A picture containing diagram

Description automatically generatedImmagine che contiene testo, clipart

Descrizione generata automaticamenteLogo

Description automatically generated

Text

Description automatically generated



**DIGITAL CITIZENSHIP**

**MODULE**

**UNIT 10: DIGITAL SECURITY**

|  |
| --- |
| ***SUMMARY OF THE MODULE*** |
| Durante questi moduli verrà introdotta agli studenti la definizione di sicurezza digitale. Gli studenti saranno in grado di assorbire l'importanza della consapevolezza digitale nella nostra vita e anche nell'istruzione. Conosceranno brevemente i suggerimenti per la sicurezza digitale a casa ea scuola. |

TABELLA DEI CONTENUTI

• Definizione di sicurezza digitale 3

• Esempi di sicurezza digitale appropriata e inappropriata 3

• Perché la sicurezza digitale è importante nell'istruzione? 4

• Cos'è la consapevolezza della sicurezza digitale per gli studenti? 5

• Perché la consapevolezza della sicurezza digitale è importante? 6

• 12 consigli sulla sicurezza digitale per gli studenti a casa ea scuola 7,8,9

• Domande di valutazione 10

• Riferimenti 11

DEFINITION

**La sicurezza digitale è le precauzioni elettroniche per garantire la sicurezza.**

**Poiché sempre più informazioni personali vengono archiviate elettronicamente, una strategia per proteggere le proprie informazioni è imperativa. Le persone devono imparare a proteggersi mentre continuano a utilizzare i dispositivi tecnologici.**

**Simile a proteggersi a casa, l'individuo ha bisogno di trovare modi per proteggere i dati elettronici personali (ad esempio, utilizzando software di protezione antivirus, erigendo firewall e facendo backup) (weebly.com)**

**ESEMPI DI SICUREZZA DIGITALE INADEGUATA**

**-Gli utenti non riescono a mantenere il software aggiornato**

**aggiornamenti o patch che proteggono i loro computer da**

**virus e spiegazione.**

**-Gli utenti non riescono a proteggere la propria identità quando utilizzano la posta elettronica,**

**social network o messaggi di testo.**



**ESEMPI DI SICUREZZA DIGITALE ADEGUATA**

**-Gli utenti si prendono il tempo per assicurarsi che la protezione antivirus e i firewall siano correttamente non datati e configurati per proteggere le informazioni personali.**

**-Insegnanti e genitori parlano agli studenti dei pericoli insiti nel fornire informazioni a chiunque tramite Internet. (weebly.com)**

**PERCHÉ LA SICUREZZA DIGITALE È IMPORTANTE NELL'ISTRUZIONE?**

L'importanza della sicurezza digitale nelle istituzioni educative è in continua crescita. Lo sviluppo dei computer e di Internet ha reso la vita più facile per le persone nelle istituzioni educative e in altre istituzioni.

Ha anche dato l'opportunità agli istituti di istruzione di essere più efficaci ed efficienti nelle loro operazioni.

Tuttavia, è anche un dato di fatto che la stessa tecnologia che rende la vita più facile alle persone può anche rendere la loro vita miserabile se viene utilizzata in modo improprio.

Internet e i computer sono diventati una parte essenziale della nostra vita quotidiana, indipendentemente dal fatto che lavoriamo o studiamo a casa, a scuola o all'università o anche sul posto di lavoro.

È quindi molto essenziale mantenere i computer al sicuro dagli hacker in modo che le informazioni personali di studenti, membri del personale e insegnanti non vengano utilizzate in modo improprio da persone senza scrupoli che potrebbero essere interessate ad acquisire informazioni riservate su studenti/personale/insegnanti a loro insaputa in modo da usarlo contro di loro in seguito. (James K.,2022)



L'importanza della sicurezza digitale negli istituti di istruzione non può essere sopravvalutata perché la tecnologia dell'informazione sta svolgendo un ruolo vitale negli istituti di istruzione.

È quindi molto importante proteggere i computer e Internet da persone non autorizzate in modo che le informazioni, che rappresentano un bene prezioso per qualsiasi istituto di istruzione, rimangano al sicuro.

Non dobbiamo dimenticare che la tecnologia dell'informazione ha reso le istituzioni educative più efficaci ed efficienti nelle loro operazioni.

Pertanto, è molto essenziale garantire la sicurezza informatica negli istituti di istruzione in modo da poter sfruttare appieno questa tecnologia. (James K.,2022)

**COS'È LA CONSAPEVOLEZZA DELLA SICUREZZA DIGITALE PER GLI STUDENTI?**



La sicurezza digitale è un settore fiorente nel mondo dell'istruzione. Con così tanti studenti che accedono quotidianamente a Internet, ci sono molte opportunità per i criminali informatici di rubare password o informazioni personali.

La formazione sulla consapevolezza della sicurezza digitale è importante perché insegna agli studenti come proteggersi dagli attacchi informatici. Gli studenti impareranno a conoscere truffe di phishing, malware, ransomware e altre minacce informatiche.

Questo è assolutamente necessario per le scuole per proteggere gli studenti. Le scuole devono proteggersi dagli hacker installando firewall, protezione da malware e altre protezioni.

La scuola deve assicurarsi che tutti i dispositivi connessi alla propria rete Wi-Fi siano protetti da password complesse.

Gli educatori possono insegnare la sicurezza digitale in classe o i genitori possono insegnarla a casa.

La consapevolezza della sicurezza digitale per gli studenti include anche insegnare loro a essere consapevoli delle minacce e dei rischi che derivano dall'uso della tecnologia. Inoltre insegna loro come utilizzare la tecnologia in modo sicuro e responsabile.

PERCHÉ È IMPORTANTE LA CONSAPEVOLEZZA DELLA SICUREZZA DIGITALE?

Internet ha reso le informazioni ampiamente disponibili al pubblico in ogni momento, il che è sia una benedizione che una maledizione. È fondamentale per qualsiasi tipo di attività, comprese le istituzioni educative.

La legislazione sulla privacy ha definito le informazioni personali come un bene essenziale che non può essere scambiato o venduto senza consenso. Se queste informazioni cadono nelle mani sbagliate, possono portare al furto di identità che crea gravi conseguenze a lungo termine.

Quando si tratta specificamente di istruzione, ciò significa che ci sono molte opportunità per gli studenti di accedere ai materiali del corso online, ma anche più pericoli.

La consapevolezza della sicurezza informatica è di fondamentale importanza perché può aiutarci a identificare potenziali minacce prima che si verifichino. Ci fornisce inoltre le conoscenze necessarie per proteggerci da siti o attacchi dannosi. Per questo motivo, è l'unico modo per proteggere gli istituti scolastici dalle minacce informatiche. Uno degli aspetti più importanti della protezione di un istituto dagli attacchi informatici è la consapevolezza, in modo che studenti e membri del personale sappiano cosa devono fare per proteggersi.

I programmi di sensibilizzazione alla sicurezza digitale dovrebbero essere obbligatori nelle scuole in modo che tutti possano imparare a stare al sicuro online. La maggior parte degli hacker è motivata dalla sfida e non dalla ricompensa finanziaria.

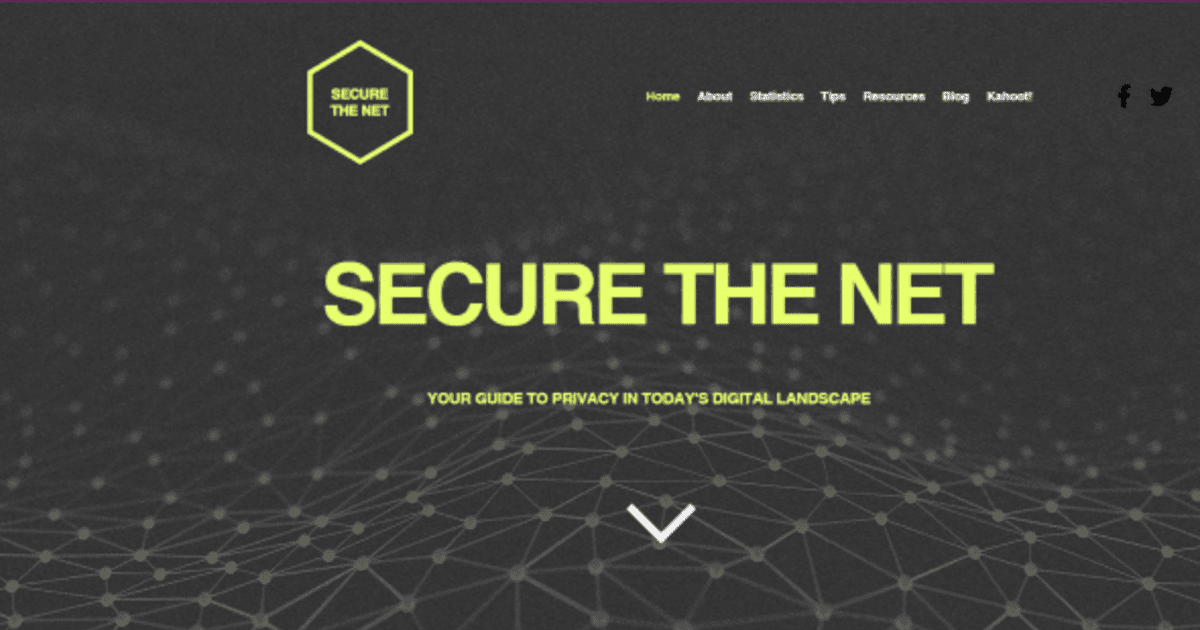
Se un hacker può attirare la tua attenzione, può entrare nel tuo sistema. Ci sono anche gruppi terroristici che hackerano per motivi ideologici.

È noto che questi gruppi prendono di mira o almeno mostrano interesse per scuole e università. Essendo consapevole di come lavorano gli hacker, puoi evitare le loro trappole e proteggere i tuoi dati da loro.

Quando si tratta di minacce informatiche, ciò che non sai PUÒ farti del male. Le scuole sono uno degli obiettivi più vulnerabili per gli attacchi informatici perché dispongono di grandi reti di computer e spesso non applicano i protocolli necessari.

Gli istituti di istruzione devono applicare politiche più severe per garantire la sicurezza degli studenti.

Educare te stesso e il tuo personale sui pericoli di malware, truffe di phishing, attacchi ransomware e altro ti offre le conoscenze e gli strumenti necessari per evitare di diventare un'altra statistica del crimine informatico. (James K., 2022)



## ****12 CONSIGLI SULLA SICUREZZA DIGITALE PER GLI STUDENTI A CASA E A SCUOLA****

## ****1. Proteggi i tuoi social media****

## **Instagram, Twitter e Facebook ti consentono di aggiornare genitori e studenti in modo divertente e coinvolgente. Tuttavia, per continuare in sicurezza, dovrai rivedere le impostazioni sulla privacy di ciascun account per proteggere i diritti alla privacy dei tuoi studenti. Scopri chi può vedere cosa e quale piattaforma condivide quali dati e con chi. Alcuni esempi:**

## **Twitter: imposta l'account Twitter della tua classe su "protetto" in modo che solo le persone che segui possano vedere i tuoi tweet.**

## **Facebook: rendi l'account "Visibile solo agli amici" nelle impostazioni di controllo della privacy.**

## **Sfocare i volti degli studenti: a meno che tu non abbia l'autorizzazione preventiva per utilizzare le loro immagini nei tuoi post, potresti violare i diritti alla privacy di studenti e genitori. Usa un'app gratuita per offuscare i volti dei tuoi studenti e qualsiasi altra informazione che potrebbe rivelare la loro identità.**

## ****2. Utilizza app, strumenti e siti Web che crittografano i dati****

## **La crittografia protegge e protegge tutti i dati che invii online da hacker, ficcanaso in rete e terze parti.**

## **Utilizza siti Web crittografati: utilizza solo siti Web con "https" nel loro URL e un'icona a forma di lucchetto accanto. La "s" sta per "sicuro" (crittografato), il che significa che qualsiasi dato trapelato o ottenuto da parti non autorizzate è inutilizzabile.**

## **Controlla l'informativa sulla privacy delle app: le app iOS impongono a tutti gli utenti di comunicare tramite https, ma lo stesso non può essere garantito per le app Android. È meglio controllare l'informativa sulla privacy di ogni strumento o ispezionare il sito Web per un timbro ufficiale di un'organizzazione per la protezione dei dati.**

## **Classtime, ad esempio, ha firmato l'accordo della California Student Privacy Alliance. Se un'app o un sito Web è coperto dal COPPA (Children's Online Privacy Protection Act), saranno già in atto rigorose misure di sicurezza dei dati.**

## ****3. Avere un piano di recupero****

## **Informare i genitori: gli errori accadono. Potresti aver catturato accidentalmente il nome o l'indirizzo di uno studente in una foto che hai pubblicato sui social media, oppure potrebbe esserci una diffusa violazione di informazioni personali o sensibili. Fai sapere ai genitori se saranno informati per posta o e-mail e chi lo farà: sarà qualcuno del reparto IT o un altro membro senior del personale?**

## **Qual è il piano? Fornire una chiara suddivisione delle misure che verranno intraprese in caso di violazione dei dati. Gli studenti saranno iscritti a un servizio di furto di identità? Aiuterai gli studenti a proteggere i loro account e a reimpostare le loro password in seguito (vedi passaggio 5)? In caso di violazione dei dati aziendali, la scuola, il distretto o lo studente possono richiedere la cancellazione dei propri dati dai server dell'azienda. Vari tipi di violazioni della privacy richiederanno soluzioni diverse.**

### *****4. Usa una VPN*****

### **Per tutte le attività relative all'istruzione: l'accesso alla rete dell'istituto dovrebbe richiedere una connessione VPN privata. Crittografa e quindi protegge il traffico Internet dei tuoi studenti da intercettatori che potrebbero voler rubare le password. Surfshark è un esempio di VPN che potresti prendere in considerazione.**

### **Sul Wi-Fi pubblico: il Wi-Fi pubblico non è protetto, il che lo rende un focolaio per gli hacker. Una VPN protegge il Wi-Fi pubblico crittografando la tua connessione. Ciò consente agli studenti remoti di lavorare dai bar, a casa o nella loro stanza del dormitorio senza preoccuparsi che gli hacker intercettino i loro dati.**

### *****5. Usa password complesse e univoche*****

### **Usa un gestore di password: ci sono milioni di nomi utente e password rubati venduti dai criminali informatici nel dark web. Le password deboli possono essere indovinate o violate in millisecondi, esponendo i dati sensibili dei tuoi studenti. Un gestore di password è un'app che genera password non decifrabili e le riempie automaticamente ogni volta che ne hai bisogno. Molti custodi di password memorizzeranno tutte le credenziali in un deposito crittografato, a cui solo tu puoi accedere.**

### **Come creare una password sicura**

### **Consiglia agli studenti di creare password lunghe, complesse e miste. Vale a dire, dovrebbero essere lunghi almeno 8 caratteri, avere un mix di lettere, numeri e caratteri speciali ed essere il più assurdi possibile. In un attacco di forza bruta, gli hacker provano combinazioni di milioni di parole e numeri del dizionario al secondo fino a quando non riescono a inserirle.**

### *****6. Prestare attenzione alle truffe di phishing*****

### **Scuole e università come obiettivi: i database degli studenti sono una miniera d'oro di informazioni personali sugli studenti. Una truffa di phishing si basa su un membro dello staff che viene indotto con l'inganno a rispondere o a fare clic su un collegamento in un'e-mail fasulla o in un messaggio di testo per diffondere malware, rubare credenziali o peggio. I criminali informatici hanno utilizzato le e-mail degli studenti per richiedere prestiti fraudolenti, rubare identità e infettare intere reti, bloccandole completamente.**

### **Prevenzione: di solito è possibile rilevare una truffa via e-mail di phishing leggendo l'indirizzo del mittente. Ad esempio, l'URL del sito Web della California Student Aid Commission www.csac.ca.gov potrebbe apparire come www.csac.ca.com e la maggior parte di noi non ne sarebbe più saggia. Per essere al sicuro, chiedi agli studenti di inviare un'e-mail separata all'autorità in questione e di non fare mai clic sui collegamenti nelle e-mail a tema COVID-19. La vigilanza è fondamentale.**

### ****7. Conoscere i termini e le condizioni****

### **Quando ti iscrivi a un sito Web, ti registri per un account di social media, scarichi un'app o addirittura usi un'app che già possiedi, tieni presente i termini e le condizioni che accetti scaricando e/o utilizzando quell'app. Un'app che usi per scansionare il tuo viso, ad esempio, potrebbe condividere quei dati combinati con nome, cronologia di navigazione, informazioni di contatto e altro per rappresentare un rischio significativo per la tua sicurezza in futuro.**

### ****8. Non condividere informazioni personali****

### **Questo è abbastanza ovvio, ma vale la pena ripeterlo: non condividere informazioni personali, o almeno sii consapevole di chi esattamente potrebbe leggere (o alla fine "scoprire") su cosa. Non ci vuole molto di una violazione delle informazioni - un indirizzo e-mail con una password debole o il tuo nome completo e indirizzo - per consentire a qualcuno disposto a usare un po' di ragionamento deduttivo e capacità di ricerca su Internet di creare una minaccia per la tua identità, sicurezza finanziaria, e altro ancora.**

### **Ciò significa anche che non è sicuro condividere account con amici, ad esempio un account Netflix.**

### **Altri consigli sulla sicurezza dei dati per studenti e scuole**

### **9. Aggiorna app e sistemi operativi del dispositivo**

### **10. Conserva backup (sicuri) di file o database importanti**

### **11. Non utilizzare fonti WiFi non protette**

### **12. Conosci il tuo contesto e le "reti" (fisiche e digitali)**

**Ad esempio, gli studenti: Conoscere i propri rischi e vulnerabilità specifici (in base all'utilizzo, all'età, agli obiettivi di carriera, ecc.) Scuole: formare il personale sulla politica scolastica e distrettuale. (Nordpass, 2022)**





DOMANDE DI VALUTAZIONE

1) Cosa significa per te “sicurezza digitale”?

2) Quali sono esempi di sicurezza digitale inappropriata?

3) Perché la sicurezza digitale è importante nell'istruzione?

4) Puoi dirmi 2 modi per essere al sicuro online?

5) Conosci abbastanza la sicurezza digitale?

**References**

<https://www.simplilearn.com/what-is-digital-security-article>

<https://mwhitmoredigitalcitizenship.weebly.com/digital-security.html>

<https://cybersecurityforme.com/importance-of-cybersecurity-in-education/#:~:text=Cybersecurity%20awareness%20training%20is%20important,schools%20to%20keep%20students%20safe>.

<https://www.teachthought.com/technology/cybersecurity-tips-for-students/>