computer service heuvelland

Zo beveilig je jouw whatsapp tegen hackers en oplichters!

Hackers hebben een nieuwe methode gevonden om WhatsApp-accounts te kapen. Via de voicemail nemen ze het account over en gebruiken ze jouw WhatsApp-nummer op hun eigen telefoon. Gelukkig kun je een account hiertegen beveiligen middels een paar eenvoudige stappen.

Dat werkt als volgt: om een WhatsApp-account in gebruik te nemen, moet het bedrijf het telefoonnummer bevestigen. Daarvoor stuurt WhatsApp doorgaans een code via sms, maar je kunt deze code ook naar je voicemail laten sturen. Door slecht beveiligde inboxen, bijvoorbeeld met de pincode 0000, kunnen hackers deze code achterhalen en jouw WhatsApp-account kapen. Met de volgende twee manieren voorkom je dat je slachtoffer wordt.

Beveilig je WhatsApp-account met een extra code

Je kunt je WhatsApp-account beveiligen door middel van zogenoemde tweestapsverificatie. Je account maakt daarbij gebruik van een unieke code, die je om de zoveel tijd moet invoeren om te bevestigen dat jij de rechtmatige eigenaar bent. Daarmee kun je dus ook kwaadwillenden buiten houden.

Wanneer jij (of iemand anders) op een smartphone inlogt op jouw WhatsApp-account, moet de tweede pincode, die gekoppeld is aan een e-mailadres, ingevoerd worden. Zo kunnen hackers niet in je account komen, zelfs als ze de verificatiecode uit je voicemail vissen.

Zo stel je tweestapsverificatie op WhatsApp:
Open WhatsApp op een iPhone of Android-smartphone
Ga naar 'Instellingen' en kies voor 'Account'
Ga naar 'Verificatie in twee stappen inschakelen' en stel de code in
De volgende keer dat je wil inloggen op WhatsApp moet je deze zescijferige pincode invoeren en ben je voor zeven dagen ingelogd. Om de zoveel dagen vraagt WhatsApp je de code opnieuw in te voeren. Mocht je de pincode vergeten, dan kun je via het opgegeven e-mailadres een nieuwe code instellen.

Maar het belangrijkst is dat deze pincode altijd gevraagd wordt als je op een nieuw apparaat bij WhatsApp inlogt, want dat is precies wat de hackers proberen te doen. Zonder toegang tot de pincode of je e-mailadres wordt dat onmogelijk.

Gebruik geen 0000 om je voicemail af te luisteren

Ten tweede kun je je voicemail beter beveiligen door een goede beveiligingscode in te stellen. Veel mensen stellen geen unieke beveiligingscode in voor hun voicemail, waardoor hackers met een standaard code als 0000 of 1234 eenvoudig kunnen inloggen.

Het instellen van een beveiligingscode voor je voicemail werkt anders bij de verschillende providers. We zetten voor de grote providers op een rij hoe je dit doet.

Zo stel je bij de grote providers een beveiligingscode voor je voicemail in:

KPN: Bel naar 1233 en toets 2 voor instellingen en optie 1 om de toegangscode te wijzigen.
T-Mobile: Bel 1233 en kies 9 voor mailboxinstellingen. Toets vervolgens 2 voor instellingen en nogmaals 2 voor wachtwoord. Voer een nieuwe code in.
Tele2: Bel naar 1233 en kies 4 in het hoofdmenu. Je kunt dan de standaard pincode vervangen met een eigen unieke code.
Vodafone: Bel 1233 en toets 11 voor het hoofdmenu. Kies vervolgens 2 voor persoonlijke instellingen en daarna 3 voor het instellen voor een pincode.

Overleven na Windows 7: zeven vragen nu de Microsoft ondersteuning stopt.

Microsoft stopt definitief met de ondersteuning voor Windows 7. Consumenten, bedrijven en organisaties kunnen in principe geen updates voor het besturingssysteem meer ontvangen.

Waarom stopt Microsoft met Windows 7?

Simpel: wat in 2009 fonkelnieuw was, is tien jaar later gedateerd. Microsoft heeft intussen twee nieuwe grote versies van zijn besturingssysteem voor pc's en laptops uitgebracht: Windows 8 en Windows 10. Het bedrijf legt op de lange termijn de focus op het laatste besturingssysteem. Oudere versies, waaronder nu dus Windows 7, worden uitgefaseerd.

Ik heb Windows 7 geïnstalleerd. Kan ik nog wel computeren?

Ja, je computer blijft wel nog gewoon werken. Wel moet je het vanaf 14 januari doen zonder beveiligingsupdates. Mochten er in Windows 7 ernstige fouten worden ontdekt, dan lost Microsoft die in principe niet meer op. Daarmee stel je jezelf bloot aan allerlei risico's. Kwaadwillenden die de fouten misbruiken, kunnen mogelijk je gegevens stelen.

Heb ik die updates wel nodig?

Zeker. De regel is: technologie is nooit waterdicht. Ook in nieuwere versies van Windows, en allerlei andere soorten software, worden foutjes ontdekt. Dat gebeurt door de ontwikkelaars van software, onafhankelijke onderzoekers en door (goedaardige of kwaadaardige) hackers.

Als een fabrikant, in dit geval Microsoft, op de hoogte wordt gebracht van die bugs, kan het bedrijf updates uitvoeren om de kwetsbaarheden weg te nemen. Daar stopt Microsoft nu mee. Je pc of laptop is in dat geval dus kwetsbaar voor aanvallen en virussen.

Daarnaast kunnen Windows 7-gebruikers niet langer gebruikmaken van technische ondersteuning door Microsoft en kunnen programma's op termijn onbruikbaar worden of kuren gaan vertonen. Microsoft raadt gebruikers dan ook aan over te stappen op Windows 10.

Is er leven na Windows 7?

Jazeker. De opvolger van het besturingssysteem, Windows 8.1, wordt in principe ook nog ondersteund. Deze versie wacht echter hetzelfde lot: vanaf 10 januari 2023 ontvangt Windows 8 geen beveiligingsupdates meer. Sinds 2018 ontvangt het besturingssysteem al geen reguliere updates meer.

Wil je op lange termijn zeker zijn, dan is de beste optie om Windows 10 te gaan gebruiken. Microsoft blijft deze software ondersteunen en aanpassen. Er komt ook geen Windows 11, heeft het bedrijf bekendgemaakt, want de focus ligt volledig op de huidige versie.

Hoe duur is overstappen op Windows 10?

Dat ligt eraan. Je hebt twee opties: een computer updaten naar Windows 10 of een nieuwe pc of laptop met Windows 10 kopen.De prijzen zijn sterk afhankelijk van het systeem en de wensen & eisen.