Coronavirus, sicurezza cibernetica

Autore: Fabio Di Nunno
Fonte: Città Nuova

L’epidemia di Covid-19 ci sta costringendo a stare in casa e a un uso intensivo e improvviso delle nuove tecnologie per il lavoro, lo studio, lo svago ed il tempo libero, con un aumento dei rischi cibernetici.

Studiare, lavorare, informarsi, vedere un film, fare sport, finanche cucinare stanno cambiando con la diffusione della pandemia di **coronavirus**, che ci forza a restare nelle nostre abitazioni e utilizzare **strumenti tecnologici connessi ad Internet**. Così **Europol**, l’agenzia dell’**Unione europea** (Ue) che assiste i 27 Stati membri nella loro lotta contro la criminalità internazionale, il terrorismo, la sicurezza interna dell’Ue e dei suoi cittadini, mette in guardia dai **pericoli cibernetici** che corriamo in questo momento, a causa del **forte incremento repentino e talvolta improvvisato nell’uso delle nuove tecnologie e dei servizi online**. Alcune raccomandazioni sono quelle oramai classiche, ma vale la pena ricordarle. Innanzitutto, è buona prassi **cambiare la password** del nostro router per la connessione wi-fi ad Internet e scegliere password complesse e differenti per le email e i profili social, istallare dei software **antivirus** a tutti gli strumenti connessi ad Internet (che, nelle nostre case aumentano sempre di più), controllare di tanto in tanto le **impostazioni di privacy** dei social media ai quali siamo iscritti, verificare i permessi concessi alle app sui nostri telefonini nonché cancellare quelle che non usiamo più, tutti gli strumenti tecnologici con password, pin, informazioni biometriche (come le impronte digitali). Da ultimo, è buona abitudine fare un **back up dei nostri dati** (per esempio un salvataggio su una memoria esterna) ed un aggiornamento dei software. Le ultime stime calcolano il 65% degli italiani in ***smart working*** (o telelavoro), ma molte aziende e moltissimi lavoratori non erano preparati. Laddove possibile, i lavoratori dovrebbero accedere alle informazioni aziendali con **strumentazione appositamente fornita dal datore di lavoro**, che andrebbe protetta adeguatamente da occhi e mani altrui, usare un accesso remoto sicuro, **utilizzare strumenti diversi per il lavoro e il tempo libero** (o almeno fare tali attività in momenti diversi) e, quando non è possibile, utilizzare con molta attenzione i propri strumenti personali, **evitare di condividere informazioni personali o dati sensibili**, riferire immediatamente al proprio datore di lavoro eventuali attività sospette. Allo stesso tempo, le aziende dovrebbero stabilire delle **procedure aziendali precise per il telelavoro**, fornendo a dipendenti e collaboratori strumenti tecnologici appositamente destinati allo *smart working*, offrire un **accesso remoto sicuro** ai sistemi aziendali, mantenendoli sempre aggiornati, assicurando la **sicurezza delle comunicazioni aziendali** ma anche fornendo un’adeguata **formazione ai propri dipendenti**, tenendo contatti regolari ma anche effettuando un buon **monitoraggio**. In questo periodo è aumentato anche lo **shopping online** e, per questo, è opportuno fare acquisti su siti web affidabili, magari controllando anche la **reputazione (rating) di venditori o siti di commercio elettronico**. Pensarci due volte prima di fare un acquisto: soprattutto se l’offerta è troppo buona perché sembri vera o se si trova un prodotto in vendita su un sito web mentre è esaurito su tutti gli altri, potrebbe essere una truffa. Se l’**uso delle carte di credito** dovrebbe essere lo strumento di pagamento principale online (alcune carte di credito offrono anche certe forme di assicurazione degli acquisti), è sempre bene controllare periodicamente l’estratto conto o il proprio conto bancario, per **osservare eventuali movimenti sospetti** in tempo utile. I **bambini** e gli **adolescenti** hanno bisogno di un’attenzione maggiore quando usano strumenti connessi alla rete o i cosiddetti ***smart toys*** (i giocattoli intelligenti). Pertanto, è cosa buona e giusta cambiare le password assegnate automaticamente dai costruttori e controllare le impostazioni di sicurezza e privacy degli *smart toys*. Il ruolo dei genitori è altresì importante: essi devono **parlare con i figli delle minacce che si trovano in rete e delle precauzioni da adottare**. Analogamente, **i genitori devono ascoltare i figli circa le loro esperienze online**, spiegando loro l’importanza di

stare attenti nella *vita online* così come nella *vita offline*. Ovviamente, tutto questo presuppone dei genitori che si aggiornino costantemente sulle nuove tecnologie che usano i figli. Infine, laddove vogliamo essere solidali con gli altri, è bene fare **donazioni online solamente tramite siti web ed app accreditati**, controllando la loro autenticità. Ugualmente, non inviare mai denaro online direttamente ad una persona. Quindi, **attenzione a condividere informazioni finanziarie personali** (dettagli della carta di credito, dati bancari ecc.). Ancora, non rispondere a messaggi o chiamate sospette e non aprire link o allegati che si trovano in email arrivateci chissà da dove e quando. Ricordiamoci anche che viviamo in un'epoca di ***fake news***: prima di condividere una notizia è bene controllare che la fonte sia attendibile e che la notizia sia recente.