computer service heuvelland

Dit moet je doen als je bent gehackt op social media!

Steeds meer social media accounts worden gehackt. Wat moet je doen als dit gebeurd?

Facebook

Worden je vrienden bestookt met duistere links, plaatst je account berichten waar je geen weet van hebt en vindt jouw Facebook-profiel spontaan pagina's leuk? Dan ben je gehackt. Zo krijg je de controle terug:

- Wijzig je wachtwoord op de daarvoor betreffende pagina bij de Facebook-instellingen.
- Op dezelfde pagina vind je een overzicht van browsers en apparaten die zijn gebruikt om in te loggen. Beëindig alle sessies die verdacht zijn.
- Laat Facebook weten dat je vermoedelijk gehacked bent. Als je aangeeft dat iemand zonder je toestemming toegang heeft gehad tot je account, controleert Facebook dat en helpt je vervolgens verder.

Instagram

- Als je nog kunt inloggen, wijzig dan eerst je wachtwoord of laat het resetten door je wachtwoord te wijzigen en het naar jezelf te laten sturen.
- Trek de toegang in van verdachte externe apps.
- Kun je niet meer inloggen? Vraag Instagram dan om een beveiligingscode naar je e-mailadres of telefoonnummer te sturen. Zo bevestig je dat jij de eigenaar bent van je account.

Als je het account niet met een beveiligingscode kunt herstellen, kun je het account rapporteren. Op deze pagina lees je hoe dat bij Android en iOS in zijn werk gaat.

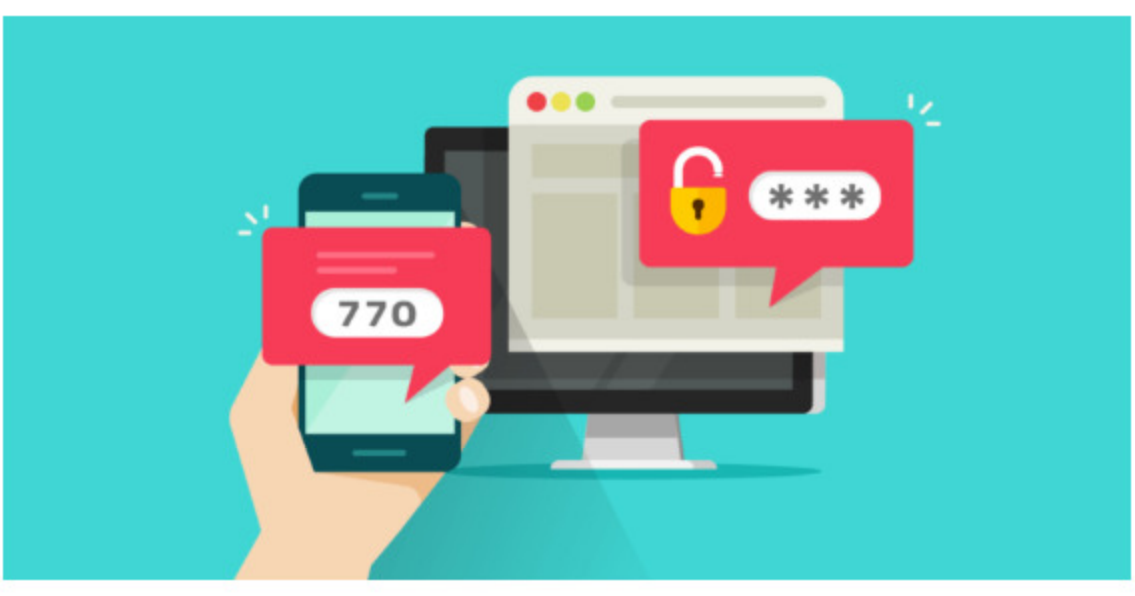
Twitter

- Ga naar de instellingen en verander je wachtwoord. Kies een sterke toegangscode die je niet eerder hebt gebruikt, ook niet ergens anders.
- Kun je niet meer inloggen? Probeer eerst je wachtwoord te resetten. Controleer vervolgens of de e-mail om je wachtwoord te resetten gestuurd is naar het adres dat aan je account is gekoppeld.
- Wanneer je nog steeds niet kunt inloggen, kun je een ondersteuningsverzoek indienen. Kies in de lijst met opties voor 'gehackt account'. Vul daar het aan je account gekoppelde e-mailadres in om meer instructies te ontvangen van Twitter. Vermeld daarbij ook je gebruikersnaam en de datum waarop je voor het laatst toegang had tot je account.
- Zorg ervoor dat het e-mailadres dat gekoppeld is aan je Twitter-account is beveiligd Het gekoppelde e-mailadres staat in direct verband met je account en is dus vrij cruciaal in dit proces. Zorg er daarom voor dat het adres beveiligd is.
- Beëindig sessies en verbindingen met applicaties van derden. Dit doe je bij je instellingen. Daar kun je de toegang intrekken voor applicaties van anderen die je niet kent en sessies beëindigen die niet door jou zijn gestart.

Voorkomen is beter dan genezen

Beperk daarom het risico met deze tips:

- Kies een sterk wachtwoord. De vuistregel is: hoe langer, hoe beter. Een combinatie van hoofdletters, kleine letters, cijfers en vreemde tekens maakt het onwaarschijnlijker dat iemand je wachtwoord raadt.
- Hergebruik hetzelfde wachtwoord niet bij verschillende diensten. Ligt het bij het ene platform op straat, bijvoorbeeld omdat het bedrijf gehackt wordt, dan is toegang tot je andere account een fluitje van een cent
- Schakel tweestapsverificatie in voor aanvullende beveiliging. Om in te loggen is dan niet alleen een wachtwoord, maar ook een aanvullende code nodig, die bijvoorbeeld per mail of sms wordt verstuurd.
- Neem een wachtwoordmanager: een digitale kluis waarin je je wachtwoorden veilig kunt opslaan. Grote diensten zijn 1Password en LastPass.



Wat is tweestapsverificatie en wat moet ik ermee?

Wil je tweestapsverificatie instellen? Die vraag wordt door steeds meer apps en websites gesteld. Maar wat is het, en waarom zou je het doen?

In feite betekent tweestapsverificatie gewoon ‘we herkennen je aan een combinatie van iets wat je weet (bijvoorbeeld je wachtwoord), iets dat je hebt (bijvoorbeeld je telefoon) en/of iets dat je bent (bijvoorbeeld je vingerafdruk of gezicht)’. In de praktijk gaat het vaak om een wachtwoord en een code die net is aangemaakt door een app, hardwaresleutel of sms.

Voorbeelden zijn tweestapsverificatie via SMS, een verificatieapp of een hardwaresleutel.

Maar waarom zou ik dit doen?

Tweestapsverificatie kan voor sommige gebruikers erg irritant zijn. Wil je op je desktop- of laptopcomputer ergens inloggen, dan zul je vaak een tweede apparaat in de buurt moeten hebben. Steeds meer apps bieden wel een mogelijkheid om voor langere tijd één apparaat te verifiëren, zodat dat niet regelmatig opnieuw hoeft te gebeuren.

Toch is het zeker de moeite waard. De afgelopen jaren werden regelmatig wachtwoorden gestolen in grote datahacks.

Met tweestapsverificatie vermijd je dat een hacker eenvoudig je account binnendringt. Hij of zij moet immers eerst kunnen bewijzen écht jou te zijn. En tot nu toe zijn er nog geen goede manieren gevonden om massaal tweestapsverificatiecodes te stelen.

Heb je hulp nodig bij het instellen of twijfel je over de juiste keuze? wij helpen je graag!

Waarom loopt de batterij van mijn telefoon steeds sneller leeg?

De batterijen van nu werken in feite nog altijd op dezelfde manier als de eerste batterij ooit, gemaakt door de Italiaan Alessandro Volta.

In het jaar 1800 bouwde hij een toren van zink- en koperplaatjes, gescheiden door papier gedrenkt in een zoutoplossing. De bovenkant en de onderkant verbond hij met metaaldraad. Pakte je die draad vast, dan kreeg je een schok. De eerste batterij was geboren.

Weinig veranderd

De huidige batterijen in bijvoorbeeld je telefoon werken op eenzelfde manier, al zijn de materialen anders. Hier reizen geen zinkionen van zink naar koper, maar lithiumionen van grafiet naar (meestal) lithiumkobaltoxide.

Een groot verschil met de batterij van Volta is dat je de processen in je telefoonbatterij kunt omkeren. Simpel gezegd: je kunt de batterij weer opladen. Steek de stekker in het stopcontact en de elektriciteit dwingt de lithiumionen naar waar ze vandaan kwamen: je batterij is weer vol.

Batterij brokkelt af

Helaas kun je niet oneindig vaak opladen. Als je al een tijdje dezelfde smartphone hebt, zul je dat gemerkt hebben: de batterij gaat minder lang mee dan voorheen. Dit komt deels doordat de stoffen in de zoutoplossing door een chemische reactie afbreken. De lithiumionen kunnen hierdoor minder goed naar de andere kant stromen.

Daarnaast ‘ademt’ de batterij. "Zowel het grafiet als de lithiumkobaltoxide krimpt en zwelt tijdens het opladen en ontladen. Dat komt doordat ze dan ionen opnemen of juist afstaan. Al dat gekrimp en gezwel zorgt voor scheurtjes in de materialen, waardoor er stukjes afbrokkelen en nutteloos worden.

Hitte is funest

Voorkomen dat je batterij slechter wordt, zal nooit lukken. Maar met een beetje zorg en aandacht kun je de achteruitgang wel vertragen. Bijvoorbeeld door je telefoon nooit helemaal op te laden en niet aan de lader te laten zitten als de batterij vol is.

Ook snelladen gebeurt met een hoger voltage en is dus onverstandig. Daarnaast kan een hoge temperatuur de vloeistof beschadigen.

Tot slot een tip voor als je een nieuwe telefoon hebt, maar je oude wilt bewaren: leg hem niet weg met een volle batterij. Een volle batterij houdt die spanning als het ware vast. En die spanning is niet goed voor de batterij. Voor de zekerheid kun je hem het best halfvol wegleggen.