GAZZETTA DI PARMA

L'ESPERTO LE REGOLE DI GRANT THORTON PER PROTEGGERSI IN RETE

Che fare? Ecco il decalogo contro i «pirati»

Dalla password all'antivirus, i consigli per proteggersi dalle minacce informatiche

Paolo Verdura

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 Thorton, divisione italiana del gruppo specializzato nella consulenza tributaria e societaria alle imprese.

1. PASSWORD Si parte dalla password, che «deve essere di almeno 8 caratteri, contenenti numeri, caratteri speciali e maiuscolo e minuscole» e va «aggiornata periodicamente». «E' 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».

2. 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».

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

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

5. SMARTPHONE E CHIAVETTE Fare attenzione a smartphone e chiavette Usb, che «possono essere portatori di virus».

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

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

8. BACK-UP E' sempre utile copiare i dati per creare un backup da utilizzare in caso di 'infezionè del computer.

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

10. 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. ◆


Primo piano

Banche, la vita al tempo degli hacker

Che fare? Ecco il decalogo contro i «pirati»

La giornata

Camera, primo stop ai vitalizi
Scontro tra Pd e M5s in aula

Costa Azzurra, l'Onda nascosta