

Vademecum Sicurezza e Buon Utilizzo del Computer

N°	Tema	
	Descrizione	Soluzione
1	Sistema Operativo	
	Un Sistema Operativo ha una struttura particolarmente complessa con insita una certa vulnerabilità; quando le "falle" vengono scoperte il produttore mette a disposizione delle "patch" che correggono gli errori	<ul style="list-style-type: none"> • configurare MS Update per ricevere aggiornamenti automatici oppure aggiornare manualmente con frequenza settimanale • configurare i servizi di rete, i protocolli e le condivisioni in modo da limitare i tentativi di intrusione
2	Politica accessi e definizione password	
	E' insensato dotarsi di sistemi di sicurezza e poi lasciare che chiunque possa accedere al nostro computer o alla nostra rete	<ul style="list-style-type: none"> • non lasciare il proprio computer incustodito senza aver prima sospeso la sessione di lavoro • configurare sempre lo screen-saver con un tempo breve e con l'opzione di protezione attivata • non concedere l'utilizzo del proprio computer con la propria password ad altre persone • introdurre regole di definizione e di utilizzo delle password tali da garantire un accesso controllato e sicuro al sistema ed alla rete; non lasciare mai le password di default, utilizzare password con almeno 8 caratteri utilizzando lettere e numeri, non usare mai nomi prevedibili come nomi di familiari, animali domestici, date di nascita o parole presenti nei dizionari • rimuovere gli utenti non attivi • se possibile utilizzare dispositivi di accesso biometrici (impronte digitali, ...)
3	Uso e conservazione delle password	
	Un utilizzo diversificato del computer comporta l'archiviazione e l'uso di molteplici user e password; non è infrequente trovare sui PC etichette adesive con la password di accesso o fogli sulla scrivania con l'elenco di tutte le credenziali di collegamento ai vari servizi	<ul style="list-style-type: none"> • non comunicare a nessuno le proprie password • non scrivere le password in luoghi accessibili ad altri • evitare di introdurre password mentre altri vi osservano • non accedere mai a servizi bancari o finanziari da PC pubblici (Internet Café) o tramite reti wireless non sicure

		<ul style="list-style-type: none"> evitare di inserire password da tastiera ed affidarsi a programmi che si occupano di farlo per voi utilizzare user e password diversificate per i diversi servizi utilizzare software specifici per l'archiviazione e l'uso di tutte le password consigliato AI Roboform
4	Antivirus	
	<p>Quotidianamente nascono nuovi programmi maligni con la capacità di inserirsi nel vostro PC ed in grado di autoreplicarsi nel vostro sistema e nei sistemi con i quali entrate in contatto</p>	<ul style="list-style-type: none"> installare un buon antivirus con scansione realtime ed impostare l'aggiornamento automatico oppure aggiornare manualmente con frequenza almeno bisettimanale prevedere una scansione completa del sistema settimanale consigliato NOD32 (a pagamento)
5	Antispyware	
	<p>Quotidianamente nascono nuovi programmi maligni con la capacità di inserirsi nel vostro PC con la missione di trafugarvi codici e password, di veicolare la vostra navigazione su siti a pagamento, di leggere le vostre tracce di navigazione per inviarvi posta indesiderata, di veicolare altro codice ostile ecc.</p>	<ul style="list-style-type: none"> se la soluzione antivirus non lo prevede o non è particolarmente efficace installare un buon antispyware con scansione realtime ed impostare l'aggiornamento automatico oppure aggiornare manualmente con frequenza almeno bisettimanale prevedere una scansione settimanale completa del sistema consigliato SpyBot Search & Destroy (free)
6	Firewall	
	<p>In Internet sono costantemente presenti individui o programmi automatici che scandagliano la rete alla ricerca di PC con possibilità di accesso in modo da veicolare programmi ostili all'interno del vostro computer o trafugare informazioni; è necessario chiudere tutte le porte agli sconosciuti</p>	<ul style="list-style-type: none"> utilizzare un buon prodotto hardware (i moderni router ADSL prevedono tale funzionalità e sono sufficienti per un utilizzo home / small office) in mancanza di un dispositivo hardware è fortemente consigliato dotarsi di un buon Firewall software e configurare attentamente le porte ed i servizi attivi consigliati Agnitum Outpost (a pagamento) o Zone Alarm (free)
7	Browser	
	<p>è il programma che utilizzate per navigare in Internet dove sono nascoste le principali insidie per la vostra sicurezza; più è insicuro maggiori sono le possibilità di contaminazione</p>	<ul style="list-style-type: none"> utilizzare un browser diverso da Internet Explorer; se ciò non è possibile utilizzare la versione più aggiornata consigliato FireFox (free)

8	Pop-Up	
	<p>Durante la navigazione non è rara l'apertura automatica di finestre non richieste che spesso conducono a contenuti non desiderati o a pagamento</p>	<ul style="list-style-type: none"> • installare una funzionalità di blocco Pop-Up • Internet Explorer 7 include uno strumento di blocco dei pop-up ma consigliamo comunque la barra di Google che aggiunge altre utili funzionalità (free)
9	Configurazione Browser	
	<p>Non è importante solo scegliere il browser ma è altrettanto importante configurarlo in modo da ridurre le probabilità di subire un'aggressione</p>	<ul style="list-style-type: none"> • configurare le impostazioni avanzate del browser in modo da ridurre al minimo la possibilità di inviare dati personali e scaricare componenti indesiderati
10	Navigazione in Internet	
	<p>In rete si nascondono le maggiori insidie per la vostra sicurezza; un comportamento attento e consapevole contribuisce in modo sostanziale a tenervi alla larga dai guai</p>	<ul style="list-style-type: none"> • navigate in modo sicuro; evitate i siti con contenuti per adulti o illegali, attenzione ai siti con contenuti multimediali come musica, video e suonerie • attenzione all'utilizzo di servizi di condivisione (file-sharing o peer to peer); spesso ai file scaricati vengono "incorporati" software di spyware. Sottoporre i file al controllo antivirus prima di utilizzarli • leggete sempre con attenzione e fino in fondo le licenze e le informazioni sulla privacy quando visitate nuovi siti o scaricate programmi; spesso l'uso di spyware è dichiarato in modo esplicito • scaricate i programmi ed i contenuti preferibilmente dai siti ufficiali dei produttori o da fonti rinomate • quando compaiono finestre di Pop-Up indesiderate non chiudetele utilizzando i pulsanti o i link predisposti ma terminatele premendo la "X" in alto a destra o utilizzando la combinazione ALT+F4 • utilizzate prudenza e buon senso • consigliato McAfee SiteAdvisor per le ricerche con Google (free)
11	Gestione Posta Elettronica	
	<p>E' il programma che utilizzate per leggere ed inviare e-mail; molti programmi ostili sono veicolati tramite posta elettronica, più è insicuro il programma maggiori sono le possibilità di</p>	<ul style="list-style-type: none"> • per un utilizzo personale senza necessità di leggere la posta off-line utilizzare i servizi di posta via Web (Webmail) • utilizzare un browser diverso da Outlook

	contaminazione	Express <ul style="list-style-type: none"> consigliato Thunderbird (free)
12	Configurazione Posta Elettronica	
	Un'attenta configurazione può aiutare a ridurre i rischi di infezione tramite e-mail	<ul style="list-style-type: none"> se il vostro provider lo prevede utilizzate servizi anti-spam disattivare la funzione di anteprima automatica del gestore di posta configurare le impostazioni avanzate del gestore di posta in modo da ridurre al minimo la possibilità scaricare componenti indesiderati
13	Comportamenti nella lettura della posta	
	Una buona parte delle minacce alla vostra sicurezza arriva con la posta elettronica sottoforma di allegati o link	<ul style="list-style-type: none"> evitare accuratamente di aprire posta con mittente sconosciuto, a maggior ragione se il messaggio contiene allegati se il messaggio proviene da un vostro corrispondente ma ha caratteristiche o contenuti strani non esitate a contattare la fonte prima di aprirlo non rispondere per nessun motivo a chi vi chiede di comunicare il vostro utente e la vostra password anche se il messaggio sembra provenire da un istituto bancario, un servizio finanziario o da un organizzazione seria; contattare la fonte prima di aprire il messaggio
14	Instant Messaging	
	Sono ora molto diffuse le applicazioni per "chattare" on line con i propri amici o conoscenti; purtroppo i criteri di sicurezza presenti in questi programmi (Messenger è il più utilizzato) sono blandi e l'uso disattento può comportare rischi per la sicurezza.	<ul style="list-style-type: none"> non includete nel vostro nick name informazioni che permettano di risalire a vostre informazioni personali (nome, cognome, soprannome, sesso, data o anno di nascita, religione, fede politica, ecc.) limitate la diffusione del vostro identificativo ai vostri corrispondenti e non aggiungetelo a community on line; il collegamento tra il vostro nick name ed il vostro indirizzo di posta vi rende più vulnerabili a fenomeni come lo spamming ed il phishing durante le conversazioni non indicate mai dati personali o informazioni come password, numeri di carte di credito ecc.. comunicare solo con i soggetti presenti nel vostro elenco contatti non aprite mai immagini, collegamenti o allegati a messaggi provenienti da persone non conosciute; aprite gli allegati o i link solo se siete

		<p>preventivamente informati del loro contenuto</p> <ul style="list-style-type: none"> • se utilizzate PC in locali pubblici non attivate le funzioni di logon automatico; chi utilizzerà il computer dopo di voi potrebbe venire in possesso delle vostre informazioni • quando vi mettete off-line non specificate il motivo o la durata della vostra assenza, qualcuno potrebbe utilizzare l'informazione a vostro danno
15	Backup	
	Quando tutti gli accorgimenti sopra descritti non sono stati sufficienti per salvaguardare i vostri dati, l'ultima ciambella di salvataggio è rappresentata dalla copia di sicurezza dei vostri archivi	<ul style="list-style-type: none"> • installare una soluzione di backup adeguata alle caratteristiche del sistema e dell'organizzazione • configurare i salvataggi automatici giornalieri • posizionare i supporti di salvataggio in un luogo sicuro e diverso da quello in cui si trovano i dati • prevedere e testare soluzioni di ripristino (disaster recovery)
16	Controllo anti-intrusione	
		<ul style="list-style-type: none"> • al termine dell'installazione e della configurazione dei componenti sopra descritti eseguire qualche utility per l'analisi della vulnerabilità del sistema e della rete
17	Aggiornamento applicazioni	
	Anche i programmi utilizzati possono contenere delle "falle" che agevolano l'ingresso di software maligno nel vostro sistema	<ul style="list-style-type: none"> • verificate regolarmente il software utilizzato per garantirvi i più recenti aggiornamenti di sicurezza
18	Manutenzione software del computer	
	Alcuni semplici accorgimenti possono rallentare il progressivo degrado delle prestazioni del vostro PC	<ul style="list-style-type: none"> • cancellate periodicamente le tracce di navigazione ed i file temporanei utilizzati per le installazioni di nuovi programmi o componenti • utilizzate periodicamente utilità di deframmentazione per mantenere le prestazioni dei dischi rigidi • consigliati CCleaner (free) e Diskeeper (a pagamento)
19	Manutenzione hardware del computer	
	Il PC ha bisogno di elettricità per funzionare e di	<ul style="list-style-type: none"> • dotarsi di un buon gruppo di continuità

<p>aria per raffreddarsi; le componenti elettroniche dei Computer sono sensibili agli sbalzi di tensione ed alle alte temperature</p>	<p>(UPS) che oltre a permettervi di spegnere in modo controllato il PC in caso di black-out preserva il sistema da sbalzi di tensione e prolunga la vita dei componenti elettronici</p> <ul style="list-style-type: none">• assicurate al PC un'adeguata ventilazione con componenti di qualità ed assicurando un flusso d'aria libero da ostacoli (polvere, griglie e filtri sporchi, ecc.)
<p>20 Aiuto</p>	
<p>Nonostante questi buoni consigli può capitare di aver bisogno dell'aiuto di esperti per risolvere problemi più complessi</p>	<ul style="list-style-type: none">• affidatevi a professionisti dalla comprovata esperienza e capacità; affidarsi a "guru" improvvisati spesso non porta a risultati soddisfacenti