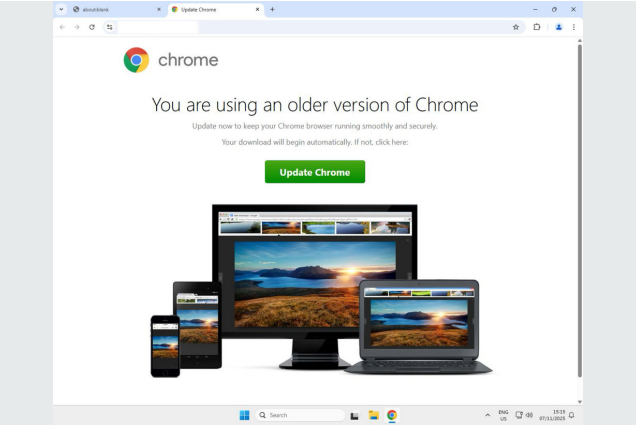
Pas op voor fake updates

UPDATE ALLEEN VIA DE OFFICIELE BRON OF IN DE APPSTORE

Cybercriminelen hebben WordPress websites gehackt en geïnfecteerd met malware. Met deze malware sturen ze u, als websitebezoeker, een fake update. Als u hierop klikt geeft u schadelijke software toegang tot uw computer. Wees alert en controleer updates goed voordat u ze accepteert.



Een groot deel van de websites wereldwijd zijn gemaakt met WordPress. Cybercriminelen hebben WordPress websites gehackt. Hierdoor hebben zij toegang gekregen tot verschillende WordPress websites en deze geïnfecteerd met SocGholish malware. Met deze malware sturen ze u, als websitebezoeker, een fake update.

Als u op deze valse melding klikt, installeert u geen officiële update, maar schadelijke software die criminelen toegang geeft tot uw (computer)systeem en gegevens. Daarom is het extra belangrijk om alert te zijn op fake updates.

Hoe herkent u een fake browser update?

- Vertrouw nooit zomaar pop-ups die opspringen in uw browser.
- Vertrouw updates niet als ze overdreven flashy zijn en schreeuwen om onmiddellijke actie.
- Een echte update komt altijd via de officiële bron, bijvoorbeeld in de systeeminstellingen of in de appstore.
- Zorg voor een up-to-date virusscanner en laat deze ook aanstaan bij installatie van nieuwe software.

Meer informatie

Kijk op politie.nl/Endgame

Politie.nl/Endgame

POL-afqssklui35-nl-NL-0626-2