

HOE VERHINDER IK ONGEWENSTE TOEGANG TOT MIJN ACCOUNT?

Je accounts beveiligen gaat verder dan enkel een sterk wachtwoord gebruiken, je moet ook dat wachtwoord veilig bewaren. Deel je wachtwoord niet met anderen, laat niemand meekijken wanneer je het invoert, en laat het zeker nergens rondslingeren op een papiertje.

TOE
GANG



06. DEEL JE WACHTWOORD NOOIT MET ANDEREN

Een wachtwoord is strikt persoonlijk. Je weet nooit wie je kunt vertrouwen. Laat dus niemand meekijken wanneer je je wachtwoord of pincode invoert. En deel het nooit met anderen, zeker niet via e-mail: berichten kunnen onderschept of omgeleid worden zonder dat je het weet. Moet je in een noodgeval toch je wachtwoord delen met iemand, doe dit dan via WhatsApp of Signal, en verander het daarna.

07. GEBRUIK VOOR ELK ACCOUNT ANDERE WACHTWOORDEN

Gebruik voor elk account een ander wachtwoord. Krijgt een hacker jouw wachtwoord toch te pakken, dan heeft hij geen toegang tot je andere accounts.

08. BEWAAR JE WACHTWOORDEN NIET OP EEN VANZELFSPREKENDE PLEK

Bewaar je wachtwoorden niet op een plek die voor iemand met kwade bedoelingen vanzelfsprekend is, zoals in je portefeuille, agenda of in de buurt van je computer. Bewaar je wachtwoorden ook niet op een apparaat, tenzij in een versleuteld bestand of, beter nog, gebruik een wachtwoordmanager.

09. WEBSITE GEHACKT? VERANDER JE WACHTWOORDEN

Is een website waarbij jij een account hebt het slachtoffer geworden van hackers, verander dan meteen je wachtwoord om te voorkomen dat iemand toegang krijgt tot je account op die site. Gebruikte je dit wachtwoord ook om aan te melden op andere sites, verander het dan ook daar meteen. En gebruik in het vervolg voor elk account een uniek wachtwoord!

10. SCHAKEL TWEESTAPSVERIFICATIE IN VOOR JE ACCOUNTS

Authenticatie of verificatie in twee stappen is een dubbele bescherming voor je accounts. Telkens als je je wachtwoord gebruikt om in te loggen, wordt er een code verzonden naar je mobiele telefoon. Met die code krijg je toegang tot je account of apparaat.

Krijgt iemand je wachtwoord in handen, dan heb je toch nog een extra beveiligingslaag. Zo schakel je tweestapsverificatie in voor je accounts:

-  Apple: Op je iPhone kan je dit inschakelen via **Instellingen** > klik op je naam > **Wachtwoord en beveiliging**; op je Mac ga je naar het **Apple-menu** > **Systeemvoorkeuren** > **Apple ID** > **Wachtwoord en beveiliging**.
-  Facebook: Klik rechtsboven op  > **Instellingen en privacy** > **Instellingen** > **Beveiliging en aanmelding** > **Tweestapsverificatie gebruiken**.
-  Google: Log in op myaccount.google.com, ga naar **Beveiliging** en klik onder **Inloggen bij Google** > **Verificatie in twee stappen**.
-  Microsoft: Meld je aan op account.microsoft.com/security en kies **Geavanceerde beveiligingsopties** > **Verificatie in twee stappen**.
-  Twitter: Klik links op **Meer** (op je smartphone druk je op je profielfoto) > **Instellingen en privacy** > **Beveiliging en accounttoegang** > **Beveiliging** > **Tweestapsverificatie**.



WIST JE DAT ...

het klassieke wachtwoord in de toekomst misschien verdwijnt? Volgens het World Wide Web Consortium (W3C) zijn wachtwoorden "één van de zwakste schakels in het waarborgen van een veilig internet". Zij voerden daarom in 2019 een nieuwe webstandaard (WebAuthn) in die grotendeels gebaseerd is op het principe van tweestapsverificatie: je identiteit bewijst je bijvoorbeeld aan de hand van een code die je toegestuurd krijgt op je smartphone, of door middel van een speciale USB-stick.