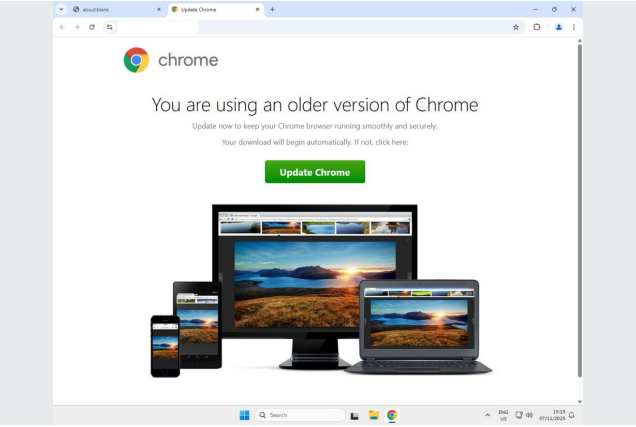
Pas op voor fake updates

EEN ECHTE UPDATE KOMT ALTIJD VIA DE OFFICIËLE BRON

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

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

Hoe herken je een fake browser update?

- Vertrouw nooit zomaar pop-ups die opspringen in jouw 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 je systeeminstellingen of in de appstore.
- Gebruik een betrouwbare ad blocker in je browser. Meer informatie is te vinden op veiliginternetten.nl

Meer informatie

Kijk op politie.nl/Endgame

Politie.nl/Endgame

POL-eftlvwzk9n5-nl-NL-0626-1