

Decalogo per utenti consumer

1. **Gli strumenti tecnologici indispensabili.** Installare un software antivirus di una azienda produttrice nota, utilizzandolo e aggiornandolo regolarmente. Un antivirus non aggiornato da diverso tempo non garantisce una protezione contro i nuovi virus. A questo proposito si consiglia di configurare il software antivirus in maniera tale che si aggiorni automaticamente. Oltre all'antivirus è necessario disporre di un firewall e di soluzioni antispware e antispam, o, in alternativa, installare un pacchetto software completo che integri tutte queste funzioni come Trend Micro Internet Security. Se si desidera controllare il proprio pc con un programma antivirus gratuito si può utilizzare un servizio di scansione come Trend Micro HouseCall. Sul sito www.trendsecure.com sono disponibili altri strumenti gratuiti come HijackThis, un tool per la rimozione dei programmi spyware e TrendProtect, un plug-in per il browser che offre un servizio di verifica della reputazione dei siti Web e filtraggio degli URL.
2. **Non accettare qualsiasi programma.** Verificare ogni nuovo programma o file che può contenere codice eseguibile prima di eseguirli o aprirli, da qualunque parte essi arrivino (email, Internet...). Bisogna stare molto attenti ad aprire file di testo e documenti di Word o Excel provenienti da fonti sconosciute, in quanto possono contenere pericolosi Trojan horse. Prestare molta attenzione inoltre nell'accettare programmi o file durante le sessioni di chat, che sembrano essere diventate uno dei principali veicoli di infezione.
3. **Attenzione a spam e phishing.** Sospettare dei messaggi di posta elettronica inattesi e insoliti, indipendentemente dal mittente. Non aprire un allegato o fare click su link contenuti in tali messaggi e non rispondere mai a email che richiedono di verificare o inserire informazioni personali (es: numero di carta di credito o ID/password per l'accesso al proprio conto corrente online). Diffidare anche delle email che invitano a cliccare su link per cancellare la propria registrazione e non ricevere più messaggi quel mittente.
4. **Sistema operativo aggiornato.** Mantenere sempre aggiornato il sistema operativo e il software applicativo aggiornandoli con le patch più recenti. (Attivare la funzione "Automatic update" di Windows). Prestare la massima attenzione al funzionamento anomalo del sistema operativo e cercare di individuare le cause anche con l'uso di strumenti specifici.
5. **Disabilitare Java, JavaScript ed ActiveX.** Se il software di posta elettronica ha la capacità di eseguire automaticamente JavaScript, ActiveX, macro di Word o altro codice eseguibile contenuto o allegato a un messaggio, disabilitare questa funzione.
6. **Back up dei dati.** Fare il back up dei dati regolarmente e custodire le copie in luoghi sicuri. L'ideale sarebbe fare il back di tutto il sistema e, se questo non fosse possibile, fare le copie dei file più importanti.
7. **Proteggere la rete wireless.** Se si utilizza una rete Wi-fi, non trascurare di proteggerla dall'accesso di estranei. Alcune suite di sicurezza come Trend Micro Internet Security comprendono anche questa funzione specifica.
8. **Dati personali al sicuro.** Non archiviare i dati personali, informazioni su conti correnti online o password sul proprio pc.
9. **Lucchetto di sicurezza sul browser.** Accertarsi che il sito di e-commerce sul quale si intende effettuare acquisti utilizzi un metodo di pagamento sicuro. Verificare la presenza sul browser dell'icona con un lucchetto prima di inserire i propri dati bancari.
10. **L'educazione alla sicurezza prima di tutto.** Ricordarsi che non basta acquistare un antivirus o un firewall per risolvere tutti i problemi di sicurezza: occorre anche assumere comportamenti prudenti, ad esempio, evitando di diffondere informazioni di carattere riservato o di navigare su siti poco affidabili.