VENERDÌ, 18 DICEMBRE 2009 ORE 15:30 A MESTRE

TECNOLOGIE INFORMATICHE E PROFESSIONE FORENSE

Avv. Giorgio BATTAGLINI - Foro di Venezia
Avv. David D'AGOSTINI - Foro di Udine
Avv. Fabrizio PETTOELLO - Foro di Udine
Avv. Marisa BONANNO - Foro di Verona

CAMERA CIVILE VENEZIANA

CIRCOLO DEI GIURISTI TELEMATICI
CGT
www.giuristitelematici.it

Avv. Giorgio Battaglini

Camera Civile Veneziana - Circolo dei Giuristi Telematici

SICUREZZA DEI DATI
DELLO STUDIO

Avv. Giorgio Battaglini
Circolo dei Giuristi Telematici – Camera Civile Veneziana

SICUREZZA

Al di là delle definizioni normative, la sicurezza va intesa come un PROCESSO ove nessuna soluzione è mai definitiva.

Il "processo sicurezza" non è un semplice prodotto da acquistare ed installare e comprende sia un fattore materiale, tecnico, sia un fattore umano, che notoriamente costituisce l'anello debole della cd. *security chain*.

La sicurezza assoluta non esiste. E' un processo che va gestito continuamente ed esistono solo livelli diversi di sicurezza, più o meno alti, che dovranno essere proporzionali all'importanza del bene da custodire.

MISURE DI SICUREZZA

OBBLIGHI NORMATIVI

→ **M. di S. MINIME**

(Artt.33-36 CODICE PRIVACY + D.T.)

RESPONSABILITA' PENALE

→ **M. di S. IDONEE**

(Art. 31 CODICE PRIVACY)

RESPONSABILITA' CIVILE

MISURE DI SICUREZZA

Art. 33 MISURE MINIME

I titolari del trattamento sono tenuti ad adottare le misure minime, individuate dal codice volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 31 MISURE IDONEE

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

MISURE MINIME DI SICUREZZA

Art. 4 Cod. Privacy DEFINIZIONE

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di distruzione o perdita (anche accidentale) dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

MISURE DI SICUREZZA

SONO PROPRIO NECESSARIE ?

MISURE DI SICUREZZA

SONO PROPRIO NECESSARIE ?

FATE UN SEMPLICE TEST DI PORTSCAN SUL VS. P.C. !

Su http://www.pcflank.com/scan.php o http://security.symantec.com/sscv6

Results of Advanced Port Scanner

TCP CONNECT scanning (scanned in 72 seconds)

We have scanned your computer' ports used by the most widespread trojan horses. Here is the description of possible ports' statuses:

"Stealthed" (by a firewall) -Means that your computer is invisible to others on the Internet and protected by a firewall or other similiar software;
"Closed" (non-stealthed) - means that this port is closed, but your computer is visible to others on the Internet that can be potentially dangerous;
"Open" - Means that this port is ready to establish (or has already established) a connection with remote address. It also means that your computer is vulnerable to attacks and could have been already hacked or infected by a trojan/backdoor;

Port:	Status	Service	Description
21	stealthed	FTP	File Transfer Protocol is used to transfer files between computers
23	stealthed	TELNET	Telnet is used to remotely create a shell (dos prompt)
80	stealthed	HTTP	HTTP web services publish web pages
135	stealthed	RPC	Remote Procedure Call (RPC) is used in client/server applications based on MS Windows operating systems
137	stealthed	NETBIOS Name Service	NetBios is used to share files through your Network Neighborhood

MISURE DI SICUREZZA

SONO PROPRIO NECESSARIE ?

FATE UN ALTRO TEST SUL SITO

http://analyze.privacy.net

This site analyzes the privacy of your Internet connection and shows what web sites can know about you when you visit. The information can be used to display personalized web content for your country and web browser and increase security for business transactions.

Your Are Visiting From:
82.60.159.37 is from Italy(IT) in Western Europe
Host name: host37-159-dynamic.60-82-r.retail.telecomitalia.it

Cookie Test

No Cookie from this site is on your system from prior visits.

Your Browser Type and Operating System:

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; IusOnDemand.com; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; .NET CLR 1.1.4322)

All information sent by your web browser when requesting this web page:

Cache-Control: no-cache Connection: Keep-Alive Content-Length: 2404 Content-Type: application/x-www-form-urlencoded Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, */* Accept-Encoding: gzip, deflate Accept-Language: it Cookie: Privacy.net_Last_Visit=6/14/2008; Privacy.net=Privacy+Analysis; bhCookieSaveSess=1; bhCookieSess=1;

Browser Type and Version

Browser: IE
Fullversion: 6.0
ServicePack: ;SP2;
Gecko: False
Crawler: False

Browser Security

Session Cookies Not Accepted
Persistant Cookies Accepted
JavaScriptEnabled: True
VBScriptEnabled: True
JavaEnabled: True
ActiveXEnabled: True
SSL: True
SSLActive: False
SSLKeySize: 128
SSLEnabled: True
Firewall: True
OpenPorts:
PopupsBlocked: True
ImagesEnabled: False
HighSecurity: False

Connection Details

Broadband: False
ConnectionType:
Firewall: True
Proxy: False
CompressGZip: True
AOL: False
MSN: False

Display and Layout

Width: 1024
WidthAvail: 1003
Height: 768
StyleSheets: True
PNG: True
FontSmoothing: True
FontColor: True
FontSize: True
TextSize: 7
Tables: True
TableBGColor: True
TableBGImage: True
ColorDepth: 32
Frames: True
IFrames: True
DisplayXDPIActual: 96
DisplayYDPIActual: 96
DisplayXDPILogical: 96
DisplayYDPILogical : 96

Scripting Capabilities

ActiveXControls: True
ActiveXEnabled: True
JavaScript: True
JavaScriptEnabled: True
JavaScriptVer: 1.3
JavaScriptBuild: 5.6.8835
VBScript: True
VBScriptEnabled: True
VBScriptBuild: 5.6.8835
XML: True
MSXML: 4
XMLHttpRequest: True
DHTML : True
FileUpload: Yes

System Details

Platform: WinXP
Win16: False
WinInstallerMinVer: 2

Plug-in Information

Plugin Flash Version: 9,0,45,0
Plugin Flash Version: 10.2r23
Plugin QuickTime Version: Installed (version 7.1.5)
Plugin RealPlayer Version: 6.0.12.1739
Plugin MediaPlayer Version: 11.0.5721.5230
Plugin Flip4Mac installed

Java Information

JavaApplets: True
JavaEnabled: True

Wireless Device Information

PDA: False
WAP: False
HDML: False

Locale Information

Country: IT
Language: Italian
User Language: it
System Language: it
Time Zone Difference: 6
Browser Date and Time : sabato 14 giugno 2008 15.16.55
Browser Date and Time ms: 1213449415296

MISURE DI SICUREZZA
SONO PROPRIO NECESSARIE ?
SI

La sicurezza è un elemento sempre più importante poiché in Internet i tentativi di intrusioni, phishing, hacking, diffusione di worm e virus continuano ad aumentare.

Con 2.000 minacce dannose emergenti ogni mese, gli utenti di Internet devono continuare a proteggere i propri strumenti elettronici e i dati in essi contenuti.

MISURE DI SICUREZZA

SICUREZZA DELL'AMBIENTE DI LAVORO

ATTIVARE IMPOSTAZIONI DI SICUREZZA DEL SISTEMA OPERATIVO

- ATTIVARE SISTEMA DI AUTENTICAZIONE PROTETTO DA PSW PER L'ACCESSO AL PC (DISATTIVARE ACCOUNT GUEST)

- ATTIVARE SE NECESSARIO SISTEMA DI AUTORIZZAZIONE PROTETTO DA PSW PER L'ACCESSO A TALUNI TIPI DI DATI

- IMPOSTARE SCREENSAVER PROTETTO DA PSW (MAX 3 min)

- EFFETTUARE PERIODICI BACK- UP

- DISABILITARE ACCESSO REMOTO AL P.C.

- NEGARE O RIDURRE AL MINIMO NECESSARIO LA CONDIVISIONE DI FILE E CARTELLE PERSONALI

N.B. UTILIZZARE SOLO PASSWORD ROBUSTE (Min. 8 caratteri e con LetteRe, num3r1 e $imbo£i)

SICUREZZA DELL'AMBIENTE DI LAVORO

ATTIVARE IMPOSTAZIONI DI SICUREZZA DEL SISTEMA OPERATIVO

- ATTIVARE SISTEMA DI AUTENTICAZIONE PROTETTO DA PSW PER L'ACCESSO AL PC
- DISATTIVARE ACCOUNT GUEST
- CREARE ACCOUNT LIMITATO "SENZA POTERI" PER ALTRI UTENTI E PER INTERNET

pannello di controllo/account utente

	Amministratore del computer	Account limitato
Installazione di programmi e hardware	✓	
Modifica delle impostazioni globali del sistema	✓	
Accesso e lettura di tutti i file non privati	✓	
Creazione ed eliminazione degli account utente	✓	
Modifica degli account di altri utenti	✓	
Modifica del nome o del tipo del proprio account	✓	
Modifica dell'immagine associata al proprio account	✓	✓
Creazione, modifica o rimozione della propria password	✓	✓

SICUREZZA DELL'AMBIENTE DI LAVORO

INSTALLARE E IMPOSTARE ALCUNI SOFTWARE PER LA SICUREZZA

- **FIREWALL** (hardware or software device which is configured to permit, deny, or proxy data through a computer network which has different levels of trust)

- **ANTI VIRUS** (worms, trojan horses, rootkits and other malicious code)

- **SOFTWARE CONTRO VARI MALWARE** (spyware, adware, nagware o annoyware, parasiteware, unwelcome cookies, aggressive advertising, keyloggers, trojans, dialers, browser hijackers, tracking components and various forms of viruses).

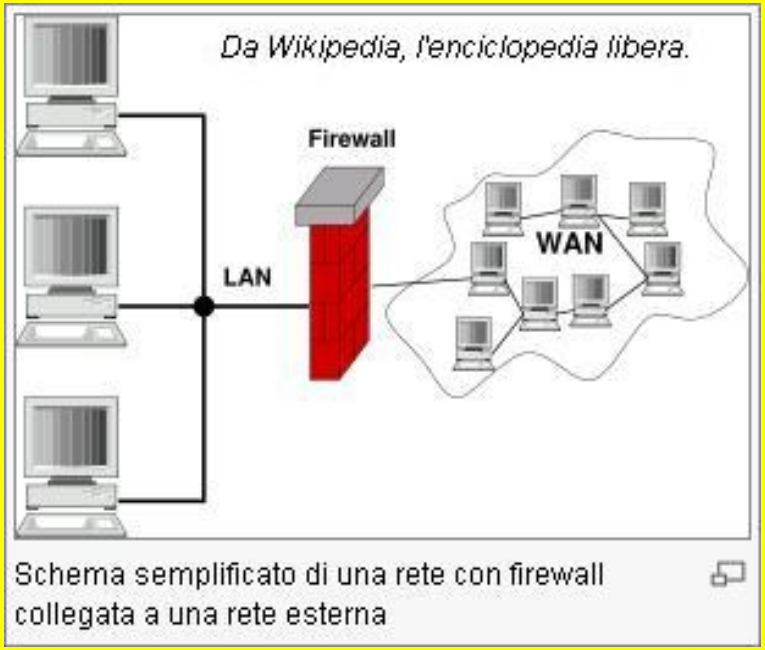
SICUREZZA DELL'AMBIENTE DI LAVORO

SOFTWARE PER LA SICUREZZA

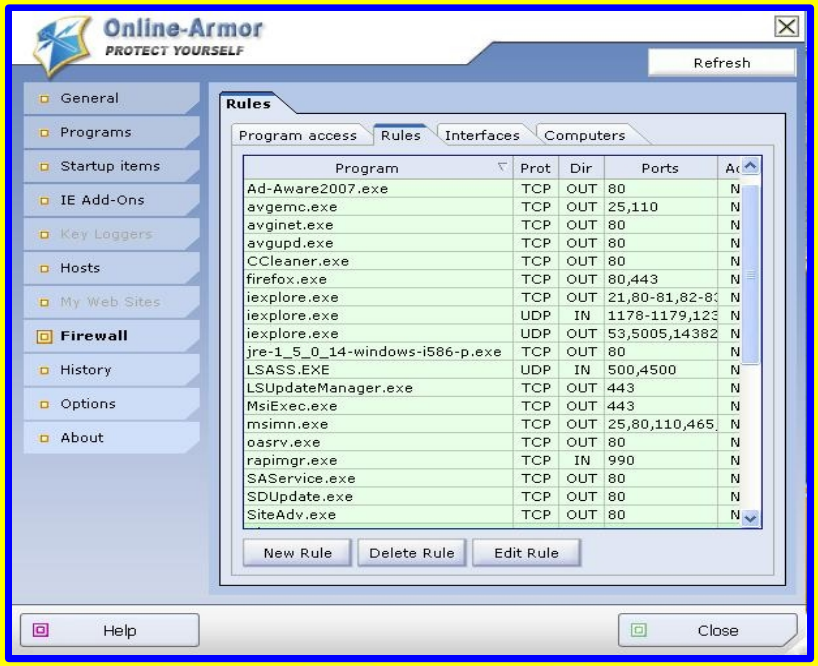
FIREWALL

Apparato di rete hardware o software che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa.

FIREWALL PERIMETRALE



PERSONAL FIREWALL

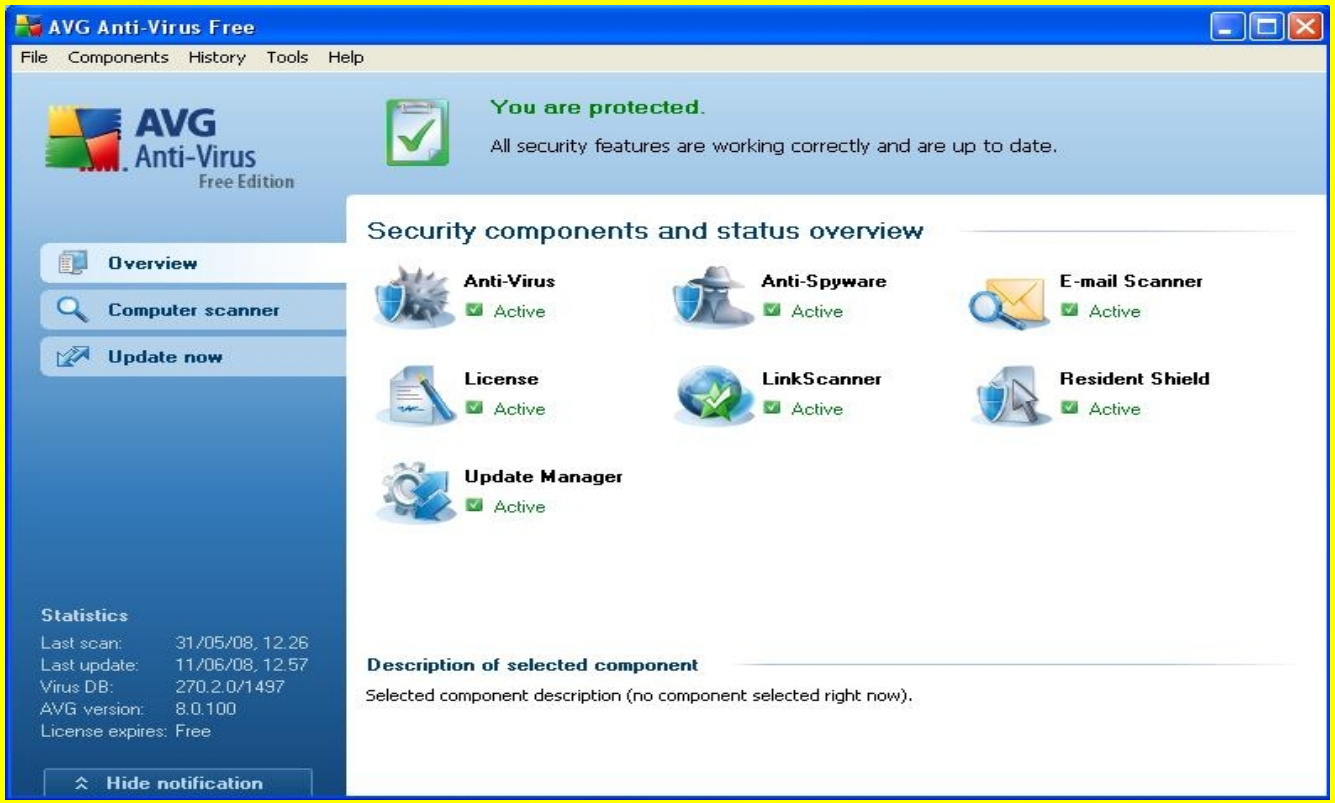


SICUREZZA DELL'AMBIENTE DI LAVORO

SOFTWARE PER LA SICUREZZA

ANTIVIRUS

Un antivirus è un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi come worm, trojan e dialer.

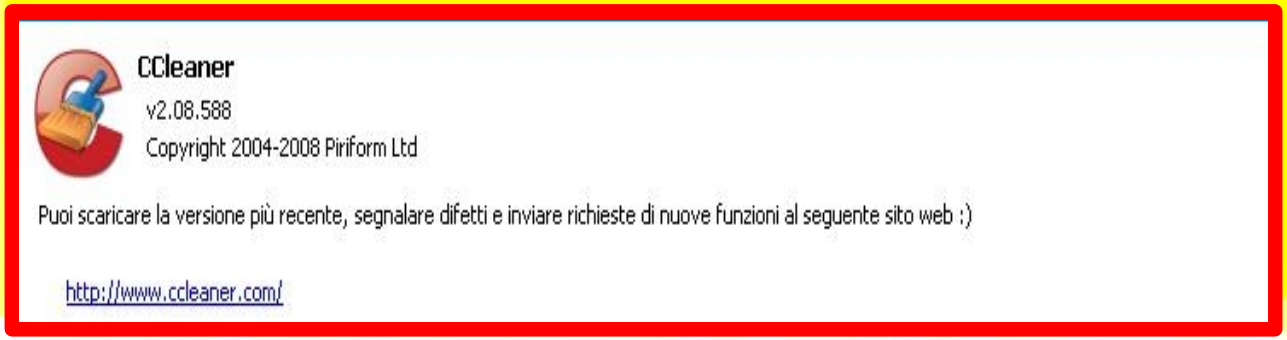


SICUREZZA DELL'AMBIENTE DI LAVORO

SOFTWARE PER LA SICUREZZA

ANTI MALWARE

rimuovono anche i cookies e tutte le liste MRU (Most Recently Used) contenenti dati sugli ultimi file aperti, eseguiti, modificati, sugli URL digitati nel browser e siti visitati

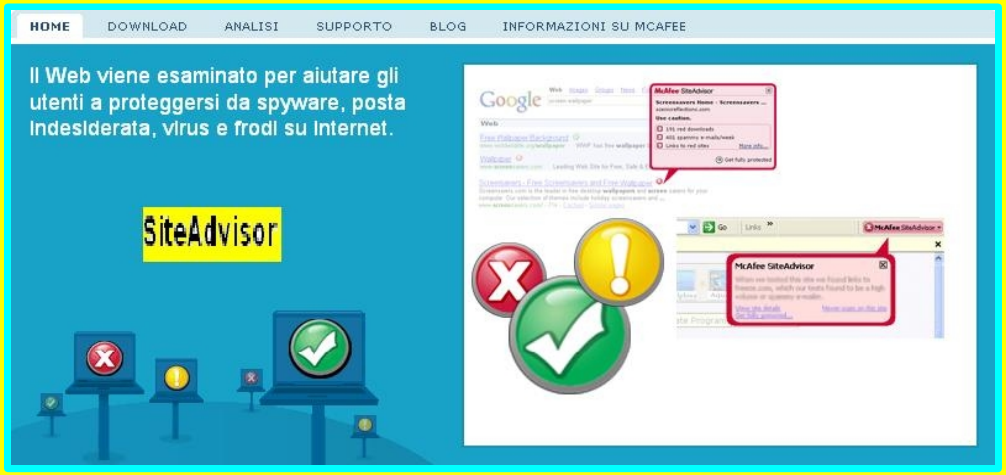


SICUREZZA DELL'AMBIENTE DI LAVORO

SOFTWARE PER LA SICUREZZA

ERASER

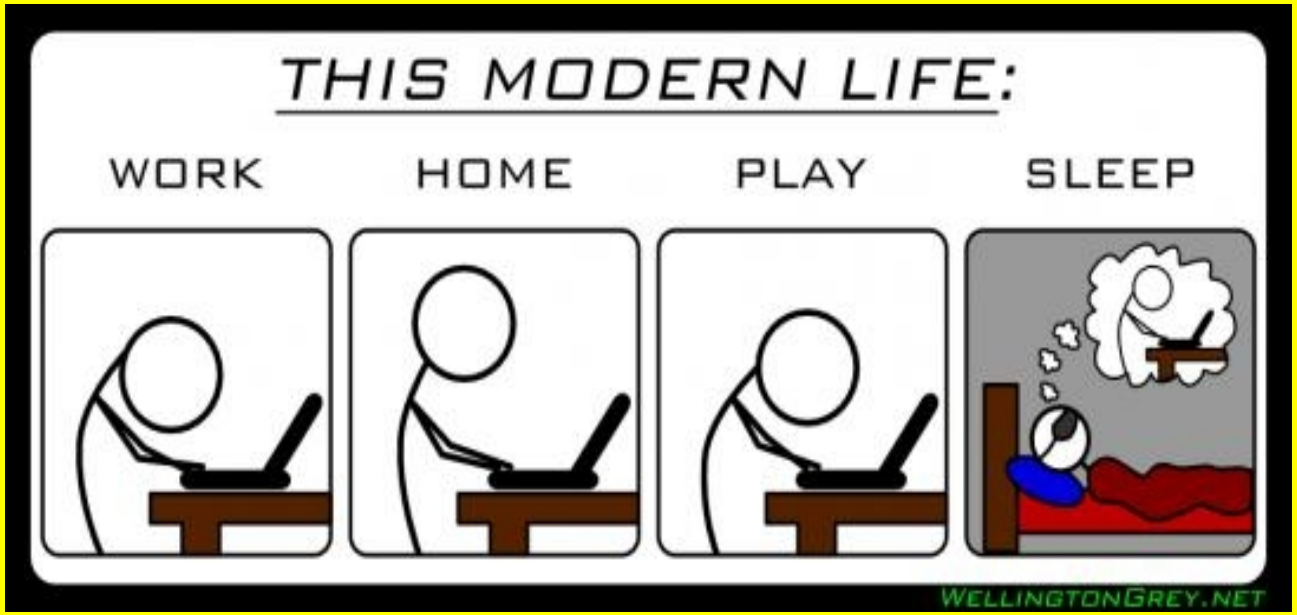
SW PER LA CANCELLAZIONE SICURA DEI FILE



SITEADVISOR

SW UTILE PER NAVIGAZIONE INTERNET (INFORMAZIONI SUI SITI VISITATI E RICERCATI)

ORAMAI SIAMO PERENNEMENTE CONNESSI



LE CONNESSIONI CONTINUE ESPONGONO MAGGIORMENTE I P.C. AGLI ATTACCHI E AI RISCHI PROVENIENTI DALLA RETE INTERNET

SICUREZZA
CONSIGLI PRATICI

- CREATE UN DISCO DI RIPRISTINO PER IL RIAVVIO DEL S.O

- AGGIORNATE GIORNALMENTE TUTTI I SOFTWARE PER LA SICUREZZA (FIREWALL, ANTIVIRUS, ETC.)

- INSTALLATE GLI AGGIORNAMENTI (PATCH) DEL SISTEMA OPERATIVO E DEI SW

- NON INSTALLATE SOFTWARE SUPERFLUO O DI DUBBIA PROVENIENZA

- MODIFICARE SPESSO (MIN. OGNI 3 MESI) TUTTE LE PSW UTILIZZATE

- FATE IL BACKUP (SETTIMANALE) DEI DATI SU SUPPORTI ESTERNI (CD, DVD, HD REMOVIBILI) E CREATE UN DISCO PER IL DISASTER RECOVERY

- PROTEGGETE I DATI SALVATI SU SUPPORTI ESTERNI (PENNE USB, HD EXT.) PER IL CASO DI SMARRIMENTO DEL SUPPORTO

- CANCELLATE IN MODO SICURO I DATI DA ELIMINARE (ERASER, WIPE)

- NON FIDATEVI DEI LINK PRESENTI NEI MESSAGGI DI POSTA ELETTRONICA

- ATTENZIONE AD APRIRE GLI ALLEGATI NON ATTESI, DI QUALUNQUE TIPO, GIUNTI PER MAIL

SICUREZZA

CONSIGLI PRATICI

- VIETARE ASSOLUTAMENTE L'INSTALLAZIONE SUI P.C. DELLO STUDIO DI SOFTWARE PER IL P2P

Per peer-to-peer (o P2P) si intende una rete che non possiede nodi gerarchizzati come client o server fissi (clienti e serventi), ma un numero di nodi equivalenti (pari, in inglese peer appunto).

L'esempio classico di rete P2P è la rete per la condivisione di file (File sharing).

Per la stessa filosofia del P2P quasi tutti i programmi di file-sharing richiedono di avere sul proprio p.c. dei file condivisi che possano quindi essere a disposizione degli utenti che ne fanno richiesta.

Questo implica da un lato la condivisione di un'area del disco sulla quale mettere i file a disposizione, dall'altro consentire il libero accesso ad alcune porte del computer con conseguente esposizione del p.c. stesso e dei dati in esso contenuti a gravi rischi di sicurezza e violazione della privacy.

SICUREZZA DEI DATI DELLO STUDIO

LINK PER IL DOWNLOAD DEI SOFTWARE

(link verificati il 17/12/2009)

Online Armor Personal Firewall Free edition
http://ita.tallemu.com/downloads.html

AVG Anti-Virus Free Edition Ver. 8.0 (Freeware)
http://free.avg.com/it-it/download-avg-anti-virus-free-edition

Sandboxie version 3.42
http://www.sandboxie.com/

Spybot - Search & Destroy Ver. 1.5.2 (Free Open-Source)
http://www.spybot.info/

CCleaner Ver. 2.08.588 (Freeware)
http://www.ccleaner.com/

Ad-Aware (Freeware)
http://www.lavasoft.com/products/ad_aware_free.php

SpywareBlaster (Freeware)
http://www.javacoolsoftware.com/sbdownload.html

Eraser 5.86 (Freeware)
http://eraser.heidi.ie/download.php

TrueCrypt Ver. 5.1a (Free Open-Source)
http://www.truecrypt.org/downloads.php

SICUREZZA DEI DATI DELLO STUDIO

LETTURE E AUDIO/VIDEO UTILI

"Sicurezza Informatica per il Cittadino" di CASPUR e Univ. Roma
http://sicurezzacittadino.caspur.it/

Bollettini di Sicurezza Informatica dello Stato Maggiore della Difesa
http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CERT/bollettini-sicurezza-informatica/

Sicurezza informatica dal sito CNIPA
http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Sicurezza_informatica/

Libro Windows XP in sicurezza di Mario Pascucci. Apogeo
http://www.apogeonline.com/2007/libri/88-503-1008-0/ebook/pdf/8850310080_open.pdf

Video dei Convegni di Security Summit
http://roma.securitysummit.it/page/video

Consigli per difendersi dal phishing di G.Costabile – Giuffrè Ed.
http://www.giuffre.it/age_files/aggiornamenti/133947/133947_capitoloVI.pdf

Guida alla sicurezza informatica Pv. Como - PolPost Lombardia
http://www.anpsitalia.eu/portale/images/pdf/sicurezza%20informatica%20completo.pdf

Corso di sicurezza informatica di PcOpen
http://www.pcopen.it/01NET/HP/0,1254,4_ART_61028,00.html

GRAZIE PER L'ATTENZIONE :-/

DOMANDE ?

Avv. Giorgio Battaglini
www.studiobattaglini.eu