ISTITUTO DI ISTRUZIONE SUPERIORE

SOLERI BERTONI

Saluzzo

SICUREZZA

TEAM DIGITALE

INDICE

1. SICUREZZA: COME NAVIGARE IN SICUREZZA pag. 3
2. CREARE UNA PASSWORD SICURA pag. 4
3. GESTIRE LE PASSWORD pag. 5
4. SICUREZZA pag. 6
5. SPOOFING pag. 7
6. PHARMING pag. 8
7. REDIRECTING pag. 9
8. ANTIVIRUS E SICUREZZA pag. 10
9. DA COSA PROTEGGE L'ANTIVIRUS? pag. 12
10. GLOSSARIO pag. 15

1. Sicurezza: come navigare in sicurezza

La **protezione** dei nostri account **deve essere la nostra priorità** quando navighiamo su internet o usiamo un dispositivo, che sia esso un PC, uno smartphone o un tablet.

La **password è il nostro primo sistema di difesa**, che impedisce ad altri di accedere ai nostri dispositivi, ai nostri account, e quindi di accedere a dati privati.

A volte anche una buona password può risultare inutile, in quanto la **minaccia arriva via email**, ben nascosta, **attraverso indirizzi mail** che ad una prima occhiata **potrebbero essere innocui**.

Lo stesso vale per la **navigazione in rete**: **non tutti i siti sono affidabili** ed è necessario saperli riconoscere per evitare di incappare in problemi.

1. Sicurezza: come navigare in sicurezza

Con **spam** si intendono quei **messaggi**, generalmente pubblicità, **inviati molto frequentemente ad un utente attraverso indirizzi generici**. Lo spam non arriva solo tramite mail, ma anche chat, tag etc.
Come detto generalmente **riguarda pubblicità, ma accade anche si tratti di email spam di truffe, che ci chiederanno di inserire i nostri dati**.

Nelle email possono comparire email spam di tipo **phishing**, ovvero **email di truffa** che, **spacciandosi per mittenti affidabili, invitano il destinatario ad inserire i propri dati per poterli rubare e utilizzare**.

Andando ad inserire i nostri dati quando richiesto da email simili potremmo **incorrere nel furto d'identità. in quanto altre persone diverse da noi utilizzeranno il nostro nome e i nostri dati**.

Vedremo di **seguito alcuni esempi** di Email spam e truffe, alcune volte anche al furto di dati.

2. Creare una password sicura

Una **password** sicura deve essere costituita da **almeno otto caratteri** tra **numeri**, **lettere** e **caratteri speciali**.

La cosa migliore è **non usare parole comuni**, il **nostro nome**, la **data di nascita**, in più vanno **alternate maiuscole e minuscole**.

Per una maggiore protezione sarebbe meglio **utilizzare una password diversa per ogni sito che la richieda**.

Potreste, per esempio, **sostituire simboli e numeri ad alcune lettere del vostro nome**.

P@$$w0Rd%E$eMp!0

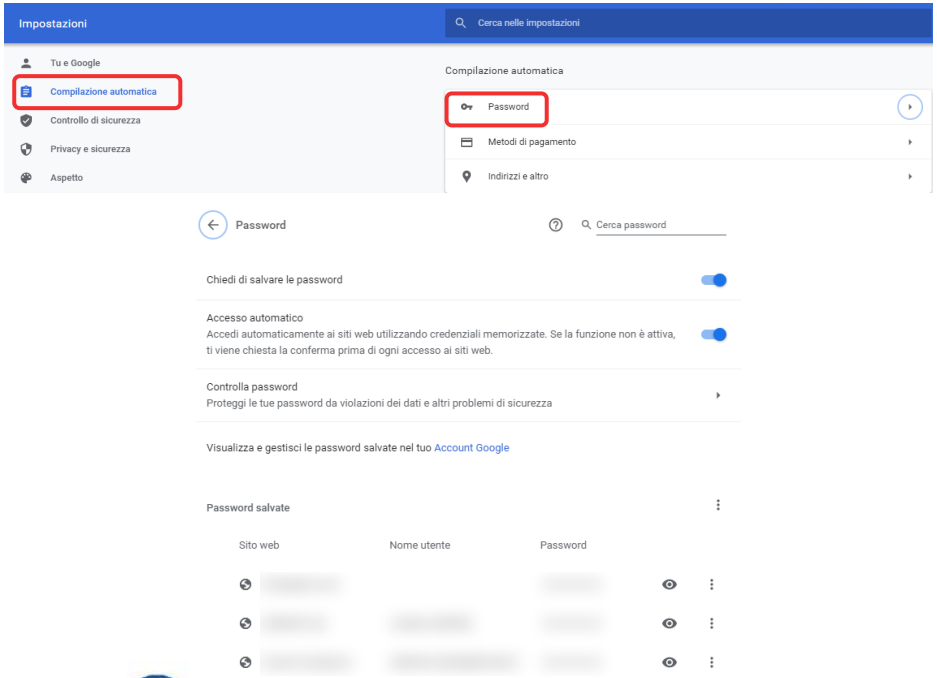
3. Gestire le password

Ricordare le **password** per diversi siti può risultare difficile e **spesso ci si dimentica o confonde**.

La cosa migliore sarebbe **evitare di scrivere le password sul pc o** nello stesso luogo in cui abbiamo la nostra postazione.

Possiamo utilizzare dei **programmi e delle applicazioni che fungono da archivio per le nostre password** e dalle quali potremo recuperarle con un click.

Anche il nostro **browser permette di salvare le password**, sebbene l'ideale sia quella di non salvare mai alcuna password.



4. Sicurezza

Sicurezza è un concetto estremamente importante per chi usa dispositivi digitali e naviga su internet.

Proteggendo con **antivirus** i nostri dispositivi eviteremo anche che qualcuno violi la nostra privacy, ma dobbiamo stare attenti noi per primi a quello che condividiamo su internet, **evitando di rendere pubblici dati che riguardano noi e chi ci sta vicino**.

Tramite **software** dedicati e alcuni piccoli accorgimenti cercheremo di proteggerci e mantenere privati dati che non vorremmo fossero condivisi.

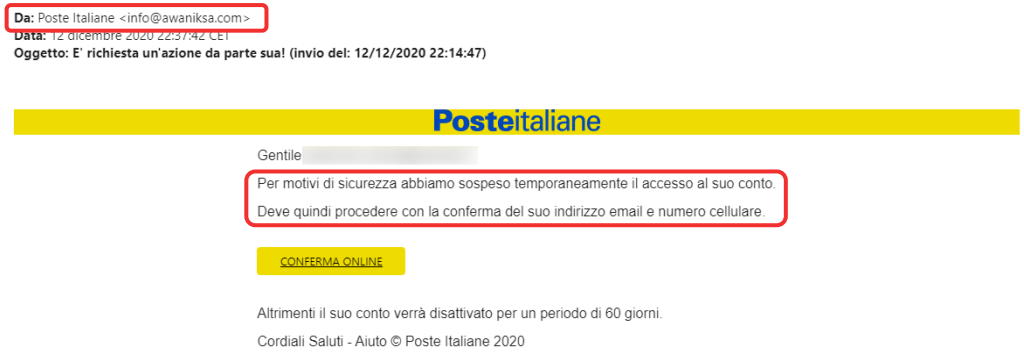
Vedremo alcuni tra i tipi di **spam** e **virus**.

5. Spoofing

Lo **Spoofing** consiste nel **mascheramento o falsificazione di diverse informazioni** riguardanti, per esempio, il mittente di un messaggio.

Qui ad esempio vediamo una mail che sembra essere inviata da Poste Italiane. In realtà, guardando bene l'indirizzo del mittente, notiamo che si tratta di una email truffa.

Possiamo inoltre **controllare il testo della email**: generalmente in questi casi si tratta di messaggi con **errori grammaticali e scritti in un italiano stentato o che richiedono nostre informazioni minacciando pagamenti o blocchi dell'account.**



Da: Poste Italiane <info@awaniksa.com>
Data: 12 dicembre 2020 22:37:42 CET
Oggetto: E' richiesta un'azione da parte sua! (invio del: 12/12/2020 22:14:47)

Posteitaliane

Gentile

Per motivi di sicurezza abbiamo sospeso temporaneamente il accesso al suo conto.
Deve quindi procedere con la conferma del suo indirizzo email e numero cellulare.

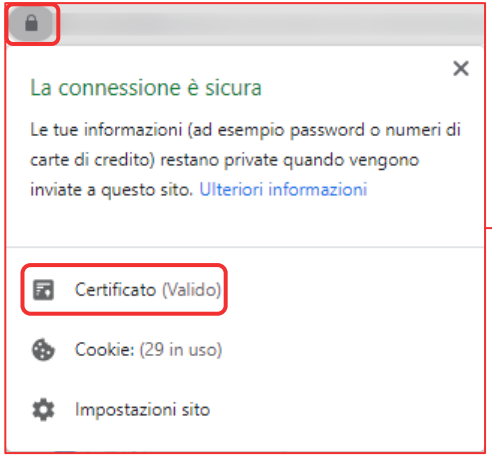
CONFERMA ONLINE

Altrimenti il suo conto verrà disattivato per un periodo di 60 giorni.
Cordiali Saluti - Aiuto © Poste Italiane 2020

6. Pharming

Il **Pharming consiste nel reindirizzamento dell'utente dal sito che stava cercando ad un altro fittizio**, il quale potrebbe **installare un virus** sul nostro dispositivo, oppure **rubare dei dati** nel momento in cui andiamo ad inserirli o tentiamo l'accesso al sito.

In questo caso è difficile riconoscere un sito fittizio, in quanto si presenta pressoché identico a quello originale, ma una **soluzione** può essere l'adozione di un buon **antivirus**, insieme ad alcuni accorgimenti: **evitare siti sospetti**, **non cliccare link in email ambigue**, prestare **attenzione ad anomalie nel sito**, che potrebbe richiederci informazioni mai richieste prima.



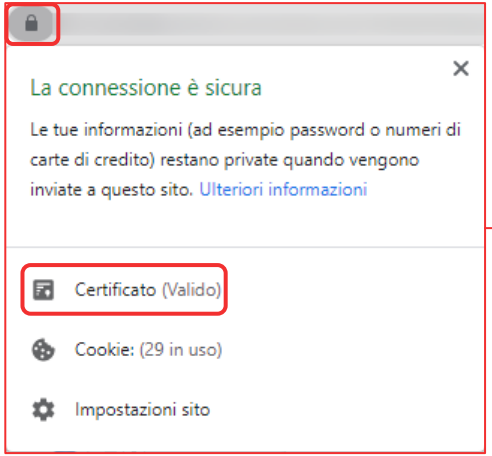
Possiamo anche cliccare sul lucchetto nella barra degli indirizzi, che ci indica un sito sicuro, ma ci permette di verificare abbia un certificato valido e sicuro.

7. Redirecting

Il **Redirecting** consiste nella **deviazione ad un altro indirizzo diverso da quello digitato**, in modo che gli utenti visualizzino una pagina differente da quella desiderata, spesso **contenente spam** o appositamente **creata per farci inserire dati personali o installare malware**.

Per difendersi da queste pratiche è necessario **controllare sempre il sito nella barra di ricerca**, che in caso di redirecting dovrebbe cambiare e ancora il **lucchetto nella barra di ricerca**.

Un buon **antivirus** dovrebbe anche **segnalare l'anomalia**.



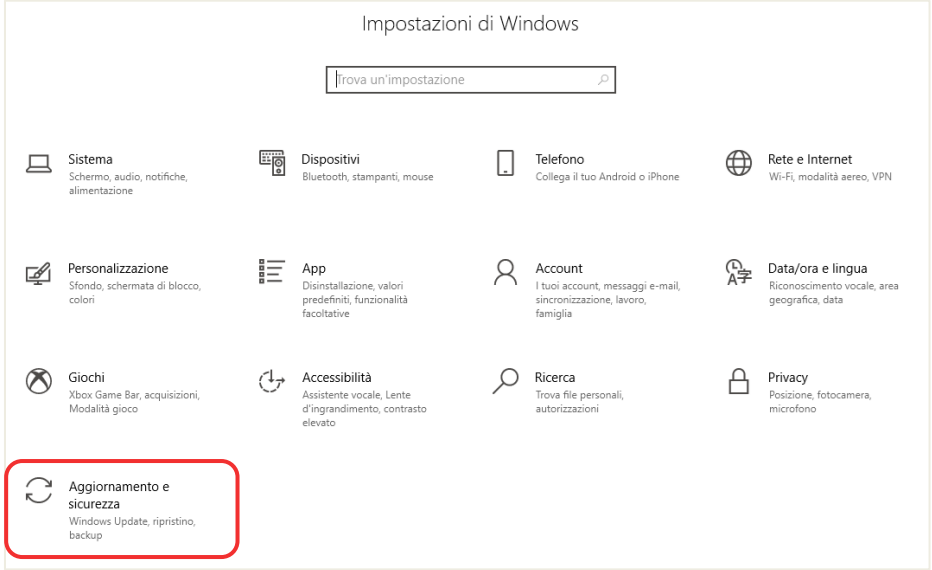
Possiamo anche cliccare sul lucchetto nella barra degli indirizzi, che ci indica un sito sicuro, ma ci permette di verificare abbia un certificato valido e sicuro.

8. Antivirus e sicurezza

L’**antivirus** è uno speciale **software che monitora il costantemente il nostro dispositivo**, ma perché sia efficace è necessario sia **sempre aggiornato**.

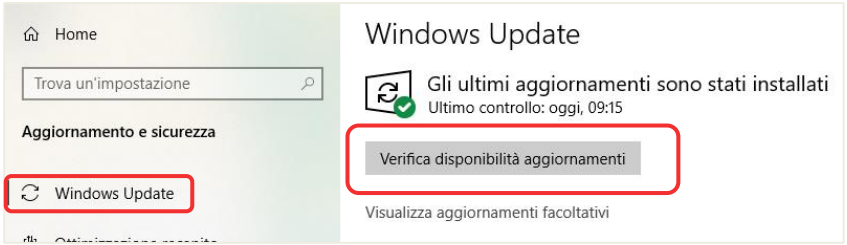
Windows ha già integrato un antivirus, ma possiamo anche acquistarne uno. Non esiste, di fatto, un software di questo tipo migliore di un altro.

Per cominciare possiamo assicurarci che quello di Windows sia attivo e aggiornato nelle **impostazioni** del nostro pc.

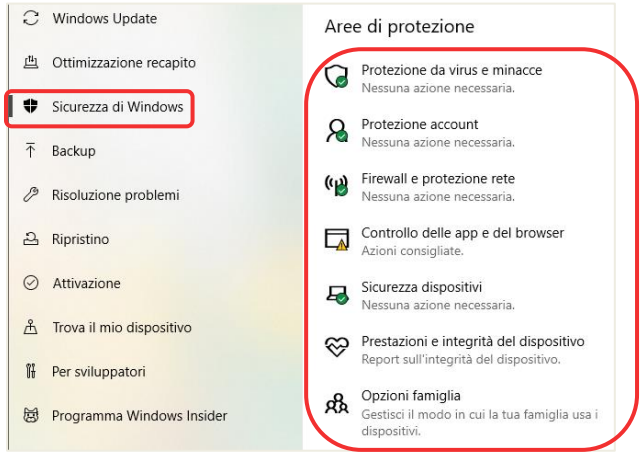


8. Antivirus e sicurezza

Controllare quindi che il **pc sia aggiornato** e, nel caso in cui non lo sia, aggiornatelo.



Potete anche assicurarvi non ci siano problemi cliccando sul tasto **Sicurezza di Windows**.



Nel caso in cui il computer avesse rilevato **attività sospette** questo ve lo **segnalerà**.

9. Da cosa ci protegge l’antivirus?

L’antivirus ci protegge dai cosiddetti **malware**, termine con il quale si identifica qualsiasi tipo di **programma utilizzato per danneggiare un computer o rubare segretamente informazioni**.

I malware possono essere di diversi tipi:

- **Virus**
- **Trojans**
- **Spyware**
- **Adware**

  etc...

10. Da cosa ci protegge l’antivirus?

Virus e Trojans

I **Virus** vengono diffusi attraverso programmi infetti e si riproducono all'interno di un computer.

I Virus **si trasmettono** principalmente tramite **email di spam** o tramite **dischi esterni infetti**, tramite **download** di programmi da Internet o attraverso **file**.

I **Trojans** sono programmi infetti che **mascherano la loro identità** così che lo si installi, magari spacciandosi addirittura per un antivirus.

I Trojan di solito vengono **diffusi** quando un **eseguiamo un allegato** di una e-mail all’apparenza innocua, o ad effettuare un **download**.

10. Da cosa ci protegge l’antivirus?

Spyware e Adware

Gli **Spyware** spiano quello che facciamo sul computer e su Internet, **raccogliendo dati e monitorando le nostre attività**. Ci mostrano anche **pubblicità indesiderate**.

Solitamente si incontrano **installando programmi da siti poco attendibili**, oppure **ad-ons infetti**.

Gli **Adware** sono speciali malware che ci **mostrano pubblicità** quando utilizziamo specifici programmi e tramite **pop-up allarmistici cercano di convincerci ad acquistare qualche cosa**.

Spesso **accompagna lo Spyware**.

GLOSSARIO

Antivirus: programma che blocca i malware e protegge il nostro dispositivo, avvisandoci in caso di comportamenti sospetti da parte di un sito, un programma o un file.

Browser: è un software che consente di navigare il World Wide Web: cioè l'insieme dei siti internet.

Consenso: Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

E-mail: posta elettronica. Servizio Internet che consente di inviare e ricevere messaggi utilizzando un dispositivo (pc, smartphone, tablet) connesso in rete attraverso un proprio account di posta registrato presso un fornitore del servizio.

Informativa: La comunicazione che fornisce tutte le informazioni utili che l'interessato deve sapere nel momento in cui decide di dare il suo consenso al trattamento dei dati personali.

Malware: Un malware, abbreviazione di "malicious software", è un software intenzionalmente progettato per causare danni a un computer. I virus informatici, worm, trojan, spyware, adware sono tipi di malware.

Password: sequenza di caratteri (lettere, numeri, caratteri speciali) utilizzata per accedere in modo esclusivo a una risorsa informatica.

Pharming: il Pharming consiste nel reindirizzamento dell'utente dal sito che stava cercando ad un altro fittizio.

Popup: Un tipo di finestra che si apre sullo schermo del dispositivo senza che l'utente selezioni un comando.

GLOSSARIO

Software: Il software è costituito da applicazioni eseguite su computer o portatili. Quando le applicazioni vengono eseguite su dispositivi mobili, vengono solitamente chiamate app.
Spyware: Tipo di malware capace di spiare le attività svolte sul computer. Uno spyware è in grado di registrare quello che digitiamo con la tastiera "rubando" le credenziali di accesso (nome utente e password) degli account

Redirecting: il Redirecting consiste nella deviazione ad un altro indirizzo diverso da quello digitato, in modo che gli utenti visualizzino una pagina differente da quella desiderata.

Spam: numero elevato di email non richieste generalmente relative a pubblicità indesiderata.

Spoofing: lo Spoofing consiste nel mascheramento o falsificazione di diverse informazioni riguardanti, per esempio, il mittente di un messaggio.

Trojans: Cavallo di Troia, un tipo di malware che utilizza un programma "buono" per entrare all'interno del sistema.