Bellinzona, 02.04.2020

9 accorgimenti per lavorare da casa in piena sicurezza

1. **Attenzione al luogo dove depositi (e salvi) i documenti**
   Se lavori da casa, sicuramente ti hanno fornito le credenziali per collegarti alla rete aziendale attraverso una rete virtuale privata di tipo VPN (Virtual Private Network). In questo modo il trasferimento dei dati gode di un buon grado di sicurezza. Tuttavia, assicurati che i dati che salvi sul tuo apparecchio elettronico, una volta disconnesso dal VPN, non vengano lasciati incustoditi in aree di lavoro non protette. Ai malintenzionati potrebbe bastare una ricerca in Google strutturata e mirata, come per esempio "*stipendi site:www.ti.ch*" per arrivare astutamente a file dimenticati in zone non adeguatamente protette.

2. **Utilizzo di memorie USB**
   Non collegare mai al tuo apparecchio elettronico aziendale memorie USB sconosciute trovate per casa, ricevute in regalo o prese in prestito da persone non autorizzate dall'azienda, ad eccezione di quelle bonificate digitalmente attraverso un processo completo di formattazione avvenuto su un altro apparecchio elettronico di cui hai il controllo. Le memorie USB sono tra i maggiori vettori di contaminazione (silenziosa) dei dati, usati per introdurre programmi malevoli. Se tuttavia non dovessi avere alternative, assicurati di disporre di un antivirus valido e aggiornato allo stato dell'arte.

3. **Apparecchi elettronici personali e professionali**
   Lavorando da casa spesso il confine che divide gli apparecchi personali da quelli ad uso professionale viene a scemare, soprattutto col passare del tempo. Questo a causa dalla falsa percezione che dentro casa nessuna persona indesiderata possa manipolarli fisicamente. Bisogna tuttavia evitare di lasciare l'apparecchio elettronico professionale privo di una password di protezione, assicurandosi che il timer di attivazione automatico del "blocco schermo" e della password sia impostato con un tempo relativamente breve in caso di inutilizzo.

4. **Altri apparecchi elettronici casalinghi collegati**
   Spesso dentro casa vi sono molteplici apparecchi elettronici collegati alla rete internet domestica, nei quali per comodità si creano cartelle virtuali condivise in cui depositare i dati e i documenti. Per quanto comodi, ricordati di non usare mai questi spazi famigliari per depositare documenti e dati aziendali sensibili, anche solo temporaneamente. Questi sono tra i primi spazi d'archiviazione che i programmi malevoli cercano una volta penetrati nella rete domestica.

5. **Collegamenti a sistemi di cloud esterni**
   Utilizzare sistemi di cloud offre senza dubbio molteplici vantaggi di condivisione e accesso rapido ai dati, soprattutto a distanza, ma spesso pone di fronte a molti rischi dovuti al fatto che i sistemi di carattere gratuito dichiarano nelle condizioni d'uso di poter fare un uso dei tuoi dati contrario alle disposizione del datore di lavoro e alla natura confidenziale dei documenti stessi, mettendo

seriamente in pericolo la reputazione del tuo datore di lavoro, oltre alla sicurezza stessa dei dati sensibili professionali. Seppur comodi, evita in modo assoluto l'utilizzo di sistemi di cloud gratuiti o non autorizzati dall'azienda.

6. **Aggiornamento di tutti gli apparecchi elettronici di casa**
   Assicurarti che tutti gli apparecchi elettronici che hai dentro casa dispongano di un antivirus adeguato e sempre aggiornato. Basta soltanto che uno di questi apparecchi collegato alla rete domestica non sia adeguatamente protetto per mettere a rischio la sicurezza di tutti gli altri apparecchi e, in particolare, per diventare un "cavallo di troia" per risalire e accedere a quello aziendale con i dati sensibili. Ricorda che l'arrivo del 5G potrebbe portare dentro casa oggetti ludici, come giochi per bambini, anch'essi collegati e interconnessi alla rete casalinga aumentando così i potenziali rischi.

7. **Le videoconferenze? Utili e necessarie, ma… attenzione!**
   Affinché i contenuti delle videoconferenze restino confidenziali, confrontati con il tuo datore di lavoro sulla piattaforma più indicata da utilizzare a questo scopo. Sussiste infatti il pericolo che alcune piattaforme di videoconferenza gratuite (per esempio zoom.com) utilizzino i propri dati per condividerli o venderli a terze parti per scopo commerciale. Per maggiori informazioni vi segnaliamo un articolo sul tema, proveniente da una fonte autorevole: https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook

8. **Quando termini il lavoro**
   Quando termini il lavoro assicurati che sull'apparecchio elettronico aziendale non rimangano documenti di lavoro incustoditi, per esempio sul desktop o in cartelle temporanee non adeguatamente protette. Controlla sempre di aver salvato tutti i file negli spazi virtuali appositi senza lasciare nulla in giro, anche quando la stanchezza, la fretta o la pressione potrebbero farti abbassare la guardia.

9. **…e non dimenticarti dei documenti cartacei e delle conversazioni telefoniche.**
   Quando lavori da casa, o in un ambiente pubblico, devi sempre ricordarti che non ti trovi in ufficio – a maggior ragione se condividi i tuoi spazi con altri. Assicurati quindi di depositare documenti confidenziali, contenenti dati sensibili o ad esclusivo uso interno, in un luogo sicuro. Inoltre, quando effettui delle conversazioni telefoniche o delle videoconferenze, assicurati che persone non autorizzate vengano a conoscenza di informazioni confidenziali o sensibili.

Buon lavoro in sicurezza!

Il gruppo Cyber sicuro
www.cybersicuro.ch