Finanziato dall'Unione europea

DigiSkiPasS – Digital Skills Passport for Senior

2023-1-BE01-KA210-ADU-000153530

www.digiskipass.com

Finanziato
dall'Unione europea

CONOSCERE E APPLICARE LA SICUREZZA INFORMATICA

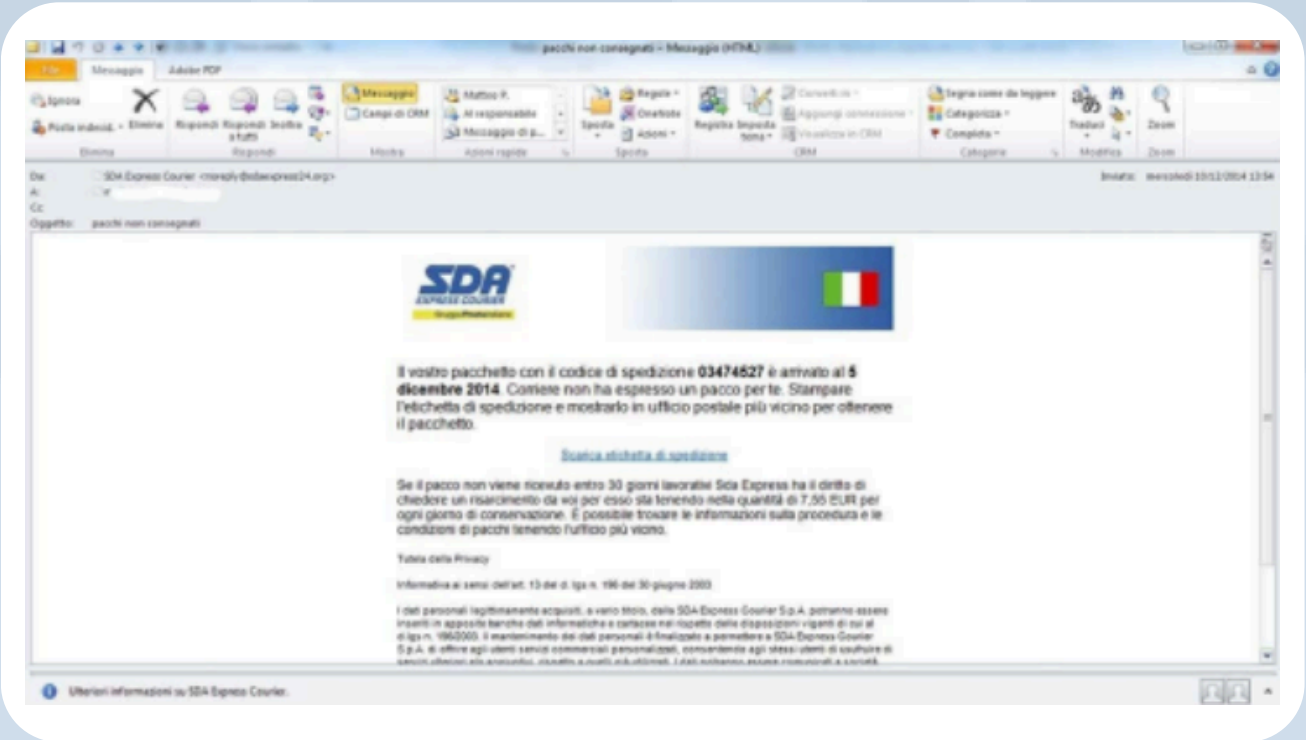
Fondazione Sviluppo Europa

Finanziato dall'Unione europea

SICUREZZA DEI DISPOSITIVI

IL MALWARE

Il **Malware** è la forma abbreviata per indicare un "software malizioso", e qualsiasi altro software in grado di compromettere il funzionamento dei computer oppure dei dispositivi mobili, acquisire informazioni delicate, rendere possibile l'accesso ai sistemi privati, oppure imporre di visualizzare pubblicità indesiderate.



Finanziato dall'Unione europea

Analizziamo ora in dettaglio i malware più comuni.

Il **TROJAN** - come il Cavallo di Troia della mitologica greca, questo tipo di malware si distingue dagli altri in quanto è un programma ideato per indurre gli utenti ad installarlo; può essere usato per rubare informazioni personali. Di solito, i computer vengono infettati dai trojan attraverso gli allegati di posta elettronica.

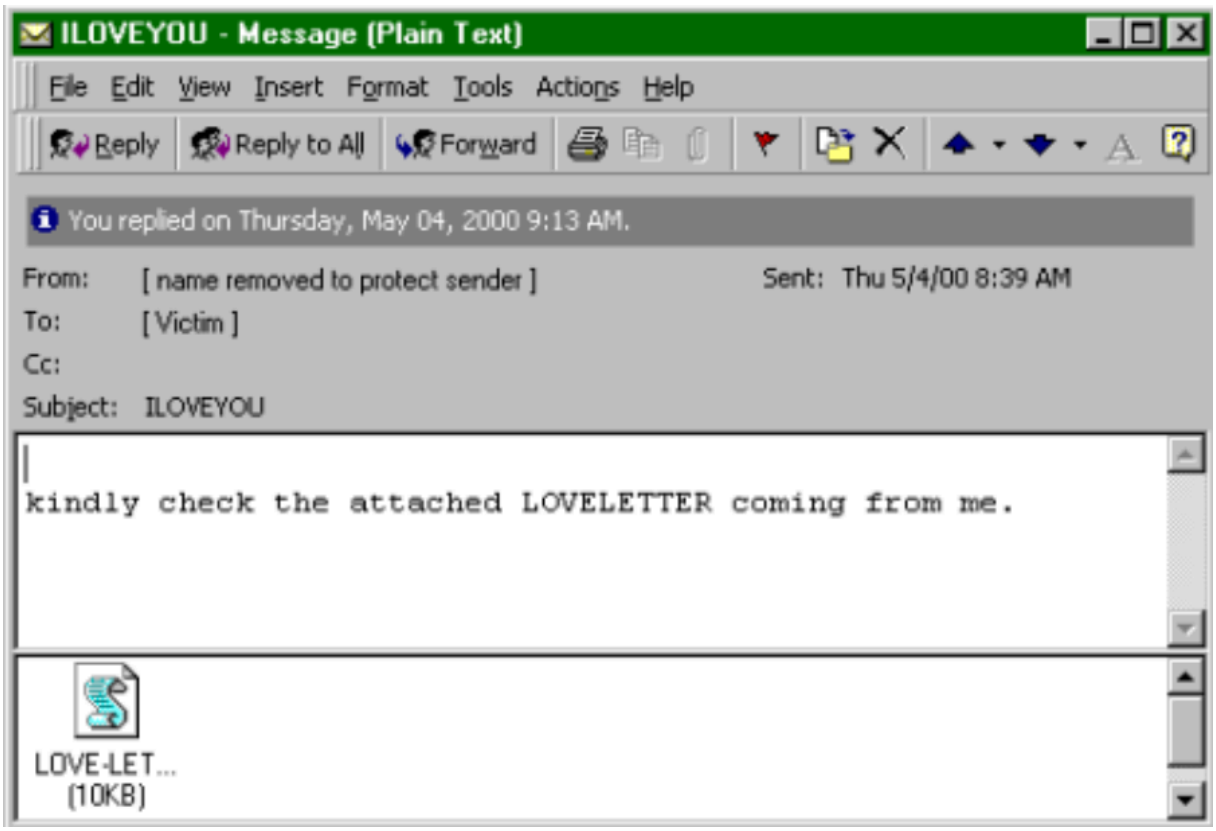
Finanziato dall'Unione europea

Analizziamo ora in dettaglio i malware più comuni.

I**VIRUS** - Si tratta di un pezzo di codice che infetta il software ospite e quindi diffonde il contagio attraverso i file del sistema. Se i file vengono condivisi attraverso un sistema il virus può essere trasmesso anche ad altri dispositivi.

Questi si possono diffondere attraverso gli allegati di posta elettronica, le chiavette USB, l'archivio nel cloud, ed altri. È buona norma **verificare** sempre i file che si ricevono. Per esempio, se ti viene inviato un video, sappi che nel caso in cui il nome includa ".exe", come ad esempio nel nome ".mov.exe" quasi certamente avrà a che fare con un virus.

Ad esempio, il virus **ILOVEYOU** è stato uno dei primi virus ad essersi diffuso per posta elettronica. Nel momento in cui gli utenti al di sopra di ogni sospetto cliccano sull'allegato, esso si diffonde infettando l'audio, l'immagine e tutti gli altri file del computer.



Il **WORM** (verme) è il tipo più comune di malware. Provoca un danno simile a quello provocato di virus. La differenza sta nel fatto che il worm informatico ha la capacità di auto-ripetersi, auto moltiplicarsi e diffondersi indipendentemente, mentre i virus si affidano all'attività umana per diffondersi (ad es., eseguire un programma, aprire un file).

I Worm si diffondono più comunemente inviando e-Mail con allegati infetti ai contatti degli utenti nella rubrica.

Lo **SPYWARE** è un tipo di malware che funziona spiando l'attività dell'utente a sua insaputa. Lo spyware può raccogliere le informazioni dell'utente (password, dati finanziari, ecc.) e monitorarne l'attività (attività su Internet, sequenze di tasti, ecc.).

Il **RANSOMWARE** è un malware informatico che si installa in modo nascosto sul dispositivo della vittima e ne tiene in ostaggio i dati fino al pagamento di un riscatto.

Finanziato dall'Unione europea

Lo **SCAREWARE** è una forma di software dannoso che utilizza l'ingegneria sociale per provocare shock, ansia o percezione di una minaccia al fine di manipolare gli utenti nell'acquisto di software indesiderato. Di solito suggerisce che gli utenti scarichino e paghino per falso software antivirus per rimuoverlo.

IL PROCESSO DI INFEZIONE DEL SISTEMA

Quali sono i modi più comuni per infettare il tuo dispositivo?

- si apre una email (infetta) da indirizzi sconosciuti,
- si naviga su siti non sicuri,
- non si aggiorna il proprio sistema operativo,
- non si esegue lo scanner antispyware,
- si scarica un software infetto,
- si scaricano software, musica o film pirata e in modo non autorizzato.

Finanziato dall'Unione europea

PREVENZIONE DELLE INFEZIONI

Anche se oggigiorno non esiste un uso sicuro del computer e di Internet, ci sono molte cose che possiamo fare per minimizzare il rischio.

1. Installa un programma antivirus autorizzato e aggiornalo regolarmente (ad esempio, **AVG, Avast, Kaspersky, McAfee**). Ci sono anche alcune opzioni gratuite disponibili.
2. Installa regolarmente gli aggiornamenti di sicurezza per il suo sistema operativo.
3. Usa un firewall.
4. Utilizza il blocco popup sul browser.
5. Imposta password complesse per i tuoi account.
6. Quando finisci di lavorare, esci sempre dal tuo account in rete su tutti i dispositivi.

Finanziato dall'Unione europea

PROGRAMMI ANTIVIRUS

Per combattere correttamente i virus, è sempre opportuno installare un programma **antivirus** nel sistema.

Il programma antivirus scelto dovrebbe avere due modalità:

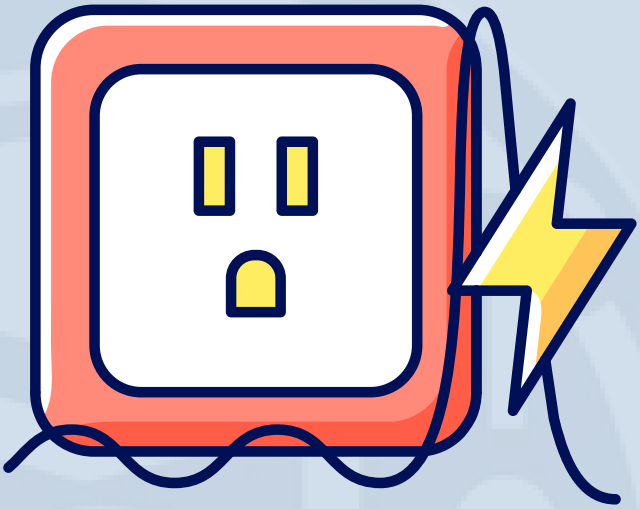
Interattivo: in questa modalità, il programma si nasconde in background e controlla l'attività del computer, sempre alla ricerca di un virus proveniente da una e-mail, www, USB, ecc.
Se viene rilevato un virus, un messaggio lampeggia sullo schermo.

Scansione: in questa modalità, il programma antivirus esegue la scansione e controlla tutte le parti della memoria del computer e del sistema di archiviazione, alla ricerca di segni di infezione.
Per ogni evenienza, si consiglia di impostare il software antivirus per la scansione automatica.

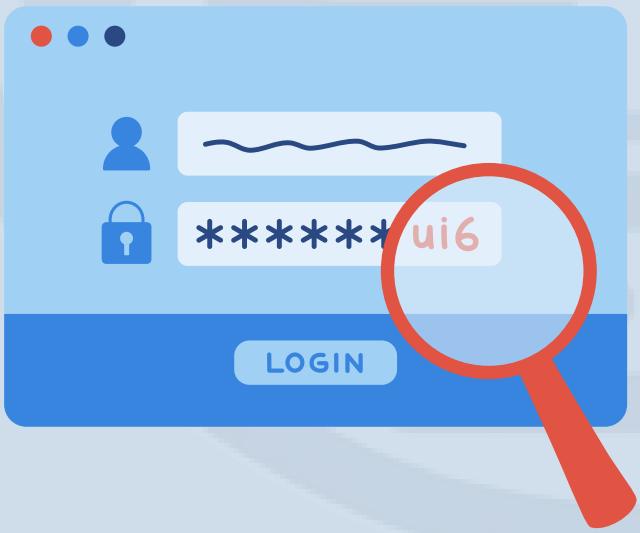
Finanziato dall'Unione europea

PROTEGGERE IL DISPOSITIVO DAL DANNO FISICO

È molto importante collegare il computer, lo schermo e il router a un **limitatore di sovratensione** e evitare che venga danneggiato durante i temporali. In questi casi, se non si dispone di un limitatore di sovratensione, è necessario almeno scollegare i dispositivi dall'impianto elettrico.



PASSWORD



La **password** o **codice di accesso** rappresenta la prima linea di difesa nella sicurezza informatica.

Ormai, tutti dovrebbero sapere che le password come "123456" e "password123" non sono abbastanza forti, cioè sicure. Tuttavia, ci sono ancora milioni di persone che non usano password sicure.

Ora, impariamo come creare una **password sicura**:

- Combinare lettere maiuscole e minuscole, numeri e simboli (ad esempio, @, #, $,%) se consentito.
- Usare almeno otto caratteri (più caratteri si utilizzano, più forte è la password).

- Usare le lettere iniziali di una frase che ti piace, specialmente se è incluso un numero o un carattere speciale.
- Prendere due cose familiari e poi combinarle con un numero o un carattere particolare.

- Si consiglia di cambiare la password ogni 3 mesi.
- Non usare la stessa password per tutti gli account in uso.
- Infine, la miglior password è una password che si RICORDA facilmente.

GESTIONE PASSWORD

Hai almeno cinque account online come **Google, Facebook, Twitter, LinkedIn e Instagram**, a cui si aggiungono l'home banking, un portale di pubblica amministrazione, ecc.

Ora che sai come creare una password sicura, è tempo di scoprire il software di gestione password. I gestori di password come **KeePass** memorizzano le tue informazioni di accesso per tutti i siti Web che utilizzi e ti aiutano ad accedere automaticamente ad essi criptando il tuo database delle password mediante l'uso di una password principale. La password principale rimane quindi **l'unica password** che è necessario ricordare.

Finanziato dall'Unione europea

SICUREZZA DEI DATI PERSONALI

IMPOSTARE LA PRIVACY DEI SERVIZI IN RETE

Per raggiungere un dato livello di sicurezza su Internet, è necessario che tu sia in grado di comprendere l'impostazione corretta per la tua riservatezza nei servizi in rete usati, e come gestirla al meglio.

RENDERE LA NAVIGAZIONE PIÙ SICURA

Ecco alcuni suggerimenti su come rendere la navigazione più sicura:

- Abilitare gli aggiornamenti automatici del tuo motore di ricerca (browser). o Bloccare i pop-up, plug-in e i siti phishing.
- Impostare il browser in modo da non memorizzare la password.
- Disattivare i cookies di terzi.
- In base al browser in uso, è necessario regolarne le impostazioni per ottenere la massima sicurezza.

Finanziato dall'Unione europea

IMPOSTARE LA PRIVACY DEI SOCIAL NETWORK

I social network permettono alle persone di connettersi, ma sono anche una piattaforma molto diffusa per lanciare minacce online e cyberbullismo. Senza volerlo, le persone, specialmente i bambini, spesso condividono più informazioni online di quanto dovrebbero.

Questo li rende particolarmente vulnerabili.

Le impostazioni sulla privacy sono controlli disponibili su vari social network (ad esempio, Facebook) e altri siti Web che consentono agli utenti di limitare l'accesso al proprio profilo e quali informazioni possono essere visualizzate dai visitatori.

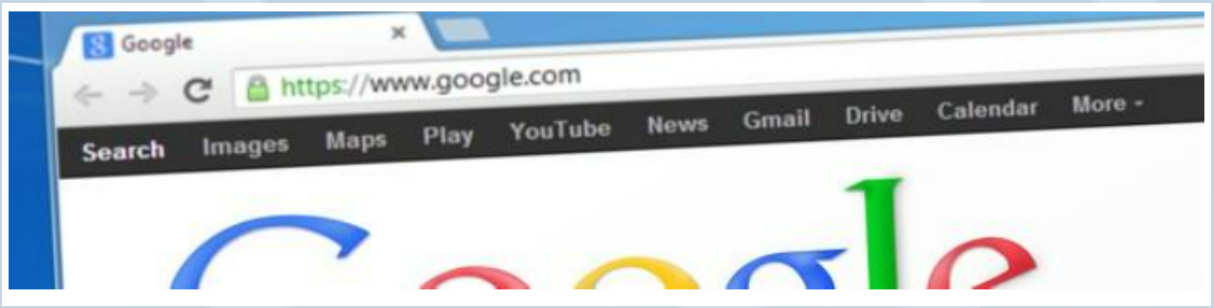
Mentre è possibile utilizzare soluzioni di filtro dei contenuti per impedire agli allievi di accedere ai social media mentre usano i computer della scuola, oggigiorno la maggior parte degli studenti porta gli smartphone a scuola e una volta che si connettono a Internet su quei dispositivi, sono fuori da ogni possibilità di controllo da parte della scuola. Ecco perché è fondamentale promuovere nei curriculum scolastici la cittadinanza digitale responsabile.

Finanziato dall'Unione europea

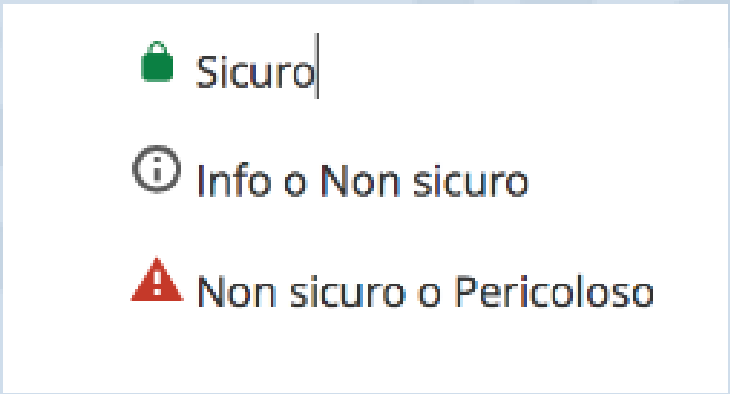
IL PROTOCOLLO HTTPS E I SITI WEB SICURI

Un sito Web sicuro non contiene programmi malware, crittografa tutti i dati che lo attraversano al fine di garantire uno scambio sicuro dei dati personali o delle transazioni finanziarie da eventuali compromissioni.

Come puoi sapere se un sito web è sicuro?
Se il sito Web utilizza HTTPS (un protocollo di comunicazione per comunicazioni sicure su una rete di computer), la parola HTTPS comparirà prima dell'indirizzo del sito web.

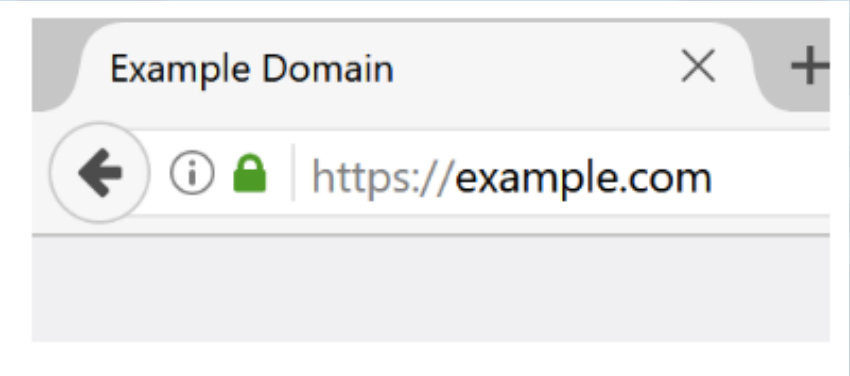


Conosci il tuo browser e le sue funzionalità. Oltre a https, può apparire un'icona. Ad esempio, se utilizzi **Google Chrome** per verificare la sicurezza di un sito, guarda lo stato della sicurezza sul lato sinistro dell'indirizzo web.

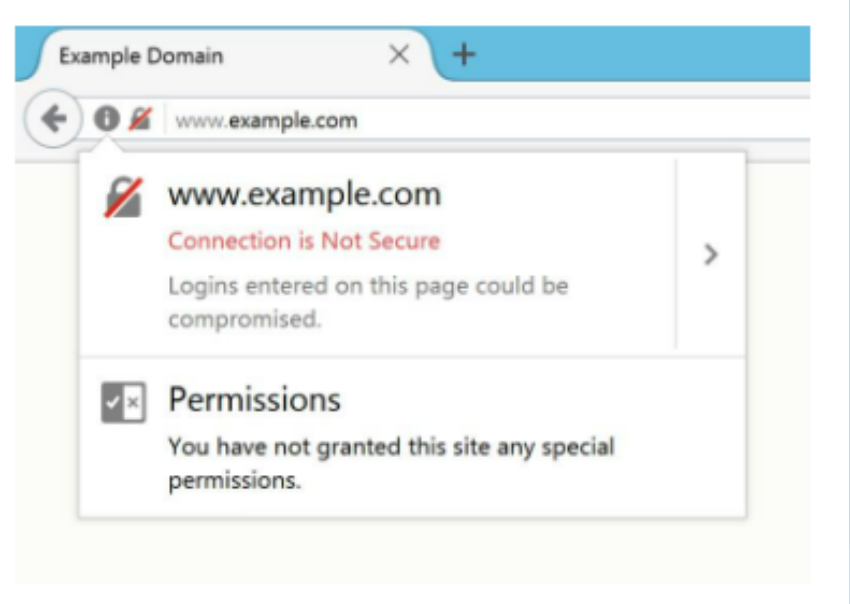


Se si utilizzi Firefox, lo stato di sicurezza si trova anche sul lato sinistro dell'indirizzo Web: ·

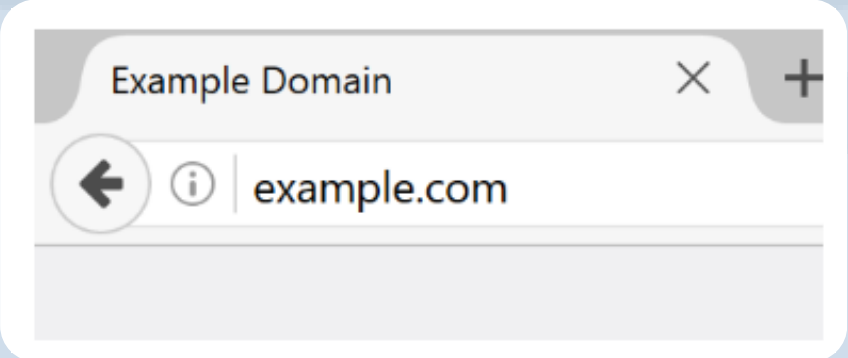
- **Sicuro**

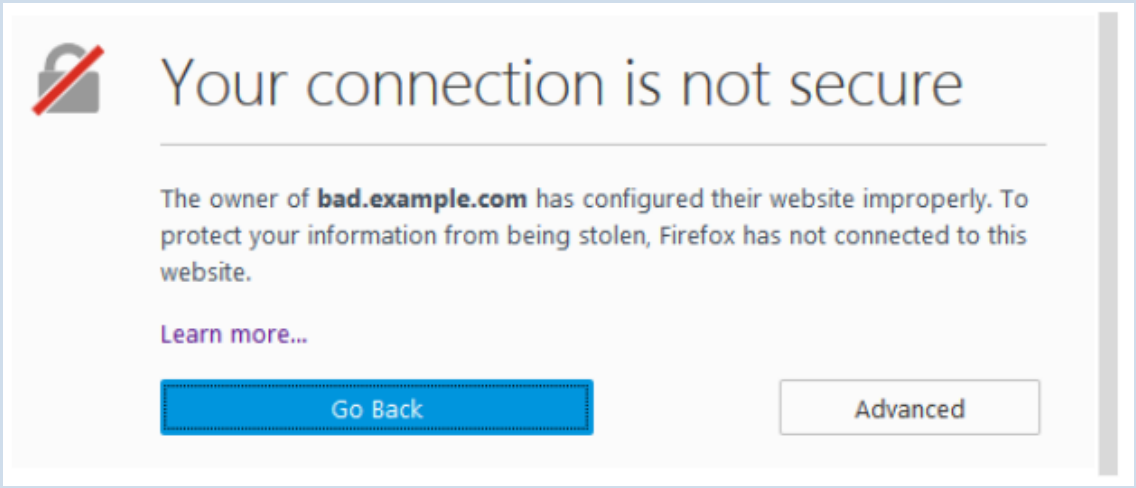


- **Avvertimento**



- **Non sicuro o pericoloso**





È necessario prestare particolare attenzione quando si trasferiscono informazioni delicate ed altamente personali sulla rete. Alcuni siti Web potrebbero non essere aggiornati ai più recenti **standard SSL**, che possono essere pericolosi per il trasferimento di dati, ma abbastanza sicuri da navigare e cercare informazioni.

I COOKIE

I cookie di Internet sono piccoli file che vengono memorizzati sul suo computer. Lo scopo principale di un cookie è identificare gli utenti e possibilmente preparare pagine Web personalizzate o archiviare le informazioni di accesso al sito. I cookie di solito non contengono informazioni delicate o altamente personali o nulla di pericoloso. Nella maggior parte dei casi, ciò significa che il sito Web ricorda il tuo nome utente. Se elimini i cookie dopo aver visitato un determinato sito web, non sarai trattato come un visitatore di ritorno. (Ad esempio, dovrai inserire nuovamente il suo nome utente).

Finanziato dall'Unione europea

NAVIGARE SU UN COMPUTER AD USO PUBBLICO

Quando usi i **computer pubblici**, come ad esempio nelle biblioteche, negli Internet cafè, negli aeroporti, negli alberghi, ecc., devi fare molta **attenzione**:

- Non chiedere a un computer pubblico di ricordare la tua password.
- Controllare se il firewall di Windows è acceso e se è stato installato un programma antivirus. · Non scaricare documenti riservati su un computer pubblico.
- Eliminare qualsiasi contenuto scaricato dalle e-mail.
- Uscire dopo aver utilizzato qualsiasi sito Web che richiede l'accesso (ad esempio Gmail, Facebook, LinkedIn, ecc.)

- Durante l'inserimento della password e dei dettagli finanziari in una pagina web, assicurarsi sempre di fare quanto segue:
    - Controllare se la barra degli indirizzi ha "https" e un blocco nell'URL.
    - Utilizzare la modalità di navigazione privata. La navigazione privata ti consentirà di navigare in Internet senza salvare alcuna informazione su quali siti e pagine hai visitato, ma non ti renderà anonimo su Internet. Ciò significa che il tuo fornitore di servizi Internet (a casa), il datore di lavoro (al lavoro) o i siti stessi possono ancora conservare traccia delle pagine che hai visitato.

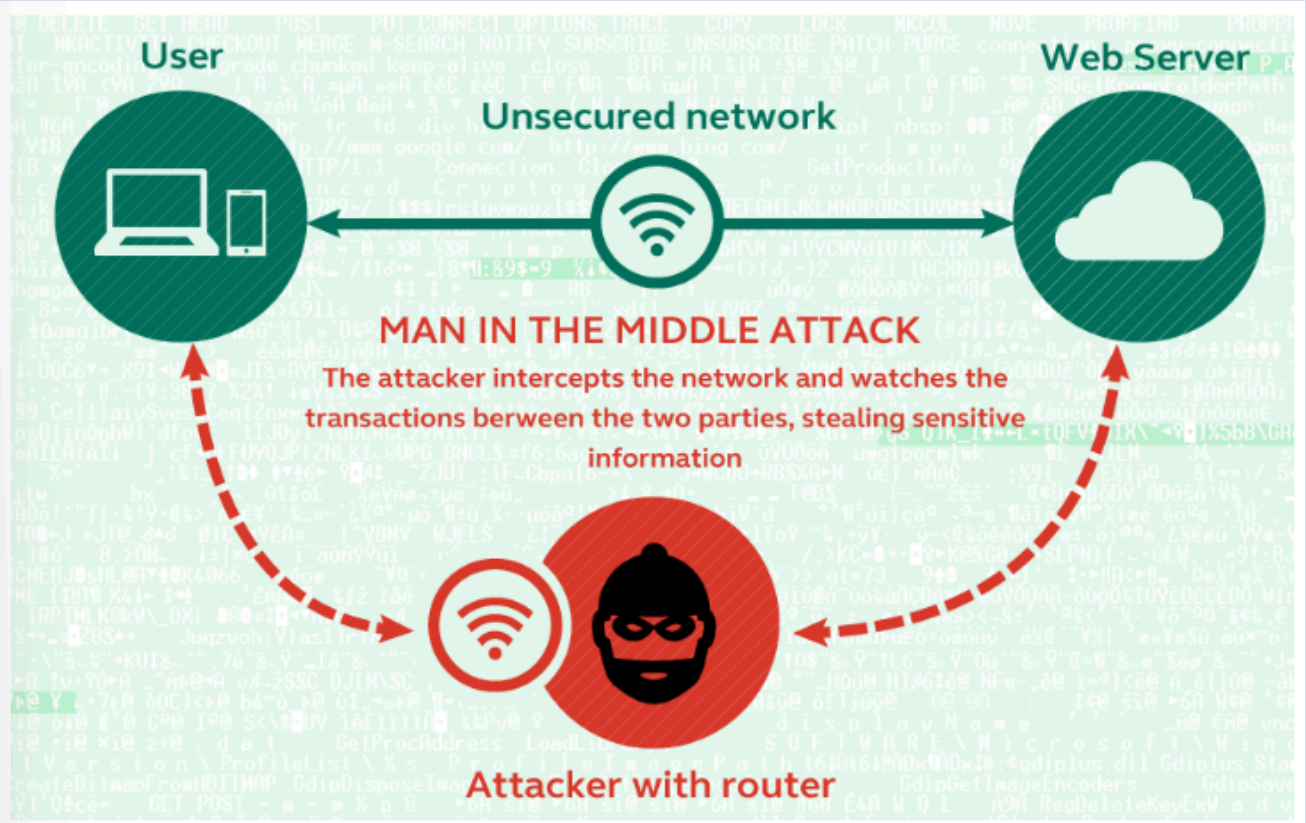
NAVIGARE SU UNA RETE PUBBLICA

Tutti, abbiamo visto segni come questo in un bar, un ristorante, edifici pubblici, ecc.

Finanziato dall'Unione europea

Ti sei mai collegato a una rete come questa mentre stavi usando il tuo portatile, tablet o smartphone? Sei riuscito a connetterti senza password? Non sei riuscito a controllare se l'indirizzo iniziava con **https://**? Se hai risposto a queste domande con Sì, hai potenzialmente messo a rischio le tue informazioni personali.
Tutti quei segnali nei luoghi dovrebbero essere in realtà sostituiti con questo:

Quando ci si connette a una rete pubblica, è quasi come invitare un estraneo a casa tua – ti fidi di lui in base alle informazioni di cui disponi. Chiunque accede alla stessa rete (non protetta), può intercettare qualsiasi passaggio di informazioni tra il tuo dispositivo e i server web.



Come rimanere sicuri?

Sebbene non ci siano garanzie, puoi seguire alcuni passaggi per minimizzare il rischio:

- Non connettersi a reti che non richiedono password. Una rete Wi-Fi ufficiale dovrebbe stabilire una password. Ad esempio, se ti trovi in un bar, chiedi allo staff di verificare qual è la loro rete. Potrebbe esserci una finta rete appositamente impostata sotto lo stesso nome del bar.

- Non connettersi a siti Web che non utilizzano il protocollo HTTPS.

Finanziato dall'Unione europea

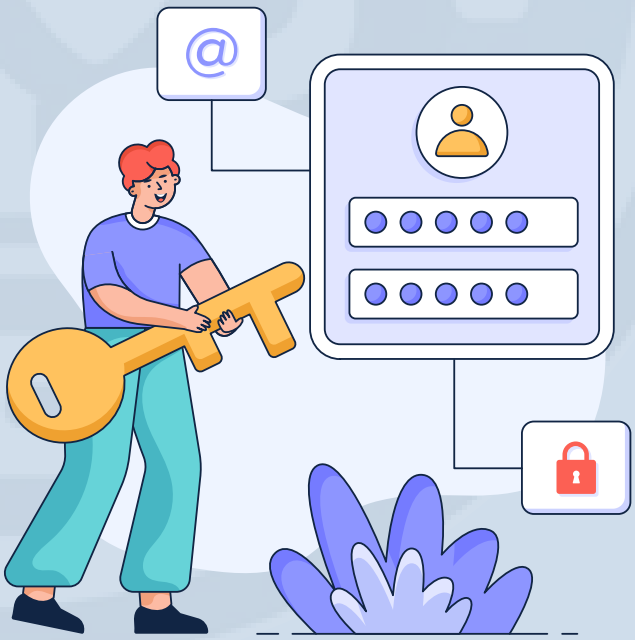
- Non connettersi alle reti pubbliche per utilizzare la carta di credito, controllare il proprio conto bancario, pagare le bollette, ecc.
- Quando hai finito di navigare usando il loro Wi-Fi, assicurarsi di disconnettersi e rimuovere la rete in modo che non ti connetta automaticamente la prossima volta che ti trovi nuovamente nel locale.
- Accendere il Wi-Fi solamente quando ne hai veramente bisogno. Ciò impedirà al tuo dispositivo di connettersi automaticamente a reti casuali.

Finanziato dall'Unione europea

UTILIZZO SICURO DELL'ARCHIVIAZIONE DEL CLOUD

Memorizzare i tuoi file (ad es. immagini, video, musica, documenti, ecc.) nell'archivio del cloud (ad es. **Google Drive, Dropbox, iCloud, Box, ecc**.) presenta molti vantaggi, ad esempio, c'è un rischio minore di perdere i dati. I file archiviati nel cloud possono essere facilmente visualizzati dal tuo computer e da un dispositivo mobile connesso a Internet. Sebbene le società di archiviazione adottino normalmente le misure di sicurezza necessarie, non ci sono garanzie. Tuttavia, è molto probabile che gli **hacker** acquisiscano i tuoi dati a causa di errore umano o negligenza, semplicemente violando la tua password. Quindi dovresti sempre assicurarti di:

- usare una password sicura e forte,
- cambiare regolarmente la password,
- non archiviare informazioni personali nel cloud
- se possibile, creare una copia di backup su un altro dispositivo (ad es. un disco rigido esterno).



Finanziato dall'Unione europea

DIGITAL FOOTPRINT: MONITORARE L'IDENTITÀ IN RETE

Un'**identità digitale** (digital footprint) è la rappresentazione online di un individuo all'interno di un mondo virtuale come una chat room, forum, videogioco o spazio comune virtuale. Tutte le attività in rete (navigazione, blog, pubblicazione su social media e forum, firma di petizioni online, ecc.) lasciano una traccia, la cosiddetta impronta digitale.

LINEE GUIDA PER PROTEGGERE LA PROPRIA IDENTITÀ IN RETE

- Utilizzare strumenti in rete per costruire un'impronta positiva.
- Non pubblicare mai nulla di cui ci si potrebbe pentire in futuro.
- Essere rispettoso di sé stesso e degli altri.
- Scegliere nomi utente e avatar appropriati.
- Immaginare cosa potrebbero pensare famigliari ed amici se vedessero quello che stai facendo in rete.
- Bloccare quegli utenti che riflettono poco sulla propria reputazione.
- Rintracciare informazioni sul proprio conto.
- Assicurarsi che gli amici usino la propria immagine solamente con il proprio permesso, e viceversa.
- Pensare prima di cliccare.

- Monitorare la propria identità digitale e le proprie impronte per proteggersi da frodi in rete e furti di identità. Pensare a come vorrebbe essere visto.

GESTIRE IDENTITÀ MULTIPLE IN RETE

Ecco alcuni vantaggi **dell'utilizzo di più identità digitali:**

- Un'identità digitale ti consente di creare profili anonimi e di fare blog o chattare in modo anonimo.
- Puoi rimanere privato e tuttavia esplorare varie opportunità.
- Puoi costruire un'identità digitale positiva per opportunità professionali (ad es. LinkedIn).
- È possibile creare un'identità digitale a scopo didattico.

Finanziato dall'Unione europea

PROTEGGERSI DA FRODI IN RETE E FURTO DI IDENTITÀ

Ecco alcune semplici regole che dovresti seguire, molte delle quali sono già state apprese in precedenti argomenti:

- Proteggere il proprio computer e dispositivo mobile con un software anti-malware forte e aggiornato.
- Usare password sicure.
- Avere password diverse per ogni account.
- Rintracciare informazioni su sé stesso - guardare quali informazioni private possono essere visualizzate dagli altri.
- Monitorare le comunicazioni bancarie e della carta di credito.
- Usare HTTPS ogni volta che è possibile.
- Riconoscere e-mail sospette e allegati.
- Pensare attentamente ogni volta che si inseriscono le proprie informazioni personali in rete.

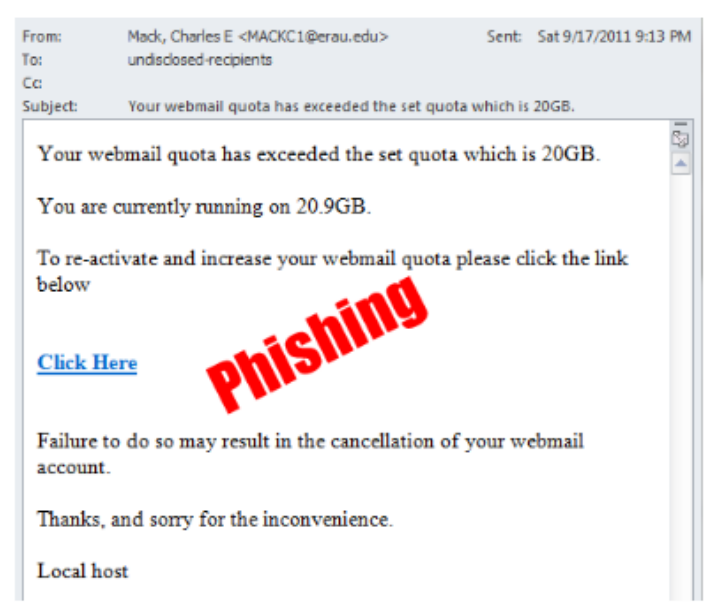
Finanziato dall'Unione europea

PHISHING

Si definisce **phishing** il tentativo di ottenere informazioni sensibili come nomi utente, password e dettagli della carta di credito, spesso per motivi dannosi, facendosi passare come entità affidabile nella comunicazione elettronica.

Il phishing viene in genere effettuato tramite lo spoofing o la messaggistica istantanea dei messaggi di posta elettronica e spesso indirizza gli utenti a immettere informazioni personali su un sito Web falso, il cui aspetto e formato sono quasi identici a quelli legittimi. Le comunicazioni che pretendono di provenire da siti Web di reti sociali, siti di aste, banche, processori di pagamento in rete o amministratori IT sono spesso utilizzate per attirare le vittime. Le e-mail di phishing possono contenere collegamenti a siti Web infetti da malware.

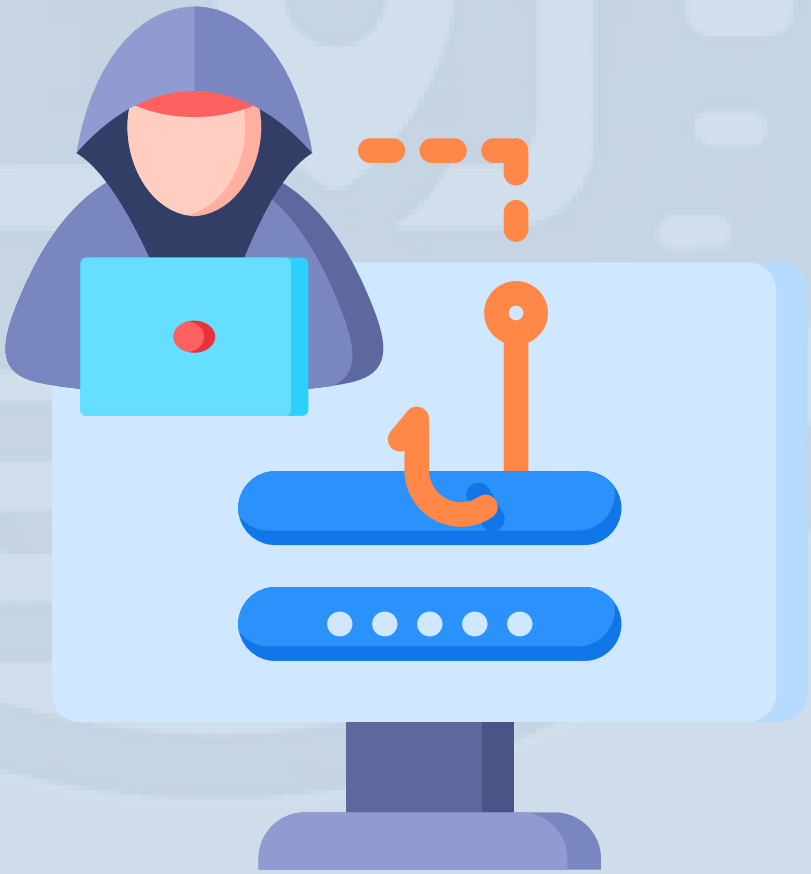
Ecco un esempio di tentativo di phishing che tenta di ottenere le informazioni email degli utenti.



Finanziato dall'Unione europea

COME IDENTIFICARE LE TRUFFE DI PHISHING

- Non fidarti del nome visualizzato sullo schermo.
- Guardare ma non cliccare.
- Controllare gli errori di ortografia.
- Analizza la forma di saluto.
- Il messaggio richiede informazioni personali.
- Fare attenzione al linguaggio urgente o minaccioso nell'oggetto del messaggio.
- Rivedere la firma.
- Non cliccare sugli allegati.
- Non credere che l'indirizzo di invio sia quello elencato nell'intestazione.
- L'offerta sembra troppo buona per essere vera.
- Il messaggio sembra provenire da un'agenzia governativa.



Finanziato dall'Unione europea

IL CYBER BULLISMO

Internet ha aperto nuove possibilità per tutti noi. L'altra faccia della medaglia è però rappresentata dai rischi legati ad un uso improprio di questo strumento: tra questi c'è il **cyberbullismo**.

Si può definire cyberbullismo l'uso delle nuove tecnologie per **intimorire, molestare, mettere in imbarazzo, far sentire a disagio o escludere altre persone.**

Per i giovani che stanno crescendo a contatto con le nuove tecnologie, la distinzione tra vita online e vita offline è davvero minima. Le attività che i ragazzi svolgono online o attraverso i media tecnologici hanno quindi spesso **conseguenze anche nella loro vita reale**. Allo stesso modo, le vite online influenzano anche il modo di comportarsi dei ragazzi offline, e questo elemento ha diverse ricadute che devono essere prese in considerazione per comprendere a fondo il cyberbullismo.

Finanziato dall'Unione europea

Tutto questo può avvenire utilizzando diverse modalità offerte dai nuovi media. Alcuni di essi sono:

- Telefonate
- Messaggi (con o senza immagini)
- **Chat** sincrone
- **Social network** (Facebook, TikTok)
- Siti di domande e risposte
- Siti di giochi online
- Forum online

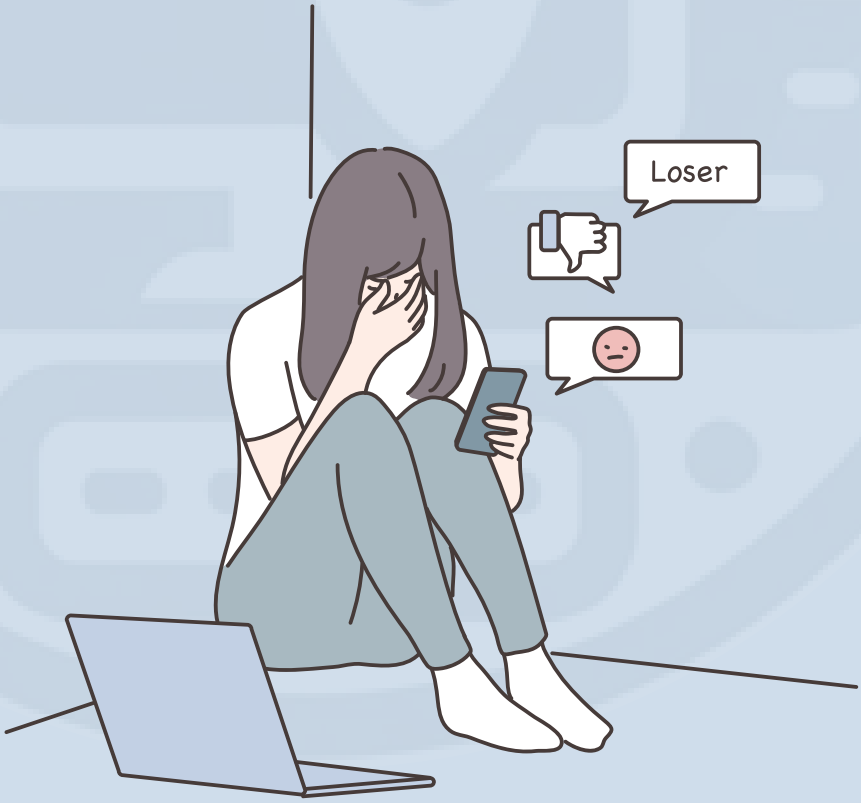
Le modalità specifiche con cui i ragazzi realizzano atti di cyberbullismo sono molte. Alcuni esempi sono:

- **pettegolezzi** diffusi attraverso messaggi sui cellulari, mail, social network;
- postando o inoltrando informazioni, **immagini o video imbarazzanti** (incluse quelle false);
- **rubando l'identità e il profilo di altri, o costruendone di falsi,** al fine di mettere in imbarazzo o danneggiare la reputazione della vittima;

- **insultando o deridendo** la vittima attraverso messaggi sul cellulare, mail, social network, blog o altri media;
- facendo **minacce fisiche** alla vittima attraverso un qualsiasi media.

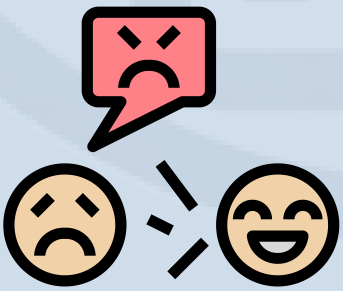
Queste aggressioni possono far seguito a episodi di bullismo (scolastico o più in generale nei luoghi di aggregazione dei ragazzi) o essere comportamenti solo online.

Il cyber bullismo potrebbe sembrare innocuo, ma se non viene affrontato in modo appropriato, può avere gravi conseguenze emotive per bambini e adolescenti.



Ecco alcuni passaggi da seguire per evitare il cyber bullismo:

- Insegnare ai bambini a non pubblicare informazioni personali o qualcosa di molto privato.
- Spiegare loro a non rispondere con rabbia e rancore a un messaggio che a sua volta esprime pure rabbia.
- Spiegare ai bambini perché non dovrebbero aprire messaggi inviati da estranei.
- Ricordare loro di cambiare regolarmente e utilizzare codici di accesso (password) diversi.
- Poiché queste impostazioni tendono a cambiare, è sempre consigliabile, ogni tanto ma regolarmente, aggiornare le impostazioni della privacy per i servizi in rete.



Finanziato dall'Unione europea

SALUTE E GREEN IT

CONOSCERE I POTENZIALI RISCHI PER LA SALUTE DURANTE IL LAVORO AL COMPUTER

Se usati correttamente e con moderazione, i computer non dovrebbero avere alcun impatto sulla salute della maggior parte delle persone. Tuttavia, l'uso intensivo del computer può causare problemi di salute occasionali e a lungo termine. I problemi e lamentele più comuni sono:

- disturbi agli arti superiori (possono interessare le dita, le mani, le braccia o le spalle),
- dolore alla schiena e al collo,
- problemi agli occhi,
- stress da mal di testa o affaticamento.

Finanziato dall'Unione europea

Digitando per ore ogni giorno è più probabile che causi **lesioni da sforzo ripetitivo (RSI)**. Questi tipi di problemi possono essere causati da:

- postura innaturale o malsana durante l'utilizzo del computer (in particolare computer portatili a causa di schermi piccoli, tastiere e dispositivi di puntamento incorporati (ad esempio un piccolo mouse o touchpad portatile),
- supporto della parte bassa della schiena inadeguato,
- seduta nella stessa posizione per un lungo periodo di tempo
- postazione di lavoro ergonomicamente scadente.

Finanziato dall'Unione europea

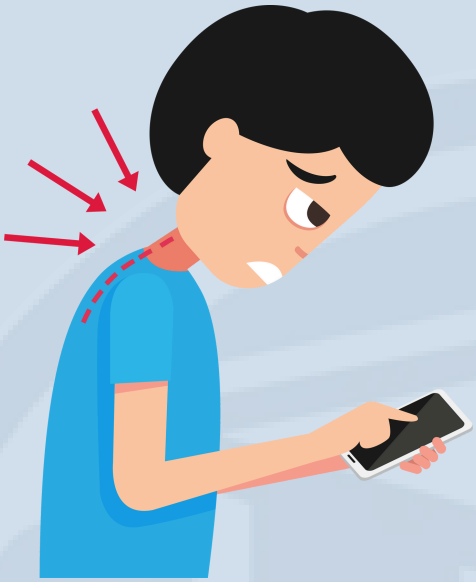
Dato che i computer sono uno strumento essenziale nella nostra **vita quotidiana** e che possono causare problemi di salute, è necessario imparare come ridurre i **rischi** per la salute derivanti dall'uso prolungato del computer.

USARE IL COMPUTER IN MODO SANO

È necessario applicare varie misure per ridurre i rischi per la salute derivanti dall'uso prolungato del computer. Ecco alcuni esempi:

- L'immagine dello **schermo** deve essere chiara, fissa e priva di bagliori e / o riflessi.
- La **tastiera** deve essere posizionata correttamente per sostenere i polsi.
- Per prevenire le conseguenze dell'uso prolungato del **mouse**, si consiglia di avere delle pause nel corso dell'attività del mouse.
- La **sedia** da lavoro dovrebbe garantire una posizione di lavoro confortevole e dovrebbe essere completamente regolabile. Dovrebbe essere regolato in modo che gli avambracci degli utenti siano posizionati orizzontalmente e che la parte superiore dello schermo sia all'altezza degli occhi. Si può usare anche un poggiapiedi.
- Accanto a queste disposizioni fisiche, i cambiamenti regolari nelle posizioni di lavoro, nonché i periodi regolari di **riposo** dal fissare lo schermo sono essenziali per evitare problemi di salute computer indotti.

Finanziato dall'Unione europea



Indicazioni chiare su come usare in modo sano i computer sono riportate nelle direttive dell'Agenzia Europea per la Sicurezza e la Salute al Lavoro Directive 90/270/EEC

COME RILASSARE I MUSCOLI DURANTE IL LAVORO AL COMPUTER

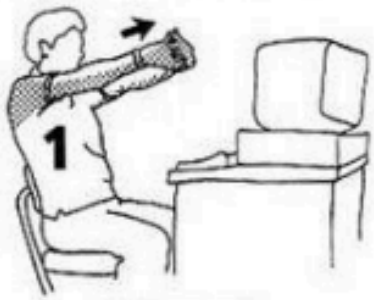
Hai già appreso che l'uso del computer può causare problemi di salute e modi per ridurre i problemi di salute con l'uso di attrezzature adeguate, **design ergonomico** del posto di lavoro e seguendo specifiche pratiche di lavoro (cambiamenti regolari nelle posizioni di lavoro e regolari periodi di riposo dallo schermo).

Al fine di migliorare la tua postura e mantenere la tua salute sotto controllo, ora esplorerai come rilassare i tuoi muscoli quando lavori tutto il giorno sul computer. L'organizzazione **americana National Institutes of Health (NIH)** fornisce un elenco completo di vari esercizi e tratti quali esercizi per gli occhi e muscolo- scheletrici, riscaldamento per il lavoro, esercizi per la schiena, esercizi aerobici e raccomandazioni per il riposo dei muscoli della schiena.

Computer & Desk Stretches

Approximately 4 Minutes

Sitting at a computer for long periods often causes neck and shoulder stiffness and occasionally lower back pain. Do these stretches every hour or so throughout the day, or whenever you feel stiff. Photocopy this and keep it in a drawer. Also, be sure to get up and walk around the office whenever you think of it. You'll feel better!



10–20 seconds
2 times

10–15 seconds

8–10 seconds
each side

15–20 seconds

3–5 seconds
3 times

10–12 seconds
each arm

10 seconds

10 seconds

8–10 seconds
each side

8–10 seconds
each side

10–15 seconds
2 times

Shake out hands
8–10 seconds

Finanziato dall'Unione europea

TROVARE EQUILIBRIO FRA VITA ONLINE E OFFLINE

Siamo circondati dalla tecnologia. Internet ha cambiato le modalità di interazione fra le persone. Oggigiorno, per **comunicare**, preferiamo usare la posta elettronica, messaggistica istantanea (IM) e siti di reti sociali. Sebbene le collaborazioni di lavoro non siano mai state più semplici, sembra che la maggior parte delle persone abbia sostituito la propria vita sociale offline con quella online. Le interazioni in rete difficilmente possono sostituire le interazioni **faccia a faccia** e più tempo passiamo a socializzare in rete, meno tempo abbiamo per socializzare offline, cioè fuori dalla rete, nel mondo reale. Anche se è più conveniente rimanere in contatto online, si impegni a raggiungere un **equilibrio** tra i mondi online e offline e non lasciare che le interazioni online sostituiscano il tempo trascorso offline con amici o familiari.

Finanziato dall'Unione europea

PROTEGGERE L'AMBIENTE

DISPOSITIVI ICT - IL NUOVO PER IL VECCHIO

La tecnologia utilizzata nei **dispositivi ICT** come telefoni cellulari, smartphone, tablet PC, portatili, televisori, schermi di computer, stazioni di gioco e dispositivi di archiviazione cambia molto spesso. I dispositivi elettronici fortemente usati dagli utenti un anno fa, ora sono diventati vecchi ed obsoleti. Anche se i "**vecchi**" dispositivi funzionano ancora bene, la gente li butta via e li sostituisce con quelli nuovi.

La nostra ossessione di avere solamente i dispositivi elettronici più attuali e di buttare via versioni obsolete nonostante funzionino ancora è un esempio della nostra società "**usa e getta**".

Finanziato dall'Unione europea

I RIFIUTI ELETTRONICI

I **rifiuti elettronici** stanno diventando un enorme problema in tutto il mondo perché ancora oggi molti dispositivi elettronici finiscono in **discariche non adeguate**. Quando i rifiuti elettronici non vengono smaltiti correttamente, i **metalli tossic**i, quali **piombo** (presente negli schermi CRT, nelle batterie), **cadmio** (batterie ricaricabili NiCd, strati fluorescenti degli schermi CRT, inchiostri e toner per stampanti), **mercurio** (lampade fluorescenti che forniscono retroilluminazione negli LCD, in alcune batterie alcaline e interruttori a contatto con mercurio), **arsenico** (all'interno dei diodi ad emissione luminosa) e **berillio** (scatole di alimentazione che contengono raddrizzatori e obiettivi a raggi X controllati al silicio) vengono assorbiti dal terreno e possono andare a **contamina l'acqua potabile**.

Finanziato dall'Unione europea

È questo il motivo per cui la maggior parte dei paesi ha introdotto regolamenti molto severi per impedire che i rifiuti elettronici vengano scaricati in **discariche inadeguate. .**

GREEN IT ED EFFICIENZA ENERGETICA

I rifiuti elettronici sono pieni di materiali preziosi come oro, nichel, acciaio, piombo, rame e plastica. Ognuno di questi materiali può essere **riutilizzato**. Ad esempio, lo **zinco** contenuto nei telefoni cellulari, potrebbe essere utilizzato nella costruzione navale o per la zincatura di inferriate metalliche e lampioni. L'**oro** contenuto nelle console dei videogiochi, può essere trasformato in gioielleria. La **plastica** può essere riutilizzata per produrre strumenti musicali.

Ci sono tre fattori chiave quando si pensa al riciclaggio, precisamente le 3 R:

- **ridurre** la quantità di rifiuti che si producono,
- **riutilizzare** gli oggetti di uso quotidiano,
- **riciclare**.

Abbiamo bisogno di una grande quantità di elettricità per alimentare milioni di dispositivi ICT in tutto il mondo. A causa del modo in cui viene generata l'elettricità, l'uso di dispositivi elettronici contribuisce alle **emissioni globali di gas serra (GHG)**, tuttavia, i dispositivi ICT possono essere utilizzati anche per ridurre il consumo energetico.

Ad esempio, molti edifici moderni dispongono di sistemi digitalizzati per il controllo ambientale. Infatti, spesso è un computer che controlla il sistema di climatizzazione, gli apri-cancelli automatici e i filtri solari per controllare l'effetto della luce solare e raffreddare l'edificio, i pannelli solari per ridurre il consumo di elettricità, i display di monitoraggio d'energia, i controlli di illuminazione LED a basso consumo e i sistemi di riutilizzo dell'acqua, soprattutto nelle fabbriche.