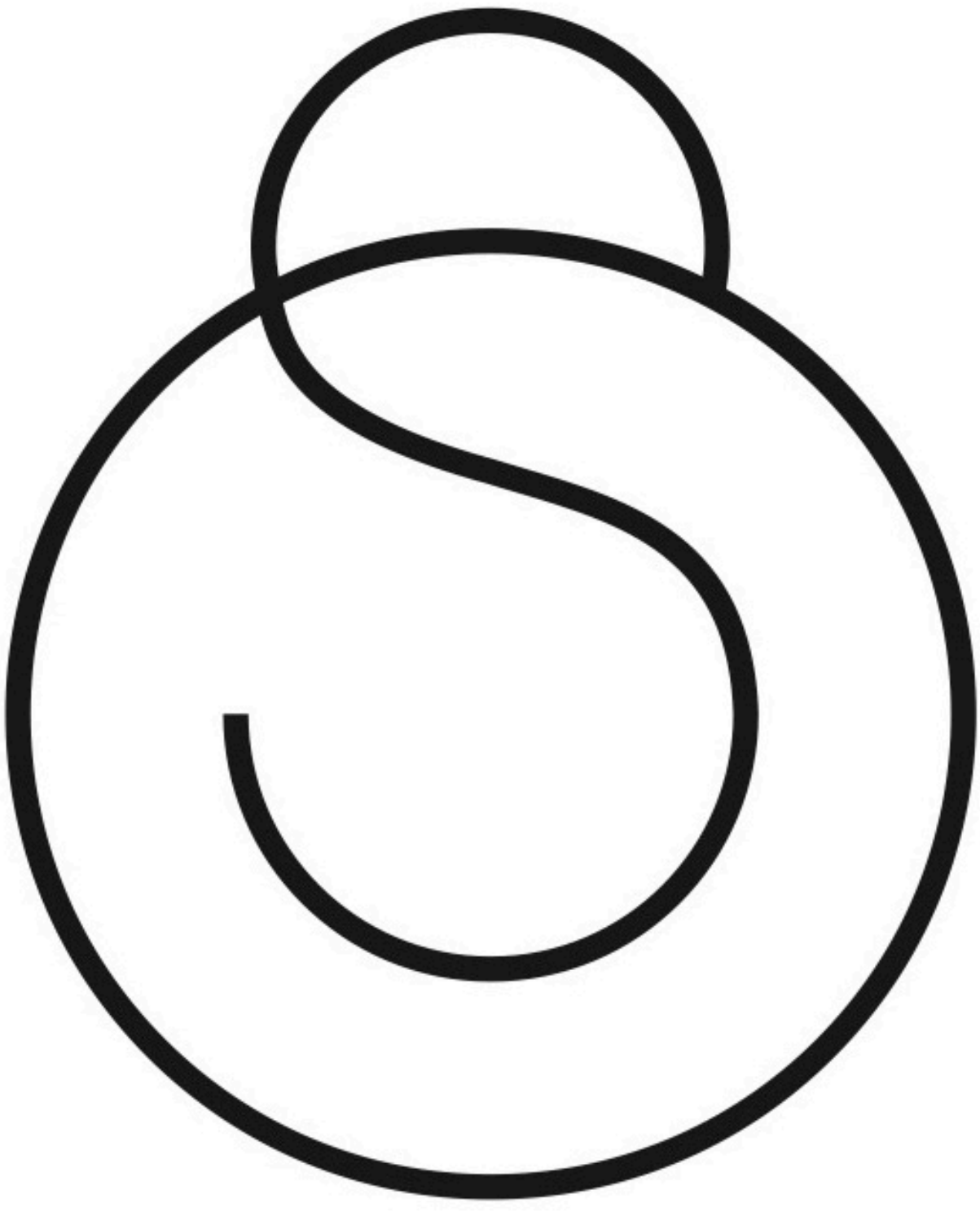
Jozef Dresselaers - Apple & Cloud & Security Expert

6 tips om uw cloud beter te beveiligen



6 tips om uw cloud veiliger te maken!

Is een cloud veilig?

Altijd, overal en op elk apparaat toegang hebben tot uw gegevens wordt steeds meer de norm. Hiervoor doen veel ondernemers beroep op een clouddienst, zoals Dropbox, iCloud, Google Drive of Microsoft Onedrive. Maar zijn uw gegevens daar wel veilig en hoe kunt u die beveiliging zelf verbeteren? **Jozef Dresselaers, Apple & Security Expert en oprichter en bedenker van SO - the best of both worlds**, geeft het antwoord.

Is de cloud veilig? Nee!

Net zoals in het echte leven is ook in de gegevensbeveiliging absolute veiligheid onbestaand. Als iemand me dus vraagt of de cloud veilig is, moet ik **nee** antwoorden.

Kunt u de cloud veilig(er) maken? Ja, absoluut!

Met de volgende zes tips kunt u het hackers en personen met slechte bedoelingen een heel pak moeilijker maken!

TIP 1: Controleer op eerdere lekken

Voor u de beveiliging van uw cloud zelf verhoogt, checkt u best of uw gegevens niet al eerder gestolen zijn. Een handige tool hiervoor is de website www.haveibeenpwned.com, waarop u kan zien of uw logingegevens al circuleren op het internet!

TIP 2: Leer phishing herkennen

Daarnaast leert u best phishing herkennen. Dit zal u helpen gegevensdiefstal te voorkomen. Bij phishing proberen hackers u om de tuin te leiden en u uw paswoord te ontfutselen door u een mail te sturen die erg sterk lijkt op de mails van bijvoorbeeld uw bank of een andere dienstverlener. Ze zullen vragen om uw paswoord ergens in te voeren om het te verifiëren of het te resetten. Wees dus steeds op uw hoede als u zulke mails krijgt en contacteer bij twijfel de desbetreffende dienstverlener via telefoon op een gekend nummer.

Wenst u uw werknemers op te leiden om phishing mails te herkennen, stuur me dan een bericht. Met Sophos Phish Threat kunnen we een "**Phishing attack simulation and training**" voorzien voor in uw bedrijf!

TIP 3: Kies een degelijk wachtwoord

(1) Kies een verschillend wachtwoord voor elke clouddienst en (2) zorg ervoor dat uw wachtwoord minimum 12 tekens bevat waaronder minstens één hoofdletter, kleine letters, leestekens en cijfers.

Tenzij u een ijzersterk geheugen heeft, zal het een hele opgave worden om al die wachtwoorden te onthouden. Gelukkig bestaan hier oplossingen voor:

- Gebruik een **wachtwoordprogramma** zoals http://www.1password.com/. U moet zich dit voorstellen als een soort van virtuele kluis waarin u al uw wachtwoorden opslaat en waarvan u de 'master key' heeft. Dit moet dan wel een zeer sterke sleutel zijn waar u voorzichtig mee omspringt. Als u die kluis in een cloud bewaart, moet u die ook extra beveiligen!

- Minder omslachtig en ook effectief: Gebruik een **wachtwoordzin**. Dit is een zin die u gemakkelijk kunt onthouden en waarvan de eerste letter van elk woord uw wachtwoord vormt. Zo wordt bijvoorbeeld '**Ik koop elke 2 weken bloemen voor mijn vrouw !'** het woord '**Ike2wbvmv!**'. Dit is een sterk wachtwoord! Om het nu nog verschillend te maken voor elk cloud-account voegt u hier bijvoorbeeld achteraan de twee eerste letters van de cloud-dienst toe –> ap voor Apple, mi voor Microsoft, go voor Google, … - en u heeft sterke wachtwoorden die u gemakkelijk kunt onthouden. => **Ike2wbvmv!ap** voor Apple, enz…

Zolang uw wachtwoorden niet gehackt zijn, is het ook niet nodig om ze regelmatig te veranderen (hoe u dit controleert, zag u in stap 1). Integendeel, meer en meer diefstallen gebeuren juist tijdens het wijzigen van wachtwoorden … , denk maar aan tip 2.

TIP 4: Ga voor tweestapsauthenticatie

Elke serieuze cloud-dienst biedt de mogelijkheid aan om tweestapsauthenticatie of Two Factor Authentication (**2FA**) in te stellen, het vergt gewoon even zoekwerk in de instellingen.

2FA bestaat uit een extra authenticatie bovenop uw wachtwoord. Dit kan bijvoorbeeld een code zijn die u wordt toegezonden via mail of sms – hoewel dit tegenwoordig niet meer zo veilig is als vroeger – of via een Authenticator app zoals Google Authenticator of Microsoft Authenticator.

Vergelijk het met de kaartlezer die u heeft om aan home-banking te doen: de code wordt ter plaatse gegenereerd en blijft maar voor een beperkte periode geldig. Zelfs als ze gestolen wordt, moeten hackers er dus zeer snel bij zijn.

TIP 5: Schep orde in uw cloudgebruik

Ga eens na hoeveel clouddiensten u gebruikt en vraag u af of dit wel nodig is. Beter één cloud-dienst gebruiken die u degelijk beveiligd hebt dan meerdere waarvan de beveiliging niet optimaal is.

Daarnaast zal het voor u ook overzichtelijker zijn en moet u niet onthouden welke data in welke cloud zitten. Bovendien zijn al deze diensten continu aan het synchroniseren, wat veel vraagt van de batterij van uw apparaat en het trager maakt.

TIP 6: Deel niet zomaar uw bestanden met iedereen

Let ten slotte goed op met wie u bestanden deelt via uw cloud-dienst.

Als u een goede beveiliging heeft, maar de persoon waarmee u gegevens deelt heeft dat niet, dan kunnen hackers alsnog via die weg inbreken!

Waak dus over wie toegang heeft en kijk zeker uw instellingen in verband met bestanden delen met derden goed na!

Wenst u een check-up van uw digitale leven?
Contacteer mij via support@powerview.be

Jozef Dresselaers - SO Apple & Security Expert
SO the best of both worlds - www.sothebestofbothworlds.be