2 – Monitorare con antivirus e firewall

Quali «porte d'accesso» sono aperte sul vostro dispositivo e quali virus vi possono arrivare? Praticamente nessuno, se avete attivato un firewall e installato un programma antivirus.

Punti principali:

- Utilizzate un programma antivirus e attivate l'aggiornamento automatico.
- Eseguite regolarmente un controllo completo del sistema per identificare eventuale malware.
- Attivate il firewall integrato di Windows o macOS prima di collegare il vostro dispositivo a Internet o a un'altra rete.

2 – Monitorare con antivirus e firewall

5 operazioni per la vostra sicurezza digitale

Tutto sotto controllo grazie al quadro strumenti!
Antivirus e **firewall** per monitorare il traffico dati!

eBanking ma sicuro! www.ebas.ch

Ecco come fare

Utilizzate un programma antivirus e un firewall che si aggiornano sempre automaticamente, in modo da essere protetti anche dai pericoli più recenti.

Windows

Windows 11 viene installato con un firewall attivo come impostazione predefinita e con il programma antivirus «Windows Defender». In questo modo godete di una protezione ottimale.

Per funzioni di protezione supplementari, come ad esempio un filtro per la protezione dei minori ecc., si possono utilizzare anche i prodotti seguenti, alcuni dei quali sono gratuiti (l'elenco non è esaustivo):

- AVG Free Anti-Virus (https://free.avg.com)
- Avira Free Antivirus (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- F-Secure (https://www.f-secure.com)

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica

- G Data (https://www.gdata.de)
- Malwarebytes (https://www.malwarebytes.com)
- McAfee (https://www.mcafee.com)
- Norton (https://ch.norton.com)
- Panda (https://www.pandasecurity.com)
- Sophos (https://www.sophos.com/it-it)
- Trend Micro (https://www.trendmicro.com)

macOS

In macOS non dimenticate di attivare il firewall, che è integrato ma per impostazione predefinita disattivo. Fate quindi clic nel menu «Apple» sulla voce «Impostazioni di Sistema...». In «Rete» nella scheda «Firewall» potete attivare il firewall, che rimarrà in funzione anche in seguito al riavvio.

macOS dispone anche di un meccanismo integrato di protezione volto a prevenire le infezioni da malware. Il software «Gatekeeper», attivo per impostazione predefinita, protegge inoltre dall'installazione involontaria di software dannoso.

Una protezione aggiuntiva si può ottenere con programmi antivirus specializzati. Possiamo raccomandare i seguenti programmi, alcuni dei quali gratuiti, che riconoscono anche i virus di Windows (l'elenco non è esaustivo):

- AVG (https://free.avg.com)
- Avira (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- F-Secure (https://www.f-secure.com)
- Norton (https://ch.norton.com)
- Trend Micro (https://www.trendmicro.com)

Smartphone und Tablet

Installare un firewall su uno smartphone o tablet non è facilissimo. Se sui dispositivi Android servono diritti root, infatti, sugli iPhone occorre effettuare un «jailbreak». In entrambi i casi si tratta di procedure che possono danneggiare il dispositivo e disattivare diversi meccanismi di protezione dei sistemi operativi. Inoltre, in molti casi si perdono tutti i diritti di garanzia. Quindi sconsigliamo di procedere in questo modo.

In **Android**, tuttavia, un antivirus andrebbe assolutamente utilizzato. Possiamo consigliare i programmi antivirus seguenti, alcuni dei quali disponibili gratuitamente:

- AhnLab (https://www.ahnlab.com)
- AVG (https://free.avg.com)
- Avira (https://www.avira.com)

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica

- Bitdefender (https://www.bitdefender.de)
- G Data (https://www.gdata.de)
- McAfee (https://www.mcafee.com)
- Norton (https://ch.norton.com)
- Sophos (https://www.sophos.com)
- Trend Micro (https://www.trendmicro.com)

Per i **dispositivi iOS** come gli iPhone o gli iPad non sono per ora disponibili programmi antivirus nel vero senso della parola. Questo perché il sistema operativo è chiuso e non dovrebbe consentire l'installazione di app sospette o altro software dannoso, limitando fortemente le autorizzazioni conferite alle app installate. Esistono tuttavia app di sicurezza per dispositivi iOS, anche di noti produttori di programmi antivirus, che offrono funzioni di protezione avanzate come la protezione dell'account, l'anti-phishing o la VPN.

Proteggete i vostri dati e tutti i vostri dispositivi con le «5 operazioni per la vostra sicurezza digitale»:

Fase 1 – Salvare (https://www.ebas.ch/it/1-salvare-i-dati/)

Fase 2 – Monitorare

Fase 3 – Prevenire (https://www.ebas.ch/it/3-prevenire-con-aggiornamenti-software/)

Fase 4 – Proteggere (https://www.ebas.ch/it/4-proteggere-gli-accessi-online/)

Fase 5 – Fare attenzione (https://www.ebas.ch/it/5-fare-attenzione-ed-essere-vigili/)

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica

Maggiori informazioni

Infezione da malware – che cosa bisogna fare?

Se sospettate un'infezione da malware per uno dei vostri dispositivi o se il vostro programma antivirus visualizza un messaggio in questo senso, qui (https://www.ebas.ch/it/infezione-da-malware/) trovate ulteriori informazioni su come procedere.

Firewall?

Quando gli utenti navigano in Internet con il computer, il tablet o lo smartphone, per instaurare la comunicazione si aprono sui dispositivi invisibili «porte d'accesso» (Ports) che li espongono agli attacchi provenienti dalla rete. Una volta installato, il firewall chiude queste porte nella misura necessaria e monitora il traffico dati tra i dispositivi e Internet. Il firewall mostra un avviso quando scopre degli scambi di dati sospetti.

Copyright – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica