**JUST Training Fiche:**

**Interagire in sicurezza in un ambiente digitale**

|  |  |
| --- | --- |
| **Titolo** | Interagire in sicurezza in un ambiente digitale |
| **Parole Chiave** | Cybersecurity, The Cloud, Privacy, Netiquette |
| **Fornito da** | Internet Web Solutions |
| **Lingua** | Italiano |
| **Obiettivi generali** | Gli obiettivi di questo modulo sono spiegare l'importanza di mantenere buone pratiche di sicurezza informatica, evidenziare l'importanza della protezione delle informazioni personali e fornire un'idea generale degli strumenti di sicurezza informatica più pratici ed efficaci. |
| **Risultati formativi**  | * Acquisire familiarità con la sicurezza informatica: i protocolli sono importanti quanto le applicazioni.
* Sviluppare la responsabilità: Netiquette e buon senso sono particolarmente importanti.
* Comprendere come mantenere la privacy: prestare molta attenzione ai contenuti condivisi online.
* Comprendere gli strumenti di utilità, come VPN, Antimalware e app cloud.
 |
| **Training Area** | **Business Etiquette** |   |
| **Digital Skills** | **X** |
| **Soft Skills** |  |
| **Smart Working** |  |
| **Indice dei contenuti** | **Interagire in sicurezza nell’ ambiente digitale****Unità 1: Suggerimenti e trucchi per la sicurezza informatica**Sezione 1.1: IntroduzioneSezione 1.2: Tieniti aggiornatoSezione 1.3: Usa il backup!Sezione 1.4: Passwords and authentications a più fattori.**Unità 2: Pratiche sicure**Sezione 2.1: Salvaguarda la tua privacySezione 2.2: Guarda le tue netiquette**Unità 3: Strumenti per migliorare la sicurezza delle ICT**Sezione 3.1: VPNsSezione 3.2: AntimalwareSezione 3.3: The Cloud |
| **Contenuto del training**  | **Interagire in sicurezza in un ambiente digitale****Unità 1: Cybersecurity: suggerimenti e trucchi****Introduzione**Viviamo in un mondo sempre più interconnesso. Ciò comprende la sensazione della necessità di condividere il meglio del nostro ultimo viaggio nella nostra cerchia di Instagram o di spostare l'argomento dal tempo libero al lavoro, ogni chiamata o scambio di e-mail a cui partecipiamo durante la nostra vita educativa e/o lavorativa.Inconsapevolmente, questi scambi di informazioni contengono moltissimi dati su di noi, spesso sensibili, che possono essere rubati e raccolti da persone che vogliono approfittarne illegalmente.Ecco perché avere protocolli di sicurezza informatica o solo pratiche (che non significa solo installare un antivirus e poi smettere di preoccuparsi) è essenziale per la nostra vita online.**Tieniti aggiornato**I nostri dispositivi di solito ci infastidiscono con scomode notifiche di "nuovo aggiornamento software". Nonostante a volte non cambino nulla a prima vista, questi aggiornamenti sono molto utili, poiché correggono bug scoperti di recente e problemi di sicurezza che potrebbero rappresentare un rischio per i nostri dispositivi e le informazioni che contengono.Tuttavia, questi aggiornamenti software potrebbero essere di breve durata poiché gli hacker sono sempre alla ricerca di vulnerabilità del software, il che sottolinea l'importanza di mantenere aggiornati i nostri dispositivi.**Usa il backup!**Mantenere una copia separata e aggiuntiva dei tuoi file è una scommessa sicura quando, nonostante i nostri sforzi, accade il peggio e i file vengono danneggiati o il nostro sistema subisce un attacco informatico. Per evitarlo, i nostri file possono essere archiviati in modo sicuro in un'unità esterna e/o in applicazioni cloud online.Contrariamente a quanto si crede, le versioni di backup dovrebbero essere create durante il processo di elaborazione e non solo una volta terminato il file. In questo modo, puoi facilmente tornare indietro alle iterazioni precedenti del file nel caso in cui qualcosa vada storto con la bozza centrale.**Passwords and autenticazione a più fattori.**Spesso trascurate, le password sono una parte vitale della sicurezza informatica. Nonostante la seccatura di ricordarle e introdurle password lunghe e perfette per i caratteri con m4nY! i tipi di personaggi possibili sono un must. Inutile dire che usare la tua data di nascita (e simili) non è un'opzione.Inoltre, a causa delle frequenti violazioni della sicurezza, le password possono essere facilmente compromesse, quindi conserva password diverse su ogni dispositivo o account e ricordati di cambiarle regolarmente!L'autenticazione a più fattori è un sistema che rende più difficile per i criminali informatici richiedendo credenziali aggiuntive oltre alla password per accedere al tuo account, ad esempio un codice SMS, una chiamata o l'utilizzo di una applicazione specifica.**Unità 2: Pratiche di sicurezza****Salvaguarda la tua privacy!**Tendiamo ad associare la sicurezza informatica agli hacker che utilizzano strumenti all'avanguardia per entrare nei nostri account. La verità è che la maggior parte del loro successo deriva dalla ricerca su Google e dalla raccolta di "informazioni pubbliche" da social media, blog e forum.In questo modo, se ci piace utilizzare per le nostre password una combinazione del nome del nostro animale domestico, del cognome della mamma, del numero della porta, ecc., è questione di tempo prima che un hacker riesca a raccogliere tutto qua e là, ricombinarlo e irrompere.Riconsidera cosa significa per te "informazioni private". Torna indietro sulla tua sequenza temporale, cerca eventuali immagini della tua carta d'identità/carta di credito/documenti personali (potrebbero essere saluti, apprezzamenti o post fittizi) ed eliminale. Inoltre, presta attenzione a tutti i profili con troppe informazioni personali non necessarie.Ricorda: se non vuoi che nessuna informazione venga vista da estranei, non pubblicarla!**Quali netiquette**“Netiquette” è un insieme di regole di cortesia pensate per facilitare la convivenza online, proprio come esistono convenzioni sociali per il mondo offline, come salutare, salutare e dire “per favore”.Inoltre, come nella vita reale, è bene considerare che questo codice di condotta non è immutabile e dipende dal contesto. Un buon esempio di ciò è l'insieme di regole solitamente appiccicose pubblicate su gruppi o forum di Facebook.Le regole originali della “netiquette” di Virginia Shea (1994) sono ancora valide con alcuni aggiornamenti, come nel seguente esempio:• Evita di usare le comunità online come sostituti di Google – Fondamentalmente, prova a cercare post/discussioni precedenti che hanno già risposto al problema.• Limitare l'uso di segni di punteggiatura extra, abbreviazioni, emoji, lettere maiuscole e grafie alternative – C0Z N0B0DY wantz T0 R3AD MESSAG3S L1KE th1s, rito???? 😃😃😃• Non inviare spam ai propri prodotti o servizi: di solito ci sono spazi specifici e separati per questo. Se non riesci a vederli, non sei nel posto giusto.• Non inviare alcuna informazione personale o privata – Si prega di fare riferimento alla sezione precedente.• Dare il giusto merito agli autori – Non solo da un punto di vista legale ma anche perché, mentre le persone odiano essere plagiate, amano vedere il proprio lavoro condiviso.**Unità 3: Strumenti per migliorare la sicurezza delle ICT****VPNs**Non tutto sarà misure, regole e abitudini. Fortunatamente, ci sono molti strumenti progettati per combattere le minacce informatiche, come VPN, Antimalware e app Cloud.Le VPN sono filtri che mascherano la tua identità online e crittografano i tuoi dati. Lo fa collegandosi a un server privato che cripta i tuoi dati, bloccando l'accesso esterno ad essi e rendendoli illeggibili in caso di furto.Inoltre, la maggior parte delle VPN ha server in diversi paesi, il che significa che abbiamo molte opzioni per camuffare il nostro IP come straniero e accedere a contenuti geo-bloccati non disponibili nel nostro paese:• NordVPN e Access sono due opzioni a pagamento che ci consentono di navigare in sicurezza.• Inoltre, Surfshark e Tunnelbear offrono piani gratuiti attraenti e affidabili.**Antimalware**Nonostante sia comunemente chiamato "Antivirus", il software Antimalware è progettato per rilevare, mettere in quarantena ed eliminare qualsiasi minaccia informatica, non solo virus.Mentre i virus sono progettati per replicarsi e causare il malfunzionamento dei dispositivi, malware è un termine generico per qualsiasi tipo di software dannoso che diffonde spam e pubblicità e ruba informazioni e password (e potrebbe persino chiedere un riscatto!).Al giorno d'oggi, è vero che la maggior parte dei software antimalware ha una app antivirus e viceversa, con una vasta gamma di funzionalità e modalità:• Per quanto riguarda le opzioni a pagamento, spiccano ESET, Norton e Avast.• Inoltre, anche le versioni gratuite di Malwarebytes e Bitdefender offrono un servizio di prim'ordine.**Il Cloud**Il “Cloud” è un servizio di hosting online che consente agli utenti di caricare, modificare, archiviare e condividere i propri file.L'archiviazione dei file online in server privati ​​salvaguarda tali file da qualsiasi attacco o danneggiamento locale e previene problemi con i dischi rigidi fisici, come mancanza di spazio, perdite o deterioramento. Nonostante il suo nome, "the Cloud" non è un'entità univoca, ma ogni provider ha il proprio, ed è per questo che ci sono diverse opzioni:• Un'opzione popolare nonostante il passaggio ai piani a pagamento, Dropbox offre un piano gratuito da 2 GB.• Con 5 GB e 15 GB, rispettivamente, OneDrive e Google Drive di Microsoft offrono anche una piena integrazione all'interno dei loro ambienti.Infine, sebbene utilizzato principalmente per la condivisione di file, MEGA consente agli utenti gratuiti di archiviare fino a 20 GB. |
| **Glossario** | **Backup**: copia digitale di un file archiviata separatamente e utilizzata in caso di smarrimento o danneggiamento dell'originale.**Autenticazione a più fattori:** Una modalità di accesso che richiede la presentazione di due o più elementi di prova per una maggiore sicurezza.**VPNs:** filtri che mascherano la tua identità online e crittografano i tuoi dati. Lo fa collegandosi a un server privato che cripta i tuoi dati, bloccando l'accesso esterno ad essi e rendendoli illeggibili in caso di furto.**Antimalware:** software progettato per rilevare, mettere in quarantena ed eliminare qualsiasi minaccia informatica, non solo virus.**The Cloud:** Servizio di hosting online che consente agli utenti di caricare, modificare, archiviare e condividere i propri file al riparo da attacchi o danneggiamenti locali. |
| **Questionario di auto-valutazione** | 1. Le Netiquette non prevedono:1. la ricerca di risposte precedenti che potrebbero aiutarti.
2. **l’uso di molte abbreviazioni.**
3. Il dare il giusto peso agli autori.

2. Pubblicare informazioni personali è più sicuro se:1. Postato privatamente
2. **Non è postato**
3. Caricato sullo spazio cloud

3. Gli hacker raccolgono la maggior parte delle loro informazioni sugli utenti medi:1. **Googlando i loro nomi**
2. Usando software sofisticato
3. Estorcendole

4. I virus e malware sono la stessa cosa?1. Si, sono sinonimi.
2. Per niente
3. **I virus sono un sottotipo di malware.**

5. Quale di questi ha più spazio?1. Google Drive
2. Dropbox
3. **Mega**
 |
| **Bibliografia** | * <https://www.ionos.es/digitalguide/online-marketing/redes-sociales/netiquette/#:~:text=Este%20t%C3%A9rmino%20hace%20referencia%20a,t%C3%A9rmino%20netiqueta%2C%20su%20traducci%C3%B3n%20directa>
* <https://www.avast.com/es-es/c-malware-vs-virus#:~:text=%C2%BFCu%C3%A1l%20es%20la%20diferencia%20entre,que%20un%20tipo%20de%20malware>
* <https://www.trellix.com/en-au/security-awareness/ransomware/malware-vs-viruses.html#:~:text=Malware%20is%20a%20catch%2Dall,its%20code%20into%20other%20programs>
 |
| **Resources (videos, reference link)** |  |