EUROPEAN INFORMATICS PASSPORT

SICUREZZA INFORMATICA

a cura del dott. Francesco Leonetti

ACCREDITATO DAL MIUR PER LA FORMAZIONE DEL
PERSONALE DELLA SCUOLA - DIRETTIVA 170/2016

Disclaimer

CERTIPASS ha predisposto questo documento per l'approfondimento dei temi relativi alla Cultura Digitale, finalizzati ad un idoneo e miglior utilizzo dei dispositivi digitali, in base agli standard e ai riferimenti Comunitari vigenti in materia.

CERTIPASS non si assume alcuna responsabilità in merito a qualsiasi tipologia di problematica che possa insorgere per effetto dell'utilizzazione e diffusione, anche da parte di terzi, della presente pubblicazione, nonché per danni di qualsiasi natura causati direttamente o indirettamente dai contenuti.

CERTIPASS, altresì, declina qualsiasi forma di responsabilità circa la completezza e correttezza dei contenuti, data la complessità e la vastità degli argomenti.

CERTIPASS si riserva, in qualsiasi momento e senza previo avviso, la facoltà di apportare modifiche e/o correzioni che, discrezionalmente, riterrà opportune.

L'Utenza destinataria ha il diritto e il dovere di informarsi in merito a quanto predetto, visitando periodicamente le apposite aree del portale eipass.com, dedicate al Programma.

Indice

INTRODUZIONE

"Non accettare caramelle dagli sconosciuti", ci raccomandavano le nostre nonne e mamme e, anche quando la tentazione era forte, ci guardavamo bene dal trasgredire questa semplice regola di sicurezza.

"Lavati bene le mani prima di mangiare", sappiamo ormai molto bene quanto l'igiene sia la prima forma di prevenzione.

Quando partiamo per una vacanza, chiudiamo a chiave la porta e ci assicuriamo che le finestre siano ben chiuse.

Quando usciamo dall'auto attiviamo il telecomando per chiuderla a chiave e magari ce ne assicuriamo provando ad aprirla con la maniglia, e così via.

Insomma, quando ci muoviamo nel mondo fisico sappiamo farlo con competenza e sicurezza. Senza esagerare nella paranoia, con equilibrio e semplice buon senso.

In rete, invece, nel mondo digitale, siamo mediamente degli sprovveduti, incoscienti ed irresponsabili, mettendo continuamente a rischio con il nostro comportamento l'integrità dei nostri dati, della nostra identità e, in alcuni casi, persino dei nostri averi.

Quando usiamo un dispositivo digitale, insomma, non ci laviamo mai le mani, accettiamo continuamente caramelle da chiunque, non chiudiamo niente a chiave e neanche ce ne preoccupiamo.

Male.

Usciamo però ora dall'analogia e proviamo a capire in che senso dobbiamo "lavarci le mani" prima di usare un computer, da chi e come dobbiamo guardarci e come serrare a chiave l'accesso ai nostri sistemi.

Parliamo di sicurezza informatica e identità digitale.

1. IDENTITÀ DIGITALE

L'articolo 1, comma 28, della Legge n. 107 del 2015, detta "La Buona Scuola", introduce espressamente l'obiettivo di dotare ogni studente di una **identità digitale**, associata al proprio profilo personale, con la quale accedere a servizi online dedicati oltre a documentare e archiviare in un portfolio personale tutte le esperienze e attività svolte nella carriera scolastica.

L'obiettivo al momento è stato tradotto prevedendo di fornire ad ogni studente la cosiddetta **"Carta dello Studente"**, in accordo all'azione 9 del PNSD (Piano Nazionale Scuola Digitale), per consentire l'accesso a politiche per il diritto allo studio (ad esempio: accesso a servizi bibliotecari, iniziative culturali convenzionate, accrediti di borse di studio, eccetera) e la creazione di un curriculum delle esperienze formative maturate durante il percorso scolastico (portfolio digitale). È una iniziativa particolarmente strategica ed importante, sebbene al momento non ancora attuata a tutti i livelli e ordini scolastici.

Circa i minori, i quali non possono avere un email/account personale presso servizi quali Google, ad esempio, un'idea potrebbe essere quella di istituire a scuola un **"Account Day"**. Una giornata in cui invitare famiglie e studenti per informarle sulle attività scolastiche che prevedono l'utilizzo di account e identità digitale e magari spiegare ai genitori come creare un account ad hoc, a loro nome, che potranno poi dare in uso ai loro figli. Diventerebbe un'ottima occasione per coinvolgere le famiglie ed educarle ad un uso responsabile e consapevole degli strumenti di rete.

Prima di ogni cosa è fondamentale essere consapevoli del fatto che la nostra identità come persona non è descritta e rappresentata solo da ciò che siamo e facciamo nel mondo tattile, fisico, materiale, quello che comunemente chiamiamo "mondo reale". Anche ciò che siamo e facciamo nel "mondo virtuale" contribuisce a definirci e a definire la nostra identità. È quella che chiamiamo "identità digitale".

Così come curiamo il nostro aspetto prima di uscire di casa per andare a scuola o ad un ristorante, un evento, eccetera, allo stesso modo dovremmo porre attenzione sul modo con cui usciamo e ci presentiamo online.

Se pensate che ciò invece non sia importante, sappiate che, ad esempio, tutte le più grandi aziende nazionali ed internazionali quando devono decidere se assumere o meno un collaboratore, sempre più spesso tengono in minima considerazione il "Curriculum Vitae", magari nel famigerato "Formato Europeo", ma guardano piuttosto come siamo e cosa diciamo nei luoghi online, in particolare nei social: twitter, instagram, facebook, linkedin, eccetera.

Curare la propria presenza social, dunque, è fondamentale, dovrebbe essere una delle competenze da formare negli studenti.

Attenzione dunque alle foto che si pubblicano e al livello di visibilità con la quale le si pubblicano (solo amici, chiunque, eccetera), attenzione al modo con cui ci si esprime e al modo con cui si gestiscono dialoghi e conflitti. Ad esempio, non è raro trovare nei gruppi Facebook frequentati da insegnanti, commenti fuori luogo, spesso offensivi, al limite della calunnia, dimostrando scarsa dialettica, addirittura approssimazione sintattica e ortografica, insomma una serie di ingenuità che non ci si aspetta da un "docente" e che ne squalificano la reputazione e la credibilità. L'identità digitale non è cosa a parte e distinta dall'identità non digitale. Non abbiamo doppie personalità (tranne casi psichiatrici, ma quello è un altro discorso), siamo un tutt'uno ed è bene averlo sempre presente.

Dovremmo, inoltre, come docenti, essere da modello ispiratore, educativo e formativo verso gli studenti, dimostrando competenze e padronanza nell'uso corretto e sano degli strumenti e degli ambienti digitali.

Insultare il Presidente della Repubblica, augurare la morte alle forze di Polizia, ad esempio, sono gesti che non si addicono ad un insegnante, oltre al fatto di essere un reato previsto dal Codice Penale, il quale vale anche online. Saper esprimere opinioni, anche dure e decise, ma in modo corretto e rispettoso, con abilità dialettica e retorica, dovrebbe essere invece l'atteggiamento che un docente, anche in qualità di "pubblico ufficiale dello Stato", dovrebbe sempre avere in ogni luogo e in ogni circostanza.

L'identità digitale, dunque, va curata e tutelata, al pari di quella reale. In che modo?

1.1 Password, profilo e contenuti

Innanzitutto scegliendo l'account con il quale prevalentemente si intende accedere ai vari servizi online, ad esempio quello su gmail.com oppure istruzione.it o quello che preferite, purché ne teniate a mente la password. La gestione della password è fondamentale.

Non preoccupatevi di definire una password criptica e arzigogolata, tranne per quei siti che, disgraziatamente, vi costringono a farlo. L'importante è che sia **una password non banalissima** e che siate in grado di ricordarla con sicurezza. Più è lunga, meglio è.

Non è tanto cioè la cripticità dei caratteri a definire la robustezza di una password, quanto la sua lunghezza. Ad esempio: "We&#!z" è molto più fragile, come password, di: "ciaomifaiaccedereperfavore?".

Abbiate cura della password e, alle brutte, sappiate gestire il semplice procedimento di recupero password che ogni sito ad accesso riservato offre alla bisogna.

Scegliete una **immagine del** vostro **profilo** di cui non dobbiate vergognarvi se dovesse vederla il dirigente scolastico o anche i vostri figli. Non certo un'immagine burocratica da passaporto, anzi, più naturali ed informali si è, meglio è. Però magari la foto ammiccante in bikini con cocktail esotico in mano, riservatela ad un gruppo più ristretto di amici, non come immagine pubblica del proprio profilo social. Evitate, inoltre, di pubblicare foto in cui siano riconoscibili

volti di minori, a meno di non esserne stati espressamente autorizzati o non siano i vostri figli. Valutate comunque sempre e comunque se è il caso di condividere la foto e verificate il livello di privacy (a chi cioè l'immagine sarà visibile).

In generale, tutte le volte che fornite un contributo online accertatevi a chi lo state rendendo visibile e provate a mettervi nei panni dei potenziali lettori del vostro contributo. Cercate di cogliere il contesto, l'intenzione della comunicazione e non assumete a priori che chi vi legge abbia la vostra stessa percezione. **Dosate dunque il vostro contributo in modo coerente all'analisi comunicativa appena fatta**.

Beninteso: massima libertà di opinione ed espressione. L'importante però è che siate consapevoli dell'effetto e delle conseguenze di ciò che viene detto e di come viene detto, in quanto contribuisce a definire la vostra identità digitale. È un accorgimento, peraltro, alla base anche delle azioni di prevenzione del cosiddetto "cyberbullismo", di cui, come docenti, dovreste essere a vostra volta conoscitori ed educatori.

2. VIRUS E RAFFREDDORI

"Accidenti, il mio computer ha preso un virus!".

Si è voluto adottare questa terminologia medica per indicare i casi in cui **un'applicazione malevola viene eseguita sul vostro computer senza che voi ne siate stati consapevoli**.

In realtà l'analogia tra il software malevolo e il virus biologico non risiede tanto sulla modalità con cui viene preso, quanto sulla velocità e modalità di replicazione e propagazione. Tant'è che si usa l'aggettivo: "virale" per indicare anche tutti quei casi in cui una certa informazione, notizia, immagine, musica, eccetera, si diffonde sui social raggiungendo in brevissimo tempo migliaia se non milioni di persone.

La metafora del virus, però, è solo una metafora, ed ovviamente non va presa alla lettera circa il suo meccanismo di azione.

Il virus biologico, infatti, lo si prende per semplice esposizione all'aria o tramite contatto con oggetti contaminati. Non si effettua un'azione esplicita, nessuno di noi insomma si inietta volontariamente un virus, a meno di non far parte di un qualche esperimento scientifico.

Con i virus informatici, invece, è sempre necessaria una qualche esplicita nostra azione.

Chiariamo infatti meglio cosa è un virus: è un programma. È cioè un'applicazione, un software, al pari di Microsoft Word, del Blocco Note, del browser Chrome, di qualunque programma voi decidete di eseguire sul vostro computer.

Perché, questo sia chiaro, **siete sempre e solo voi a decidere quale software eseguire**, non è mai una scelta spontanea del computer o, meglio, del sistema operativo installato sul vostro computer. Non è dunque il computer a "prendere il virus", ma voi ad aver eseguito quel software, più o meno consapevolmente.

Ad esempio, se ricevete un messaggio email dal contenuto scritto in un italiano incerto che vi invita ad aprire un documento allegato perché contiene importanti informazioni circa un premio in denaro che avete vinto o una qualche altra allettante motivazione, non aprite il file allegato. Con alta probabilità contiene codice malevolo, quello che comunemente chiamiamo, appunto, virus. Se invece lo aprite, il programma/virus siete stati voi ad eseguirlo, non è stato il "computer a prendere il virus". Nella fattispecie, siete caduti nello stesso tranello che Ulisse giocò ai troiani con il famoso cavallo di legno. Non a caso, infatti, questo tipo di programma malevolo viene chiamato: **"trojan"**.

Insomma, come dicevamo all'inizio: "non accettare caramelle dagli sconosciuti", è un accorgimento che vale anche in rete.

Certo, non sempre è così evidente riconoscere un tentativo di farci aprire ed eseguire un programma malevolo. Vediamo dunque come in genere può presentarsi un "virus" e anche cosa di effettivamente "malevolo" fa sul nostro computer.

2.1 Tipologie di Malware

Innanzitutto facciamo una precisazione terminologica: il "virus" è in realtà una particolare tipologia della più generale categoria di software malevolo, detta: **"malware"**. Programmi cioè che in qualche modo impediscono al computer un funzionamento regolare o addirittura ne distruggono in modo permanente i dati o ne sfruttano le risorse per altri scopi.

Questi programmi, in genere, sfruttano particolari difetti di progettazione dei sistemi operativi (i cosiddetti **"bachi"**) ma, **sempre più spesso, usano tecniche di "ingegneria sociale"**, sfruttando cioè psicologia, comportamenti e debolezze umane, per indurre direttamente l'utente ad eseguire il programma malevolo, come abbiamo visto nell'esempio della email con allegato allettante.

Di tipi di "malware" ce ne sono vari, ne elenchiamo qui i principali:

- **virus**

  è un programma che attende di essere esplicitamente eseguito. Quando si avvia, il suo codice non fa altro che replicarsi all'interno dei file che si trovano nel computer dove sta girando. In questo senso l'analogia con il virus biologico è calzante.

  In genere rimane sul computer dove è stato eseguito. Se però in questo computer si inserisce ad esempio una chiavetta USB, gli eventuali file contenuti nelle chiavetta vengono "infettati" dal virus (nel senso che il programma si replica anche all'interno dei file presenti sulla chiavetta). Se poi si inserisce la chiavetta USB su un altro computer, quest'ultimo viene a sua volta "infettato" e così via. Un altro motivo per fare a meno delle penne USB e passare al cloud.

  Il danno provocato dalla sua esecuzione è soprattutto legato al consumo delle risorse del computer (memoria e processore), fino ad esaurirle a far arrivare al blocco e riavvio del computer.

- **worm**

sono analoghi ai virus, ma per replicarsi non hanno bisogno di inserirsi nei file del computer. Una volta eseguiti, grazie sempre ad esplicita azione dell'utente, si installano e impostano il sistema operativo in modo da avviarsi automaticamente all'accensione del computer. Per raggiungere altri computer sfruttano internet, in particolare, all'insaputa dell'utente, usano la lista dei contatti email dell'utente per inviare messaggi che i destinatari crederanno essere spediti dall'utente, con allegato il programma malevolo. Costoro, fidandosi, eseguiranno il programma allegato, che in realtà è il worm, il quale si installerà su quest'altro computer e così via.

Analogamente ai virus, i worm in genere mirano a rallentare le funzioni del computer fino a saturarlo e portarlo in blocco.

- **trojan**

Simile al worm. Si presenta come un programma, una foto, insomma un contenuto interessante e allettante, e quando l'utente lo apre, di fatto ne esegue il codice.

In genere sono allegati ad email.

- **ransomware**

sono i malware più pericolosi e dannosi perché hanno un obiettivo davvero criminale.

Una volta eseguiti, in genere con la tecnica dei "trojan", cioè presentandosi come persuasivi allegati ad email, criptano tutti i file presenti sul computer, compresi quelli eventualmente raggiungibili dalla rete locale a cui il computer è connesso. I file, una volta criptati, di fatto non riuscite più a leggerli e ad aprirli. Documenti, foto, ogni contenuto diventa illeggibile. L'operazione viene conclusa con un messaggio, in inglese, con il quale vi si chiede un riscatto in denaro, da pagare seguendo le istruzioni fornite, in modo da ricevere un programma che de-cripta i file riportandoli al loro stato originario. Insomma, è una estorsione a tutti gli effetti. Non cedete al riscatto e anzi denunciate il fatto alla polizia postale in modo che possa attivarsi per tentare di rintracciare la provenienza del programma malevolo, spesso comunque localizzata all'estero.

- **spyware**

è una tipologia di malware che in realtà non danneggia e ostacola il funzionamento del vostro computer, anzi, meno si fa notare meglio è. Il suo scopo, infatti, una volta installatosi ed eseguito, è quello di raccogliere quanti più dati possibile su ciò che fate (siti web che visitate, applicazioni che aprite, mail che scrivete, eccetera) per inviarle ad una azienda che sfrutta queste informazioni per venderle ad agenzie di marketing, ad esempio. Alle volte, noi stessi, con i nostri comportamenti sui social, ci comportiamo di fatto come degli "spyware" ovvero li alimentiamo esplicitamente. Ad esempio, quando su Facebook ci vengono proposti dei giochini del tipo: "quale personaggio storico saresti stato?" o cose del genere, di fatto stiamo autorizzando delle applicazioni, per eseguire il gioco, a raccogliere i nostri dati personali e farne un po' quello che vogliono. Una recente legislazione europea (GDPR) tenta di disciplinare l'esecuzione di questi programmi in modo che anche l'utente più ingenuo e sprovveduto possa essere consapevole di ciò che sta facendo, ma una legge non basta. Occorre, appunto, la saggezza e il buon senso delle nostre nonne. Anche in rete. Divertiamoci, certo, svaghiamoci, giochiamo anche in rete, ci mancherebbe. Ma in modo sano, responsabile e, soprattutto, consapevole.

- **adware**

anche questa è una tipologia di malware che non fa grossi danni tranne che dare un gran fastidio. Una volta eseguito, infatti, di solito modifica il comportamento del nostro browser, mostrandoci continuamente, su ogni sito web e pagina che visitiamo, annunci pubblicitari vari e improbabili, alcuni persino dal contenuto scabroso e inopportuno.

3. COME DIFENDERCI DAI MALWARE?

Innanzitutto installando sul nostro computer delle applicazioni che hanno il compito di riconoscere ed intercettare l'esecuzione di software malevolo e di bloccarle: i cosiddetti **"anti-virus"**. Sul mercato ce ne sono tanti in circolazione, alcuni gratuiti, altri a pagamento. È importante tenere aggiornato l'antivirus in modo che sia in grado di riconoscere anche gli ultimi malware diffusi continuamente in rete.

In secondo luogo, facendo sistematici e frequenti **"backup"** del vostro computer, cioè delle copie integrali del contenuto dei dischi del computer su altri dischi, su penne USB o, meglio ancora, su archivi cloud. Infine e, direi, la cosa più importante, **buon senso**. Abbiate buon senso quando consultate la posta e visitate siti web. In particolare, fate attenzione ai cosiddetti tentativi di **"phishing"**, cioè a quelle mail, inviate magari dalla vostra banca (apparentemente) che vi chiedono di cliccare un determinato link per modificare le credenziali di accesso e che in realtà vi portano ad una pagina web che graficamente riproduce quella della banca ma, se fate caso all'url, non corrisponde davvero all'indirizzo web della banca (un po' come quegli oggetti contraffatti come gli orologi CCCCP, scarpe Avidas, e così via) e hanno lo scopo di raccogliere la vostra password e quindi farci con essa operazioni di prelievo sul vostro vero conto, prosciugandolo.

Insomma, occhi aperti, guardate bene il link che state cliccando, analizzatene l'url, cestinate messaggi che vi sembrano "strani", scritti con grammatica incerta, persino se provenienti da mittenti che conoscete e di cui di solito vi fidate. Lasciate perdere le penne USB, se potete. Buon senso.

3.1 Virus che non ce l'hanno con noi

Potrebbe venire naturale chiederci: virus, cui prodest? A chi giova sabotare computer di mezzo mondo? Perché darsi tanta pena nell'escogitare sistemi che sfruttano falle e vulnerabilità dei nostri dispositivi e, soprattutto, le nostre personali debolezze psicologiche, per metterli fuori uso?

In origine i "virus" erano il modo con il quale un movimento di sviluppatori e informatici di tutto il mondo voleva metterci in guardia su come stessimo ingenuamente affidando parti importanti della nostra vita a sistemi oggettivamente deboli e fragili, dei quali non avevamo neanche piena competenza. È questa idea alla base del movimento dell'etica "hacker". In questo senso il virus va inteso positivamente. Dovremmo cioè essere grati agli "hacker" tutte le volte che rilevano i difetti strutturali dei sistemi informatici con i quali ormai regoliamo ogni azione della nostra esistenza, dai computer delle sale di rianimazione degli ospedali, a quelli che controllano il traffico dei voli, alle banche che gestiscono i nostri risparmi, al computer domestico e tutti i vari dispositivi digitali presenti ormai in ogni casa: router wifi, smartphone, videocamere, eccetera.

Oggi, però, "hacker" ha acquisito un'accezione negativa, associata a furti e distruzioni di dati, ricatti online, eccetera. Più propriamente gli autori di tali azioni, veri e propri reati, si chiamano "**cracker"**. In Italia l'assonanza con i cracker salati, con cui alcuni hanno l'abitudine di fare lo spuntino di mezza giornata, ha scoraggiato l'uso di questo termine, preferendo il più suggestivo: "hacker".

Sempre più di frequente può capitare, però, che i virus installati sul nostro computer non abbiano come obiettivo né i dati del nostro computer, né ottenere un immediato profitto economico. Non ce l'hanno insomma con noi. Anzi, rimangono nascosti e silenti cercando di farsi notare il meno possibile. Il loro vero obiettivo è altro, e cioè sfruttare, in un momento convenuto, il nostro computer per usare le sue risorse, insieme a migliaia, anzi, milioni di altri computer nel frattempo "infetti", per lanciare in modo coordinato e sincronizzato un attacco verso il vero obiettivo. Spesso il vero obiettivo è un sito governativo, se l'organizzazione autore del virus è di tipo politico o a carattere terroristico, oppure un sito strategico, popolare e famoso. Il nostro dispositivo, insomma, è solo un inconsapevole strumento di offesa verso un altro obiettivo.

Immaginate, infatti, di inviare tutte insieme, nello stesso momento, milioni di richieste ad uno stesso sito, una montagna tale di richieste da far andare in tilt il sito stesso, il quale, in questi casi, si blocca mettendosi in uno speciale stato di protezione che lo porta a rifiutare del tutto ogni richiesta, in inglese: **"Denial Of Service"**.

Questo tipo di attacchi prendono il nome di DOS (Denial Of Service). Per raggiungere l'obiettivo, occorrono però, appunto, migliaia, milioni di dispositivi che nello stesso tempo inondando il sito obiettivo. In genere questi dispositivi sono distribuiti in tutto il mondo, e allora l'attacco si chiama: **Distributed Denial Of Service (DDOS)**.

È quello che è successo, ad esempio, il 21 ottobre del 2016, giorno in cui i più importanti siti della costa est degli Stati Uniti rimasero oscurati per diverse ore, suscitando panico e persino contraccolpi in borsa. Servizi come Netflix, Twitter, Spotify, New York Times, eccetera, del tutto fuori uso.

Cos'era successo? Un DDOS rivolto verso la società che forniva i rispettivi server, la Dyn.

In pratica è come se in Italia avessero messo fuori uso le centraline della TIM, senza usare bombe ma solo virus informatici.

È interessante e soprattutto istruttivo citare questo episodio perché a seguito delle indagini che seguirono si scoprì da dove fossero provenute le richieste simultanee che nel loro insieme hanno messo fuori uso i sistemi della Dyn: dagli Stati Uniti stessi.

E, pensate un po', la maggior parte di questi dispositivi non erano neanche computer, bensì oggetti comuni posseduti da ignari e onesti cittadini americani: videocamere di sorveglianza, router wifi domestici, fotocamere digitali, eccetera.

Quando compriamo un oggetto digitale che prevede che si connetta ad internet, pochi di noi si preoccupano di cambiare le impostazioni di fabbrica, in particolare la password di amministrazione che permette di configurare inizialmente il dispositivo in modo che possa essere usato nella nostra rete. Questa debolezza umana è stata sfruttata dal virus messo a punto per l'attacco dell'ottobre 2016. Il virus, infatti, cercava di prendere il controllo dei dispositivi provando in modo automatico tutte le possibili password "di fabbrica", ad esempio: admin/admin, admin/password, admin/1234, e così via, confidando che non fossero state modificate. Una volta preso il controllo, si è installato ed è rimasto lì in esecuzione, silente e tranquillo. Al momento predefinito, sfruttando la connessione ad internet del dispositivo ha inviato la richiesta al sito obiettivo, insieme agli altri migliaia, realizzando l'attacco.

Qual è la morale della storia? **Quando comprate un dispositivo digitale**, un router, una videocamera di sorveglianza wifi, e così via, **cambiate la password** di amministrazione fornita dalla fabbrica. Nel manualetto che in genere accompagna il dispositivo sono indicate chiaramente le istruzioni su come fare. Ricordatevelo, se non volete essere involontari complici di un attacco informatico.

3.2 Navigare in incognito

Spesso a scuola capita di usare un computer che **non è di uso personale** ed esclusivo. Non è cioè il nostro computer portatile, oppure tablet o smartphone, ma un computer d'uso condiviso, magari nella sala docenti, oppure in classe collegato alla LIM e così via.

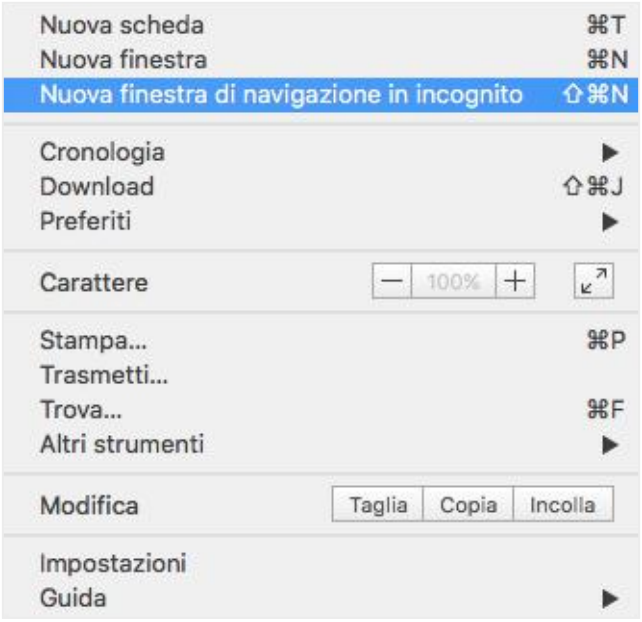
Su questo tipo di computer si può avere la necessità di effettuare l'accesso però a servizi personali, quale ad esempio Google Drive, oppure Gmail e in generale ogni altro sito che prevede credenziali di accesso riservate.

Non è una buona pratica inserirle in maniera disinvolta. Anche se ci assicuriamo di non aver salvato la password, infatti, rimane comunque traccia su quel computer dei siti che abbiamo usato e perlomeno dell'account iniziale che abbiamo fornito, ad esempio il nostro indirizzo email.

In questo caso è utile attivare sul browser la cosiddetta "navigazione in incognito".

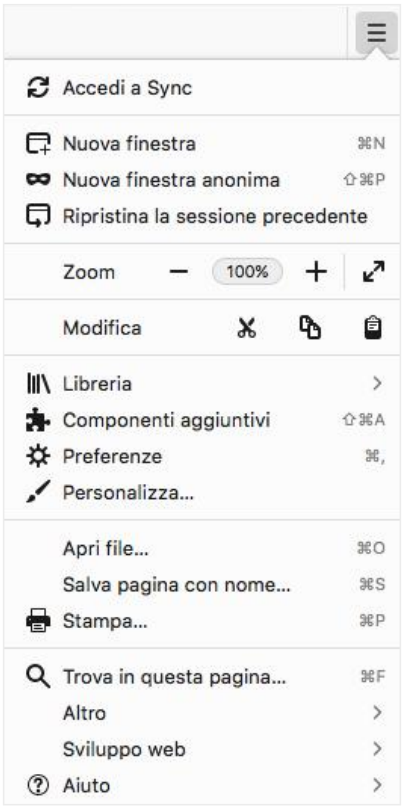
Questa impedisce al browser di memorizzare e tenere traccia della cronologia della navigazione (la sequenza dei siti visitati) e anche di ogni dato scritto per accedere a servizi riservati (email, password, eccetera).

Tutti i browser prevedono l'attivazione di questa modalità; qui vedete ad esempio come attivarla su Chrome:



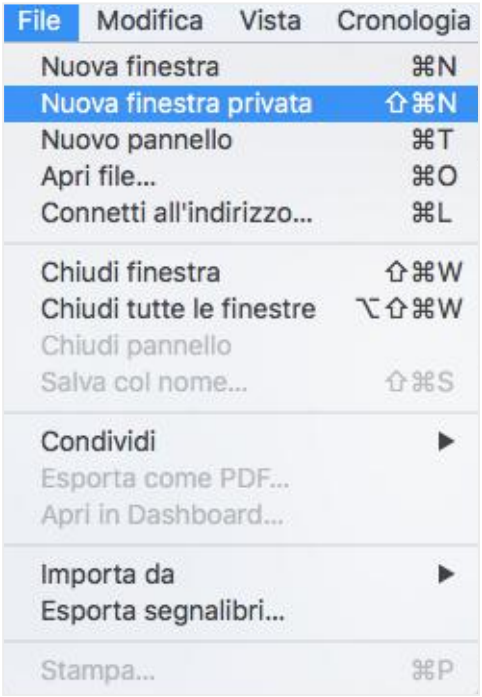
3.1 | Apertura di una nuova finestra di navigazione in incognito su Chrome

su Mozilla Firefox:



3.2 | Apertura di una Nuova finestra anonima su Mozilla Firefox

su Safari:



3.3 | Apertura di una nuova finestra privata su Safari

Se state usando un altro browser e non siete sicuri su come attivare la modalità "navigazione in incognito" andate su Google e cercate una guida di riferimento, digitando magari il nome del browser che state usando e poi "navigazione privata" oppure "navigazione in incognito" come criterio di ricerca.

Sicuramente otterrete tra i risultati delle pagine che potranno spiegarvi la procedura e quindi seguirla.

Buona navigazione, sana e sicura!

www.certipass.org

- ENTE EROGATORE DEI PROGRAMMI INTERNAZIONALI DI CERTIFICAZIONE DELLE COMPETENZE DIGITALI EIPASS
- ENTE ACCREDITATO DAL MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA PER LA FORMAZIONE DEL PERSONALE DELLA SCUOLA – DIRETTIVA 170/2016
- ENTE ISCRITTO AL WORKSHOP ICT SKILLS, ORGANIZZATO DAL CEN (EUROPEAN COMMITTEE FOR STANDARDIZATION)
- ENTE ADERENTE ALLA COALIZIONE PER LE COMPETENZE DIGITALI – AGID
- ENTE ISCRITTO AL PORTALE DEGLI ACQUISTI IN RETE DELLA PUBBLICA AMMINISTRAZIONE, MINISTERO DELL'ECONOMIA E DELLE FINANZE, CONSIP (L. 135 7 AGOSTO 2012) | MEPA
- ENTE PRESENTE SU PIATTAFORMA SOFIA E CARTA DEL DOCENTE

PER INFORMAZIONI SULLE CERTIFICAZIONI INFORMATICHE **VISITA IL SITO**

www.eipass.com