso si utilizzi un router commerciale, non gestito da un operatore telefonico, verificare o far verificare a un tecnico specializzato che il firmware del router sia aggiornato
- Verificare di aver installato tutti gli aggiornamenti sia del sistema operativo che dei programmi utilizzati, ad esempio la suite di office automation, il reader dei file pdf, il browser internet e tutti i programmi che vengono utilizzati per la didattica a distanza
- Attivare le funzionalità di firewall, presenti ormai di default, anche nei sistemi operativi che hanno una configurazione standard

### **Ecco, invece, i consigli dal lato docenti/istituti**

- Scegliere piattaforme commerciali che offrono un servizio di prova, per verificare la possibilità di settare i parametri di sicurezza e privacy
- Inviare i dettagli del collegamento in modo sicuro, preferire le sessioni che richiedono la registrazione dell'utente e controllare sempre (ad esempio invitando alla lezione via email) chi si collega in anticipo, in modo tale da verificare durante la lezione che il numero dei partecipanti non sia superiore a quello atteso. Se i numeri lo consentono, fare l'appello
- Controllare i seguenti parametri nel momento in cui si attiva una lezione a distanza:
  - disattivare la funzionalità di invito alla lezione per i partecipanti
  - disattivare la funzionalità di poter vedere la lista di tutti i partecipanti
  - disattivare la funzionalità di poter modificare l'evento per i partecipanti
  - attivare le funzionalità di cifratura (Encryption) delle comunicazioni
  - limitare o disattivare le funzionalità di File Transfer
  - limitare o disattivare le funzionalità di chat private tra i partecipanti lasciando attiva solo quella pubblica
  - se non indispensabile, disattivare le capacità video
  - in generale attivare o disattivare tutte quelle funzioni che potrebbero violare il rispetto della privacy
- quando si utilizzano siti o tools per sessioni Q&A, accertarsi che le comunicazioni avvengano in modalità cifrata e verificare la gestione della privacy del servizio stesso
- verificare che non vengano violate le regole sul Copyright per i materiali utilizzati
- evitare di far collegare in video gli studenti se non strettamente necessario o attivare la sessione video singolarmente e non per la totalità dei partecipanti. Sostituire anche le foto con fotografie generiche. Non inserire nome e cognome al momento del collegamento, se possibile utilizzare solo il solo nome o dei nickname.

In generale, è importante evitare il più possibile di disseminare online troppe informazioni, che potrebbero essere sfruttate per campagne mirate di phishing e colpire gli utenti con malware o ransomware, chiedendo poi riscatti in denaro per sbloccare i computer. Oggi esiste però anche un altro rischio, quello dei deepfake. I cybercriminali potrebbero impossessarsi degli audio e dei video sparsi online per produrre video falsi, ad esempio utilizzando un insegnante per fargli lanciare comunicazioni o notizie falsi agli studenti, che a loro volta potrebbero vedere il loro volto utilizzato in altre campagne maligne.