MOIGE & TREND MICRO UNITI CONTRO I CYBER RISK DELLE FAMIGLIE CONSIGLI UTILI PER GENITORI, STUDENTI E DOCENTI SU UN USO CORRETTO E SICURO DELLE PIATTAFORME ONLINE

In queste settimane, a causa della delicata situazione nella quale purtroppo ci troviamo in seguito al diffondersi dell'epidemia di Covid-19, si parla sempre più spesso di didattica a distanza, diventata ormai la normalità per molti studenti. Così come altre tecnologie utilizzate in questo periodo, anche gli strumenti per la didattica a distanza erano già presenti sul mercato da diverso tempo e sono molto simili a quelli che le aziende hanno implementato per lo Smart Working.

La differenza principale è che una buona parte delle organizzazioni che si erano già dotate di queste piattaforme aveva scelto implementazioni commerciali, mentre chi ha dovuto rincorrere la situazione di emergenza ha optato per quelle che sono le versioni di prova o limitate dei differenti prodotti presenti sul mercato.

Questo aspetto è importante e va tenuto in considerazione, perché la disponibilità di funzioni nelle versioni di prova dei prodotti è limitata rispetto all'upgrade commerciale e questo impatta anche sulla componente security.

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? Dieci consigli pratici:

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

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

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

Controllare i seguenti parametri nel momento in cui si attiva una lezione a distanza:

1. Disattivare la funzionalità di invito alla lezione per i partecipanti

2. Disattivare la funzionalità di poter vedere la lista di tutti i partecipanti

3. Disattivare la funzionalità di poter modificare l'evento per i partecipanti

4. Attivare le funzionalità di cifratura (Encryption) delle comunicazioni

5. Limitare o disattivare le funzionalità di File Transfer

6. Limitare o disattivare le funzionalità di chat private tra i partecipanti lasciando attiva solo quella pubblica

7. Se non indispensabile, disattivare le capacità video

8. In generale attivare o disattivare tutte quelle funzioni che potrebbero violare il rispetto della privacy

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.