Riassunto per punti delle attenzioni da tenere

1. A inizio giornata accedo al **PC personale** con l'utenza **SmartWork** o al **portatile** fornito **dall'Ateneo** con le **credenziali di Ateneo** o quelle concordate con il Dipartimento.
2. **Preferisco** sempre la modalità con **VPN accesa**. Male non fa. Mi fa passare attraverso i nostri firewall e quindi aumenta il livello di protezione della mia navigazione.
   E' vero che alcuni applicativi in Cineca (U-Gov, ESSE3, ...) sono accessibili anche senza VPN ma la tengo come modalità di riserva nel caso qualcosa non funzioni (e magari poi lo segnalo).
3. La **VPN** è **NECESSARIA** per poter accedere agli applicativi su Intranet come **Cartellino**, **Titulus**, **Rassegna Stampa** ed altri applicativi vari. Diversamente NON funziona. Con la VPN attiva si accede anche alle **Risorse Bibliografiche** dell'Università di Trieste.
4. La **VPN** è **NECESSARIA** per poter fare una connessione al **Desktop Remoto** verso i PC dell'Ateneo, diversamente NON funziona.
5. **NON utilizzo** la **VPN** se faccio una **videoconferenza** perché non è necessaria e introduce ritardi che possono impattare negativamente sulla videoconferenza.
6. La **modalità corretta per lavorare** nella massima protezione è via **Desktop Remoto direttamente nel PC dell'ufficio**. Tutto resta là e quando tornerò al lavoro non rischio di lasciare pezzi a casa.
7. Se devo lavorare su materiali presenti sui **dischi di rete** è **NECESSARIO** eseguire una connessione in **Desktop Remoto**.
8. **Copiare i file dal lavoro al PC di casa** per elaborarli in locale va fatto **solo in caso di reale necessità** (es ci devo lavorare per forza offline perché spengo la saponetta...). Se lo faccio, a fine giornata riposiziono i file al lavoro e cancello quelli in locale.
9. Mi ricordo di **spegnere** la **VPN a fine sessione** lavorativa. Così evito di veicolare traffico personale sulla Rete della Ricerca e velocizzo la navigazione su servizi non universitari.

Cose da EVITARE

Perché deteriorano la connessione:

- Collegarsi al wifi quando ci si può collegare via cavo
- Collegarsi via rete 4G/5G quando ci si può collegare con ADSL o VDSL o fibra.
- Collegarsi a reti di telefonia mobile 2G/3G/EDGE o via modem telefonico o ISDN
- Attivare la VPN quando ci si collega ad una videoconferenza

Perché sono un rischio per la sicurezza:

- Usare una rete Wi-Fi senza password o non propria (dei vicini, di un esercizio commerciale, del comune)
- Usare password corte o prevedibili (con un significato in qualsiasi lingua)
- Collegarsi al lavoro senza usare una VPN
- Collegarsi al lavoro con un account amministrativo dal PC di casa
- Usare un sistema operativo non aggiornato
- Usare windows 8.1 o macOS senza antivirus
- Salvare documenti lavorativi sul proprio PC
- Cliccare sui link senza controllare dove portano
- Cliccare su allegati email sospetti
- Collegarsi a siti con lucchetto aperto o che attivano avvisi di sicurezza
- Allontanarsi dalla postazione lasciando il pc acceso con sessioni di desktop remoto attive in presenza di conviventi
- Lasciare aperte delle sessioni di lavoro a fine attività lavorativa
- Collegare chiavette USB di origine sconosciuta