

DA PASSWORD AD ANTIVIRUS

Dieci mosse per proteggersi in rete

Un decalogo per affrontare le minacce informatiche. Dopo l'attacco a Unicredit lo ha predisposto Stefano Salvadeo, responsabile "Growth and Advisory Services" di Bernoni Grant Thornton, la divisione italiana del gruppo specializzato nella consulenza tributaria e societaria alle imprese.

● **PASSWORD.** Si parte dalla password, che «deve essere di almeno 8 caratteri, contenenti numeri, caratteri speciali e maiuscolo e minuscole» e va «aggiornata periodicamente». «È assolutamente vietato utilizzare la stessa chiave d'accesso per più siti e portali - sottolinea Salvadeo - e non va condivisa con nessuno, né scritta da qualche parte, nemmeno sul telefono».

● **E-MAIL.** «Ognuno ne riceve, quotidianamente, in numero molto elevato». Quelle che possono contenere

virus o minacce si riconoscono dall'oggetto: «Se non è attinente con le vostre attività - chiarisce il manager - è meglio cestinarle direttamente». Occhio poi «alla forma grammaticale», perché i messaggi più pericolosi vengono inviati «contemporaneamente in più Paesi e chi li spedisce si serve di traduttori automatici». Diffidare anche quando il mittente «sembra una persona conosciuta».

● **FILE SOSPETTI.** Evitare di «lanciare file eseguibili dei quali non si è assolutamente certi dell'affidabilità».

● **NAVIGAZIONE SU WEB.** Occorre «navigare su internet in modo sicuro», facendo attenzione ai contenuti e al certificato dei siti, che non deve essere scaduto.

● **SMARTPHONE E CHIAVETTE.** Fare attenzione a smartphone e chiavette Usb,

che «possono essere portatori di virus».

● **AGGIORNAMENTO SISTEMA OPERATIVO.** Sui Pc bisogna «aggiornare il sistema operativo per tempo».

● **ANTIVIRUS.** Necessario anche aggiornare l'antivirus, che «non è un optional».

● **BACK-UP.** È sempre utile copiare i dati per creare un backup da utilizzare in caso di 'infezione del computer.

● **RIAVVIARE NON SERVE.** In caso di Pc infettato, «spegnere e riaccendere non è la soluzione».

● **DOPPIO UTENTE.** Una buona prevenzione dagli attacchi informatici consiste nel «creare due utenti» con «compiti e privilegi diversi», mentre per le reti occorre farlo con le modalità d'accesso ai singoli dischi.

