

## Decalogo per navigare in sicurezza

Decalogo della sicurezza online

Ogni giorno sentiamo di nuove [minacce](#) informatiche a causa delle quali è possibile restare vittima di furti di dati sensibili, come numeri di carta di credito, credenziali per l'accesso a siti di online banking e così via oppure cadere in trappole tessute per spillarci denaro in maniera fraudolenta. I computer che utilizziamo, i software di navigazione quali Internet Explorer, Firefox, Chrome ed Opera ed i comportamenti che adottiamo spesso non sono consoni a tenerci al riparo da queste spiacevoli situazioni. Ecco perché abbiamo deciso di stilare un elenco di dieci regole miranti a sensibilizzare il "cittadino del web" sui corretti comportamenti da tenere durante la navigazione.

---

**1. Installare sul proprio PC e mantenere aggiornato un software antivirus.**

Potete sceglierne anche uno gratuito come Avast o Avira, oppure rivolgervi alle offerte a pagamento che tutto sommato costano cifre più che accessibili. Il migliore al momento sembra essere l'antivirus proposto dalla tedesca G DATA ma vanno bene anche i prodotti di Kaspersky, McAfee o [Norton](#). Vi raccomandiamo di tenere l'antivirus sempre aggiornato, magari lasciando che il software scarichi automatiche le nuove firme ed gli upgrade del motore. Vi consigliamo altresì di non farvi prendere dal panico installando più software antivirus sullo stesso sistema: uno è più che sufficiente!

---

**2. Mantenere sempre aggiornato il sistema operativo.**

Sia che siate fan di Microsoft, sia che abbiate votato la vostra vita all'open source e ai sistemi operativi del pinguino o ancora a quelli della mela, l'imperativo è "Aggiorna!". Un sistema operativo sempre aggiornato, ma lo stesso vale anche per qualunque altro software, permette di evitare che qualche malintenzionato possa introdursi nel vostro sistema a vostra insaputa per farne ciò che vuole.

**3. Evita di disattivare il [firewall](#) e gli altri tool installati nel sistema operativo se non sei cosciente di ciò che stai facendo.**

Oggi non solo Windows, ma anche gli altri sistemi operativi, sono dotati di alcuni componenti che permettono di evitare accessi indesiderati. Fra questi i software di firewall, come quello integrato in Windows XP dal Service Pack 2 in poi, o Windows Defender presente in Windows Vista. Se non siete esperti e non sapete cosa state facendo evitate di disattivarli e mantenetele sempre aggiornati (di default l'aggiornamento avviene automaticamente) in quanto essi possono darvi comunque una mano.

---

**4. Non salvare mai le password importanti sul browser.**

Oggi tutti i browser, Internet Explorer, Firefox, Chrome e Opera, tanto per citare i più noti, offrono la possibilità di salvare nome utente e password dei siti visitati in modo da non doverle ridigitare quando si torna nuovamente sul sito. Opzione sicuramente molto comoda ma assolutamente non sicura! Se volete salvare le password poco importanti fate pure, ma evitate di salvare quelle relative al vostro servizio di online banking, del conto corrente postale, di eBay e così via.

**5. Evita di utilizzare password troppo facili da indovinare.**

Non è mai buona norma usare una password uguale alla username oppure che riguardi informazioni personali e nomi di personaggi famosi. In generale è buona norma invece utilizzare delle password composte da lettere, numeri e simboli. E come è possibile ricordarle? Potreste per esempio ricavarle da una canzone o da un proverbio. Ad esempio se prendete il detto "Tanto va la gatta al lardo che ci lascia lo zampino", potreste ricavare una password dalle sue iniziali: Tvlgalcellz.

**6. Evita di scaricare gli allegati delle email sospette e se potete usate solo client online.**

Ogni giorno arrivano nella propria casella di posta elettronica numerosi messaggi. Quelli che realmente sono interessanti restano però molto pochi. Gli altri sono tipicamente pubblicità indesiderate (spam), messaggi fasulli che si spacciano come provenienti da servizi noti ([phishing](#)) o messaggi con [malware](#) in allegato. Discernere fra "buoni e cattivi" purtroppo

---

non è così facile soprattutto per i meno esperti, ma anche qui una buona dose di buon senso potrebbe aiutare. Anzitutto guardate come il messaggio è scritto: spesso quelli contenenti virus e quelli di phishing (vedi punto 5) sono scritti in inglese oppure con un italiano davvero penoso. Il mittente potrebbe anche non essere indicativo ma solitamente quelli che arrivano da sconosciuti nel 99% dei casi sono malevoli mentre per quelli che arrivano da utenti conosciuti è meglio controllare. L'allegato sospetto non va mai aperto: se proprio siete certi del chi e del cosa, controllatelo prima con un software antivirus.

7. **Non seguire MAI le istruzioni riportate nelle email che chiedono di inserire i propri dati sensibili (nome utente, password, numero di carta di credito) su qualche sito web.**  
Avete un servizio di banca online e vi arriva una email da quella banca che vi chiede di inserire i vostri dati come username e password o il numero di carta di credito in una pagina linkata in fondo al messaggio che assomiglia in tutto e per tutto al sito della vostra banca. Questa è una delle truffe online che oggi va per la maggiore. Evitate questi messaggi come la peste, cestinateli subito! Se avete qualche dubbio contattate voi stessi la vostra banca la quale non vi invierebbe mai un messaggio per chiedervi i dati di accesso. Inoltre guardate sempre l'indirizzo del sito web sulla barra delle applicazioni: quelli che implicano transazioni di denaro sono sempre basati su protocollo sicuro che inizia per "https://" e non "http://".
8. **Evitare di cliccare sui link sospetti inviati anche da contatti facenti parte della propria lista dei contatti di Messenger o altri Instant Messaging.**  
Può accadere che utilizzando MSN Messenger o qualche altro tool di messaggistica istantanea, ci si veda recapitati messaggi strani, magari scritti in inglese da contatti che non abbiamo mai conosciuto ma anche da contatti che fanno parte della nostra lista di amici. Ebbene, nella maggior parte dei casi si tratta di messaggi che in qualche modo vi stanno imbrogliando offrendovi link da cliccare o indicazioni su siti da visitare. Evitateli oppure controllate direttamente con il vostro amico rendendovi voi parte attiva: scrivetegli e chiedete se è stato davvero lui a mandarvi il messaggio.

---

9. **Evitare di scaricare applicazioni di provenienza dubbia in quanto nel 90% dei casi esse possono contenere software malevolo.**  
Installare qualunque tipo di software sul proprio computer è una operazione da evitare sempre e comunque, ma ci rendiamo anche conto che soprattutto chi utilizza da poco un PC è molto curioso e desidera provare tutto ciò che c'è da provare. Quando scaricate del software dal Web, però, state attenti alla loro provenienza: siate certi che il sito da cui lo state prendendo sia riconosciuto ed affidabile, fate ricerche ulteriori se non siete certi di cosa state per installare nel sistema o magari chiedete al vostro amico esperto. Eviterete in questo modo di installare nel sistema software malevoli che possono spiarvi, rubare i vostri dati e causare dei danni al sistema.
10. **Usare il buonsenso non solo quando si è sulla "terraferma" ma anche su Internet.**  
Spesso non ci si rende conto che le regole del buonsenso che valgono per la quotidianità, dovrebbero valere anche su Internet. La mamma non vi aveva raccomandati da piccoli che non è buona cosa accettare caramelle dagli sconosciuti? E allora perché i messaggi email o MSN dagli sconosciuti li accettate? Allo stesso modo se qualcuno vi offrisse una grossa somma di denaro ma voi dovrete dargli subito dei soldi per averla, non vi verrebbe il dubbio che forse quel tizio potrebbe essere un truffatore? Se questa cosa ve la proponessero via email occorrerebbe metterci la stessa *malizia*.