Misure di cybersecurity e protezione dati da osservare durante il lavoro in vpn non in modalità agile

Sommario

Lavorare da Remoto in modo sicuro in 13 punti

1. **Per accedere in modo sicuro e confidenziale alle risorse informatiche protette di Ateneo utilizza la VPN fornita dall'Università e sconnettiti quando navighi liberamente**

2. **Configura una buona password, lunga e complessa, sulla tua connessione Wi-Fi per garantire che il tuo traffico non possa essere intercettato facilmente**

3. **Crea sul tuo computer un utente specifico dedicato allo smartworking per tenere separato l'ambiente di lavoro da quello personale e imposta il blocco del computer quando ti allontani dalla postazione**

4. **Utilizza sempre un Antivirus mantenendolo sempre aggiornato e se non lo hai già puoi utilizzare l'Antivirus fornito dall'Ateneo**

5. **Evita di collegare dispositivi esterni (penna USB, Hard Disk esterni) di cui non conosci la provenienza**

6. **Per lavorare utilizza sempre gli strumenti di Ateneo per salvare e o condividere dati (es. Unimibox, Dataserver, ecc.) che garantiscono maggior affidabilità oltre che il backup dei dati. Non salvare documenti sul PC o in archivi personali**

7. **Stai sempre allerta quando leggi le mail evitando di scaricare allegati o cliccare su link ricevuti in e-mail da mittenti sconosciuti. Prediligi l'uso della webmail ed evita di usare la casella di posta come archivio di dati**

8. **Presta attenzione durante la navigazione in Internet evitando siti sconosciuti e rischiosi**

9. **Usa sistemi operativi e software aggiornati all'ultima versione disponibile evitando di installare programmi non più aggiornabili; non installare software provenienti da fonti non ufficiali, in particolare programmi, software o file che violino la licenza d'uso, illegali o modificati illegalmente**

10. **Utilizza delle password robuste (lunghe e complesse) e differenziate per i vari servizi creandone 1 per l'accesso al PC, 1 per i servizi di Unimi e tante password diverse quanti sono i servizi esterni che utilizzi**

11. **Come strumento per riunioni e meeting prediligi Microsoft Teams**

12. **Effettua sempre il log out dai Servizi/Portali di Ateneo**

13. **Se ritieni di aver subito un incidente informatico (allarme antivirus che segnali un software pericoloso; apertura erronea di allegati di una mail insidiosa) comunica**

l'accaduto con una mail a sicurezza@unimi.it **- se nell'incidente sospetti una violazione di dati personali scrivi a** violazione.dati@unimi.it

Premessa

Tutti i dipendenti dell'ente sono tenuti a seguire le indicazioni e le disposizioni dell'Università degli Studi di Milano in materia di sicurezza informatica e protezione dati personali, anche quando operano in modalità agile e ad agire in modo conforme alle normative vigenti.

In relazione al trattamento di dati personali, si ricorda che l'Università degli Studi di Milano, in qualità di titolare del trattamento dei dati personali dell'Ateneo, dispone che chiunque abbia accesso a dati personali, li consulti, li archivi, li diffonda, li modifichi, li raccolga o, comunque, effettui qualsiasi operazione su informazioni, sia in formato elettronico che cartaceo, , non possa trattare tali dati se non con modalità descritte nella **circolare rettorale 164/2019 del 30/10/2019 e nei suoi allegati che ne costituiscono parte integrante.** Le istruzioni dell'Ateneo per il trattamento dei dati personali sono reperibili nell'apposita sezione dedicata alla Sicurezza Informatica e alla Protezione dei dati, del portale work.unimi.it ai link qui di seguito riportati:

- Istruzioni per il trattamento dati
- Istruzioni per proteggersi dal phishing
- Istruzioni per la protezione da Data Breach

Tali istruzioni sono da considerarsi valide a tutti gli effetti anche nel caso la prestazione lavorativa sia resa in modalità agile.

In questo caso particolare devono essere prese ulteriori misure e cautele per la protezione delle informazioni trattate

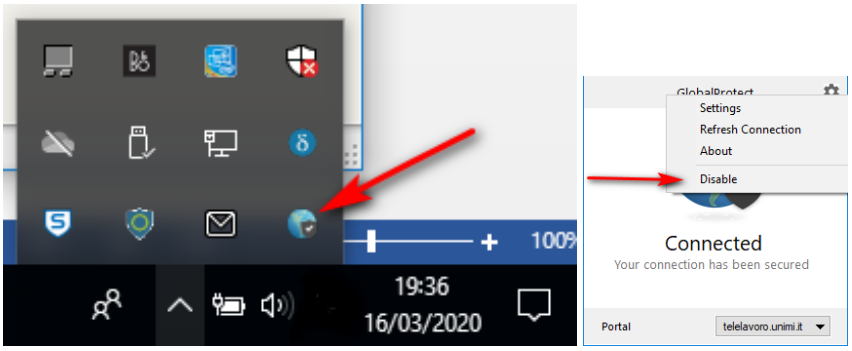
Indicazioni da seguire

Accesso sicuro alla rete di Ateneo

Dal proprio domicilio per accedere in modo sicuro e confidenziale alle risorse informatiche (sistemi, servizi informatici e dati) dell'Ateneo, è necessario l'utilizzo del servizio di VPN offerto dal Settore Cybersecurity, Protezione Dati e Conformità. Le informazioni per utilizzare il servizio sono disponibili al link Istruzioni VPN

Si fa presente a tutti gli utenti che la VPN è ad uso esclusivo lavorativo, pertanto si invita a disconnettere la VPN dalla propria postazione di lavoro remota ogni qual volta si intenda navigare in rete per questioni personali e per attività di natura non lavorativa. Per garantire una maggior separazione tra le attività lavorative e quelle personali anche durante la fascia oraria lavorativa è dunque sempre possibile disconnettere temporaneamente la VPN per ripristinarla quando riprendono le attività di lavoro.

Per disconnettere la VPN è sufficiente posizionarsi sull'icona del Global Protect, e posizionarsi sulla rotellina dell'ingranaggio e cliccare su "**Disable**" come mostrato in figura.



Per ripristinare la VPN è sufficiente posizionarsi sull'icona del programma Global Protect, in basso a destra (Fig 1) e rappresentata da un mappamondo e cliccare su ENABLE (Fig 2). Dopo pochi secondi il sistema è già pronto ad operare in VPN.

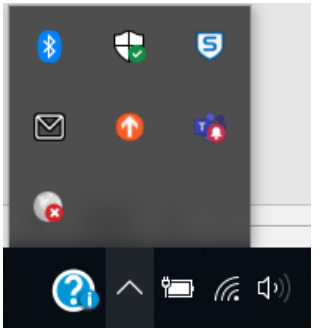


Figura 1

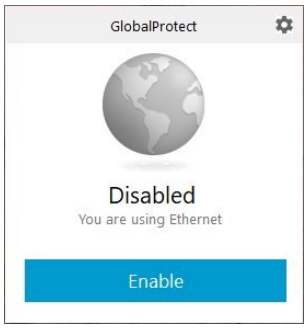
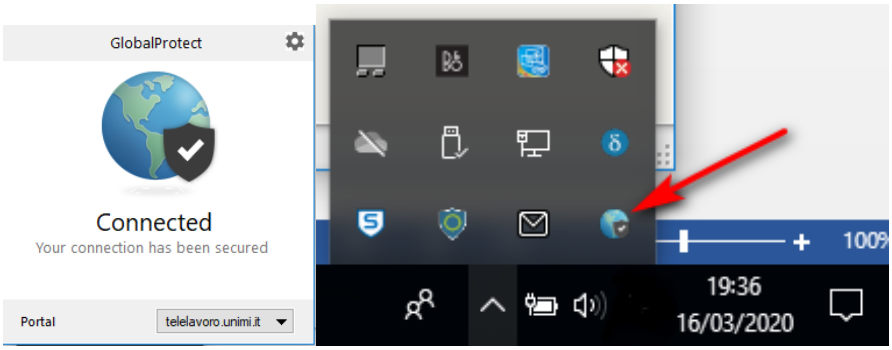


Figura 2

Dovrebbe apparire la l'icona che indica che la connessione è stata stabilita:



Connettività alla rete

Il servizio VPN descritto in precedenza garantisce un alto livello di confidenzialità della connessione alla rete. Pertanto, nel caso si stia lavorando da casa e non si stia usando la VPN di Ateneo, è bene ricordare che quando ci si connette alla rete dati domestica è buona norma essersi sincerati che sia stata modificata la password di default, impostata generalmente dal produttore del dispositivo, della connessione alla rete Wi-Fi di casa e la password di default di amministrazione del router Wi-Fi in quanto queste password potrebbero essere note ad altri o insicure. Inoltre per lavorare da remoto è sempre consigliato, se non si sta usando la VPN di Ateneo, di non connettersi mai da hot spot pubblici come ad esempio aeroporti, stazioni, bar ecc.

Accesso e Gestione del PC e dei dispositivi usati per il lavoro da remoto tramite vpn

I dispositivi personali utilizzati per le attività lavorative devono essere usati con la massima diligenza sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro (Università o al proprio domicilio), avendo cura di adottare gli accorgimenti e le misure utili ad evitare il verificarsi di danni o sottrazioni di dati. A tal proposito occorre prestare particolare attenzione a non lasciare incustoditi i dispositivi portatili in auto, su treni o aerei.

I dispositivi devono essere integri non devono, cioè, essere stati sottoposti a operazioni che possano compromettere il corretto funzionamento dei meccanismi di protezione del software quali ad esempio jailbreaking e rooting dei dispositivi portatili o installazione di software non correttamente licenziato nei PC. È responsabilità degli utenti effettuare questa verifica.

I dispositivi devono sempre essere protetti da sistemi di autenticazione (ad es. username e password). È consigliato creare una utenza specifica, senza poteri di amministrazione del dispositivo, dedicata al lavoro agile e protetta da uno username e da una password che devono essere diverse dalle credenziali di Ateneo.

Stessa precauzione si può applicare sui dispositivi portatili Android, dove è possibile attivare un apposito profilo di lavoro e separare in questo modo i dati privati da quelli legati ad esigenze lavorative. Istruzioni dettagliate su come creare il profilo di lavoro sono pubblicate sul sito di supporto di Android

Deve essere anche previsto il salvaschermo (screensaver) con blocco automatico della sessione protetta da credenziali di autenticazione dopo al massimo 5 minuti di inattività.

È necessario che sulla postazione siano attivi sia il firewall personale che l'antivirus; questo significa che nell'angolo destro della barra delle applicazioni devo essere presenti le seguenti icone:

Per attivare il firewall di Windows seguire le seguenti istruzioni

Qualora l'antivirus non fosse installato si DEVE procedere alla sua installazione.

Antivirus

Il PC utilizzato per accedere da remoto alle risorse di Ateneo deve obbligatoriamente essere dotato di un sistema antivirus conforme ed automaticamente e costantemente aggiornato. Se non si dispone già sul proprio pc di un Antivirus, il personale strutturato può utilizzare l'antivirus di Ateneo (Sophos). Le informazioni e le modalità per l'installazione dell'Antivirus di Ateneo sono reperibili sul portale di Ateneo alla pagina dedicata al servizio antivirus. I pc e portatili forniti dall'Amministrazione hanno già l'Antivirus di Ateneo installato.

Dispositivi Esterni

Bisogna evitare di collegare al PC dispositivi mobili (penna USB, hard disk esterno ecc.) di cui non si conosce la provenienza, mentre quelli che si usano abitualmente vanno scansionati regolarmente con l'antivirus.

Strumenti di Ateneo

I lavoratori nello svolgimento delle proprie attività, seppur lavorando in modalità agile, devono attenersi alle istruzioni impartite dai propri responsabili e, nell'ambito dell'attività assegnata, utilizzare gli strumenti di lavoro forniti dall'Ateneo. È importante non salvare i dati relativi al

proprio lavoro direttamente sul proprio computer, in quanto potrebbe non essere garantito un adeguato livello di protezione. E', quindi, necessario utilizzare sempre le soluzioni e gli strumenti di Ateneo che permettono di salvare i dati in remoto e garantiscono, in modo trasparente all'utente, la protezione e il backup dei dati.

A questo proposito gli utenti dell'Amministrazione Centrale possono accedere agli archivi presenti su Dataserver seguendo queste istruzioni. Gli utenti dei Dipartimenti possono utilizzare i file server o altre risorse eventualmente messe a disposizione all'interno della propria struttura. Tutti gli utenti dotati di credenziali @unimi.it possono condividere file e dati con altri soggetti autorizzati mediante il sistema di Ateneo Unimibox.

Posta elettronica

E' necessario prestare la massima attenzione nella gestione delle mail in arrivo nella propria casella di lavoro. Le email con particolari richieste o contenenti link sospetti devono essere trattate con la massima cautela. Alcune informazioni possono essere trovate nella Guida pratica per analizzare le email e Indicazioni utili a proteggersi dal Phishing pubblicate sul portale work.unimi.it nell'apposita sezione "Sicurezza informatica e protezione dei dati personali".

E' da privilegiare, ove possibile, la gestione della posta elettronica di Ateneo tramite webmail in luogo dell'installazione, sul proprio dispositivo, di un programma di posta elettronica (ad esempio Outlook o Thunderbird); ciò consente di evitare di salvare la posta di lavoro sul proprio PC in quanto potrebbero esservi mail contenenti dati personali o informazioni riservate. Si ricorda inoltre che la casella di posta non deve essere utilizzata mai come archivio. Nel caso in cui si ricevano documenti contenenti dati qualificabili come particolari[1] (ex sensibili) e di pertinenza dell'Ateneo, per il rispetto delle norme sulla protezione dei dati, si richiede di salvarli immediatamente negli spazi di archiviazione remota messi a disposizione dall'Ateneo e cancellarli dalla propria casella di posta elettronica.

Navigazione

Ciascun utente deve prestare molta attenzione alla navigazione, evitando di navigare in siti sconosciuti o potenzialmente rischiosi. L'attenzione e le precauzioni durante la navigazione

[1] **Dato particolare:** i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

devono essere elevate in quanto l'infezione del pc o del dispositivo potrebbe comportare danni alle risorse personali e di Ateneo.

Software installato

Al fine di garantire un elevato livello di sicurezza del sistema operativo e degli applicativi installati sul pc e sui dispositivi mobili utilizzati per le attività lavorative, è indispensabile che gli stessi siano costantemente aggiornati e che siano applicate tempestivamente le patch di sicurezza appena disponibili. Sul PC usato smart working si raccomanda di non utilizzare mai software non aggiornati, con licenza scaduta o non più supportati dal fornitore. Devono essere installati SOLO programmi, o applicativi software regolarmente licenziati e non provenienti da supporti o siti non ufficiali, che potrebbero comportare l'installazione di programmi malevoli.

Politica di gestione password

Le password utilizzate per il lavoro agile come per ogni altra attività devono essere robuste ovvero con lunghezza idonea di almeno 8 caratteri, formate da lettere maiuscole e minuscole, numeri e/o caratteri e sempre diverse da quelle utilizzate in precedenza.

È opportuno che ogni utente disponga di password che devono essere diverse per ogni servizio utilizzato in particolare:

1. una password per accedere alla postazione del lavoro;
2. una password per accedere ai servizi di UNIMI utili allo svolgimento del lavoro agile;
3. altre password personali per svolgere attività non istituzionali.

È importante non salvare le password sul browser e si ricorda, inoltre, che le credenziali utilizzate per lo svolgimento di attività lavorative non possono assolutamente essere comunicate o condivise con terzi, ivi compresi i colleghi.

Poiché l'uso di numerose password risulta spesso di difficile gestione è consigliato l'uso di un password manager che consente la memorizzazione e la gestione sicura di password multiple. I password manager sono programmi o app che archiviano in modo sicuro e cifrato le credenziali (username e password) di accesso ai servizi web e non solo, in una sorta di cassaforte ("Vault") virtuale, rendendola disponibile all'utente quando ne avrà bisogno. Sono protetti da una Master Password, che serve per aprirli e diventa perciò l'unica password che occorre ricordare inoltre hanno la capacità di generare automaticamente password sicure e complesse.

Un esempio di questo tipo di strumento, libero e disponibile per le piattaforme più diffuse, è KeePass

Strumenti per meeting e riunioni

Per le riunioni a distanza, l'Ateneo mette a disposizione Microsoft Teams come strumento di collaborazione istituzionale.

Log out dai servizi/portali di Ateneo

Dopo aver utilizzato i servizi ed i portali di Ateneo ed in generale tutti i servizi che richiedono l'autenticazione iniziale è sempre buona norma effettuare il log out cliccando sul tasto apposito: questo per evitare attacchi informatici che sfruttano le autenticazioni sui servizi ancora attivi.

Cosa fare in caso di problemi di sicurezza informatica o di sospetta violazione dati

Il dipendente che operando da remoto riscontri problemi di sicurezza informatica, quali una segnalazione dell'antivirus, apra erroneamente un allegato di un messaggio di posta elettronica di dubbia provenienza, subisca un furto o smarrisca il proprio dispositivo ecc. è tenuto ad avvisare il Settore Cybersecurity, Protezione Dati e Conformità inviando immediatamente una email a **sicurezza@unimi.it** .

Nel caso di sospetta violazione di dati personali, ad esempio a seguito dello smarrimento o furto del dispositivo o del pc, è necessario segnalare immediatamente l'accaduto all'Unità di Staff Cybersecurity, Protezione Dati e Conformità e al Responsabile della Protezione Dati di Ateneo inviando una mail a **violazione.dati@unimi.it** secondo queste istruzioni

Si rammenta che nel caso di furto o smarrimento del dispositivo acquisito con fondi/risorse di Ateneo è necessario recarsi a denunciare l'accaduto alle competenti forze dell'ordine entro 15gg o, in caso di *furto con destrezza*[2], entro 72 ore. Dopo aver effettuato la denuncia, è necessario trasmetterla a violazione.dati@unimi.it in modo da poter avviare la pratica assicurativa.

Riferimenti e approfondimenti

Per gli approfondimenti e gli aggiornamenti di quanto descritto nel presente documento, per le modalità di implementazione delle misure di sicurezza richieste e per la consultazione del materiale divulgativo in tema di protezione dei dati personali e sicurezza informatica, è possibile fare riferimento ai documenti del Settore Cybersecurity, Protezione Dati e Conformità di Ateneo pubblicati sul portale nella sezione dedicata alla "Sicurezza informatica e protezione dei dati personali" e in particolare:

[2] Per furto con destrezza si intende il furto compiuto con **agilità, l'astuzia e la rapidità di gesti** del colpevole considerati superiori a quelli utilizzati dal ladro comune e tali da permettere di eludere la vigilanza normale dell'assegnatario del dispositivo.

Sicurezza Informatica e Protezione dei Dati Personali

Regolamenti Istruzioni e Linee Guida

Avvisi di Sicurezza

Settore Cybersecurity, Protezione Dati e Conformità

Il Responsabile

Dott.ssa Nicla Ivana Diomede