



Awake

Vrijwaar uw e-reputatie op Facebook

In het kort

De Facebook Timeline werd aangekondigd in september 2011 tijdens de f8-conferentie en is vandaag beschikbaar voor de 800 miljoen gebruikers van het sociale netwerk. Hoe moet u haar installeren? Facebook heeft deze presentatie uitgewerkt om de gebruikers gerust te stellen, aangezien die altijd wat terughoudend zijn telkens er een nieuwe update van het platform is. <https://www.facebook.com/about/timeline>

De ingebruikneming van de Timeline ving aan op 15 december van vorig jaar in Frankrijk. Deze belangrijke update vereist alle aandacht van de gebruikers van Facebook omdat hiermee de fundamenten gelegd worden van een nieuwe weg van sociaal verkeer. We beleven een overgang van het profiel naar het dagboek. Het privéleven van de gebruiker krijgt een opmaak via Facebook. Om de gebruikers van het sociale netwerk te beschermen, publiceert Bitdefender enkele nuttige adviezen bij wijze van hulp bij het vrijwaren van hun e-reputatie, zowel op persoonlijk als op professioneel vlak.

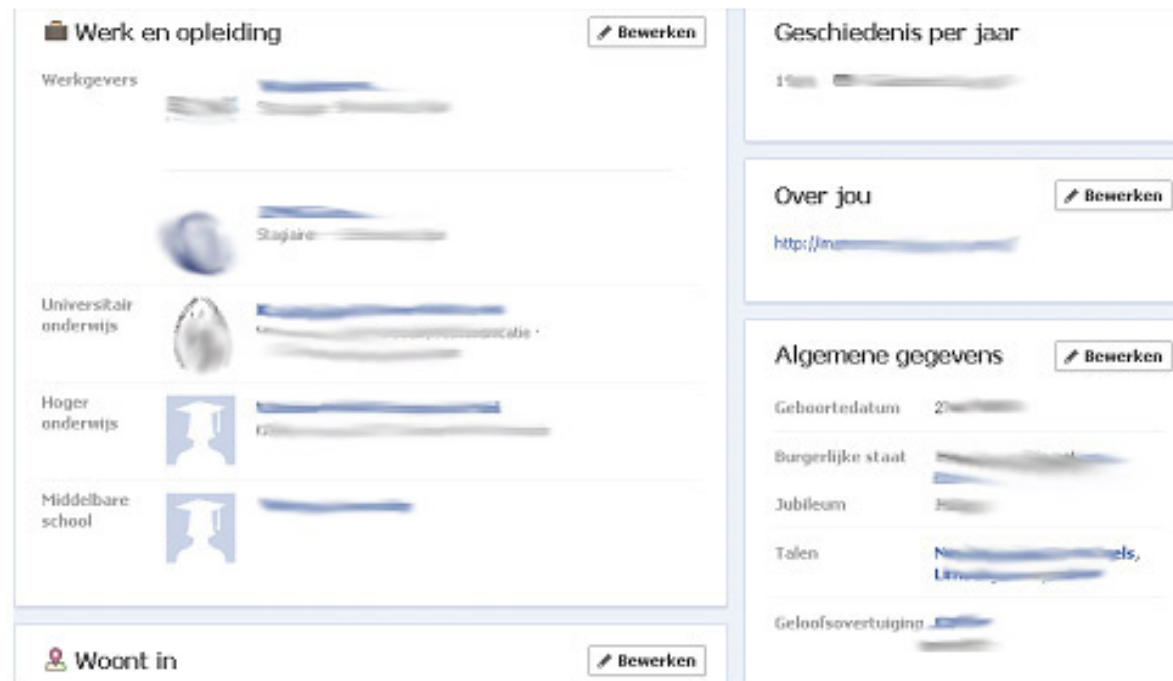
1. Hoe ziet de Timeline eruit?



4 grote wijzigingen :

1) De Intelligente Lijsten

De invoering van *Intelligente Lijsten* spoort de gebruiker aan om een pak persoonlijke informatie, zoals adres, Twitter-account, curriculum vitae, familiale gegevens, enz. te verstrekken. In navolging van tal van professionele netwerken heeft de gebruiker de mogelijkheid om bijzonder veel informatie mee te geven en om mensen te identificeren als familieleden, collega's, medewerkers of anderen. Je hoort wel eens dat Facebook geknipt is voor professioneel gebruik, maar wij raden de gebruikers aan om de vertrouwelijkheid van deze informatie goed in de hand te houden, want openbare informatie kan een perfect wapen vormen voor doelgerichte aanvallen en onrechtmatige inbezitneming van identiteit.



2) Informatie in blok

De « Timeline » van Facebook gaat ervan uit dat foto's, vermeldingen, artikels, toepassingen,... tot het publieke domein behoren. Het meest hinderlijke aspect hiervan is dat deze informatie standaard als « publiek » wordt beschouwd. Weldra wordt het makkelijk om informatie over gezondheid te delen, zoals een breuk, een chirurgische ingreep of een ziekte. De programmering van de vertrouwelijkheid van het dagboek van de gebruiker voorkomt de verspreiding van persoonlijke informatie.



3) De « Timeline », een biografie 2.0 die publiek kan worden gemaakt.

Al wat wordt gedeeld op Facebook is voortaan beschikbaar en makkelijk toegankelijk. De « Timeline » vormt een revolutie op het vlak van gebruiksvriendelijkheid, maar ze houdt tevens in dat ons virtuele leven openbaar wordt. Als de standaardparameters niet worden gewijzigd door de gebruiker om de toegang tot zijn wall te beperken, zal zijn geschiedenis voor iedereen zichtbaar worden: vrienden, foto's, plaatsen die de gebruiker heeft bezocht, relaties en nog veel meer. In enkele muisklikken kan een bezoeker posts terugvinden van jaren geleden. Al wat wordt gedeeld op Facebook is voortaan beschikbaar en makkelijk toegankelijk.



4) De sidebar met acties

Deze balk bevindt zich boven de chat en biedt de kans om in real time de acties in beeld te brengen die worden uitgevoerd door de omgeving van de gebruiker: posts, vermeldingen, commentaren, shares, ... Om meer interactie tussen de gebruikers te stimuleren, opent deze functionaliteit een nieuwe weg voor het delen en zichtbaar maken van alle niet geprogrammeerde publieke posts.



2. « Overzicht van het profiel als ... »

Weet de gebruiker heel precies wat zijn vrienden of nobele onbekenden te zien krijgen wanneer ze zijn naam intikken op Facebook? Om dat te weten, moet hij naar zijn profiel gaan, klikken op de regelknop en nadien op « *Overzicht van het profiel als ...* ».



Met deze tool kan de gebruiker visualiseren hoe zijn dagboek in beeld wordt gebracht bij zijn vrienden of andere gebruikers van Facebook. Hij kan ook elk van zijn posts programmeren in functie van het publiek van zijn keuze.

3. Controle over de vertrouwelijkheid van de posts

Het belang van Facebook schuilt volgens M. Zuckerberg in het creëren van een band en het delen van info met zoveel mogelijk anderen. Het is echter mogelijk om shares te beperken tot de eigen community van vrienden en niet beschikbaar te maken voor de hele Facebook-gemeenschap. Daartoe moet de gebruiker naar de rubriek « *Vertrouwelijkheidsparameters* » gaan waar hij kiest voor « *Gepersonaliseerd* ». Vervolgens selecteert hij de mensen met wie hij zijn status, updates en foto's wenst te delen.

facebook Zoeken Startpagina

Privacyinstellingen

Privacy bepalen tijdens plaatsen van berichten

Je kunt de privacy van je statusupdates, foto's en gegevens bepalen met de inlinepubliekselectie. Dit kun je tijdens of na het plaatsen van je informatie doen. De mensen waarmee je informatie deelt, kunnen je informatie altijd met anderen delen, ook met toepassingen. Je kunt je [tijdlijninformatie bewerken](#) om te zien hoe dit werkt of hier klikken voor [lees meer](#).

Wat ben je aan het doen?

San Francisco Aangepast Plaatsen

Je standaardprivacy bepalen

Deze instelling is van toepassing op statusupdates en foto's die je plaatst op je tijdlijn vanuit een Facebook-app die niet beschikt over een intern hulpmiddel voor publiekselectie, bijvoorbeeld Facebook voor BlackBerry.

Openbaar Vrienden Aangepast

Wij raden de gebruikers zelfs aan om lijsten met vrienden samen te stellen in functie van de relaties die ze onderhouden met hun « vrienden » op Facebook. Bijvoorbeeld een specifieke lijst voor familieleden, een andere voor collega's, voor vrienden, voor professionele contacten, ... Op die manier kunnen ze hun publiek kiezen naargelang hun posts.

4. Privégeheimen veiligstellen

Sociale games zoals PetVille, FarmVille of wedstrijdspellen kennen steeds meer succes op Facebook ... maar ze hebben de neiging om het nieuwsoverzicht van de omgeving van de gebruiker te overspoelen met notifications die de geringste vordering in het spel willen meegeven. Vandaag kan de gebruiker muziek beluisteren via streaming-muziektoepassingen, die worden gesynchroniseerd met een Facebook-account. Maar de gebruiker wenst misschien niet dat zijn omgeving de inhoud van zijn playlists in detail kent. Wat kan hij doen om zijn diverse spelletjesactiviteiten op sociale netwerken te beschermen?

The screenshot shows the 'App-instellingen' (App Settings) page on Facebook. At the top, it states: 'Je hebt deze app toestemming gegeven om te communiceren met je Facebook-account:'. Below this, there are two app entries. The first entry is for an app that was used 'Meer dan 6 maanden geleden' (More than 6 months ago) and has a 'Bewerken' (Edit) button. The second entry is for an app that was 'Laatst aangemeld: 24 januari' (Last logged in: 24 January) and has an 'App verwijderen' (Remove app) button. The main section is titled 'Deze app kan/heeft:' (This app can/have:). It lists two types of access: 'Toegang tot de basisinformatie van' (Access to basic information of) and 'Toegang tot de informatie die mensen met mij' (Access to information that people share with me). A dropdown menu is open, showing privacy options: 'Openbaar' (Public), 'Vrienden' (Friends), 'Alleen ik' (Only me), and 'Aangepast' (Custom). The 'Alleen ik' option is selected. Below this, there are sections for 'Laatste gegevensteegang:' (Last data access:), 'Privacy voor app-activiteiten:' (Privacy for app activities:), and 'Meldingen:' (Notifications:). At the bottom, there is a 'Sluiten' (Close) button.

5. De achterhoede beschermen

Er werden « *social reader applications* » ontworpen om het delen van content met de omgeving te vergemakkelijken of om een blik te kunnen werpen op wat de anderen lezen. Toch willen we dat bepaalde reads geheim blijven. Daartoe moet de gebruiker tijdens de installatie van die toepassingen gaan naar « *Accountparameters-> Toepassingen* » en klikken op « *Wijzigen* » naast de toepassing waarvoor hij de vertrouwelijkheid van de posts wil veranderen. Op die manier zullen deze toepassingen geen reads onthullen die de gebruiker bij voorkeur voor zich houdt.



The screenshot shows the Facebook privacy settings for an application. The interface is in Dutch. The main section is titled 'Deze app kan/heeft:' and lists two types of access: 'Toegang tot de basisinformatie van Z...' (Basic information) and 'Toegang tot de informatie die mensen met mij...' (Information from people I interact with). The 'Basic information' access is currently set to 'Verplicht' (Required). A dropdown menu is open, showing options: 'Openbaar' (Public), 'Vrienden' (Friends), 'Alleen ik' (Only me) - which is selected and has a checkmark, 'Aangepast' (Custom), 'Goede vrienden' (Close friends), and 'Alle lijsten weergeven...' (Show all lists). Below this, the 'Laatste gegevenstoegang:' (Last data access) is shown as 'Algemene gegevens' (General information) with links for 'Details weergeven' and 'Meer informatie'. The 'Privacy voor app-activiteiten:' (App activity privacy) section asks 'Wie kan er berichten en activiteiten van deze app op Facebook zien?' (Who can see messages and activities from this app on Facebook?) and is currently set to 'Alleen ik'. The 'Meldingen:' (Notifications) section has a dropdown menu set to 'De app me een verzoek s...'. A 'Sluiten' (Close) button is at the bottom.

Deze app kan/heeft:	Toegang tot de basisinformatie van Z...	Verplicht
	Inclusief naam, profielfoto, geslacht, netwerken, gebruikers... Lees verder	
	Toegang tot de informatie die mensen met mij... Woonplaatsen en Huidige woonplaatsen	

Laatste gegevenstoegang: Algemene gegevens
[Details weergeven](#) · [Meer informatie](#)

Privacy voor app-activiteiten: Wie kan er berichten en activiteiten van deze app op Facebook zien?
Alleen ik

Meldingen: Stuur me een bericht wanneer: De app me een verzoek s...

[Sluiten](#)

6. Informatie posten of featuren?

Men kan de posts in het dagboek volgens twee criteria kwalificeren: « *Wijzigen of intrekken* » en « *Featured* ». Zodra de gebruiker klikt op een shareknop van Facebook, die te vinden is in de meeste websites, wordt het artikel automatisch gedeeld in het dagboek van de gebruiker. Als de gebruiker zichtbaarheid wenst te geven aan dit artikel, moet hij enkel klikken op « *Featured* ». En als de gebruiker tot slot zijn omgeving niet langer wil laten genieten van dit artikel, moet hij enkel klikken op « *Wijzigen of intrekken* » en kiezen tussen « *Niet tonen in het dagboek* », « *Dislike...* ».



This screenshot shows a Facebook post from a user whose profile picture is blurred. The post text reads: "heeft een link gedeeld. 2 seconden geleden". The link preview features a red octagonal logo with "MALWARE CITY.COM" in white. The title is "Timeline Worries Twice Removed? - MalwareCity : Computer Security Blog" with the URL "www.malwarecity.com". The description says: "The answers NO. You cant shake the Timeline off. Once its on, its there to stay. - MalwareCity Blog on viruses description, botnets, spam review, malware". At the top right, a dark button labeled "Hoogtepunt" is visible. Below the post, the interaction options "Vind ik leuk · Reageren · Delen" are shown.



This screenshot shows the same Facebook post as the previous one. The text and link preview are identical. However, at the top right, a dark button labeled "Bewerken of verwijderen" is visible instead of "Hoogtepunt". The interaction options "Vind ik leuk · Reageren · Delen" are also present at the bottom.

7. Werking van de identificaties

De identificatie, beter gekend onder de naam tag, biedt de mogelijkheid om een virtueel label te kleven op een persoon of op de gebruiker, zelfs in verschillende types van toepassingen, zoals foto's en video's. Als de gebruiker niet wil dat zijn naam wordt gekoppeld aan een vooraf goedgekeurde content (vrienden kunnen soms grappenmakers zijn), kan hij terecht bij « *Vertrouwelijkheidsparameters* » en dan bij « *Werking van de identificaties* ».



The image shows a screenshot of the Facebook settings page for tags, titled "Instellingen voor tags". It contains five settings items, each with a description and a control element on the right:

- Tijdlijncontrole** van berichten van vrienden waarin je wordt getagd voordat ze op je tijdlijn komen (opmerking: tags worden wellicht wel elders op Facebook weergegeven) Aan >
- Tag Review** voor tags die vrienden willen toevoegen aan je berichten Aan >
- Maximale zichtbaarheid van je tijdlijn** van berichten waarin je bent getagd zodra ze op je tijdlijn staan * Aangepast ▾
- Tag Suggestions** wanneer vrienden foto's uploaden die op jou lijken Vrienden >
- Vrienden kunnen je bij plaatsen inchecken** die de Mobile Places-app gebruiken Aan >

At the bottom right of the settings area, there is a blue button labeled "Klaar".

Deze lijst kan misschien geruststellend en intuïtief lijken, maar de knoppen *On/Off* zijn op zijn zachtst gezegd bedrieglijk. Temeer daar ze de gebruiker allebei naar een bijkomende stap leiden waar hij dezelfde functie moet activeren/uitschakelen, wat ertoe kan leiden dat de gebruiker zich gaat afvragen waar hij zich de eerste keer heeft vergist.

De functies « *Onderzoek van het profiel* » en « *Controle voor tags* » zouden dus moeten worden ingeschakeld als de gebruiker op de hoogte wil worden gehouden wanneer hij wordt « getagd » door zijn vrienden of wanneer vrienden tags toevoegen aan content die de gebruiker heeft gepost.

Laten we het nu hebben over de uit te schakelen functies. De « *Tagsuggesties* » stellen aan de vrienden van de gebruiker voor om makkelijker foto's van eenzelfde gebeurtenis te posten. Zijn vrienden krijgen dan suggesties van mensen die ze kunnen taggen op een foto in functie van hun gelijkenis. De laatste functionaliteit, « *Uw vrienden kunnen aanduiden waar u zich bevindt* », zou de gebruiker in een lastig parket kunnen brengen. Tenzij hij zich bevindt naast de persoon die hem lokaliseert en akkoord gaat met diens handeling.

8. Abonnementen

Net zoals Twitter biedt Facebook zijn klanten de mogelijkheid om zich te abonneren op updates van gebruikers die niet noodzakelijk vrienden van de gebruiker zijn. Het is bijvoorbeeld mogelijk om toegang te krijgen tot de status, de artikels of de foto's van Mark Zuckerberg, de stichter van Facebook.

Als de gebruiker niet wil dat indiscrete ogen een blik kunnen werpen op zijn status, zijn foto's en zijn diverse posts, moet hij enkel klikken op het gedeelte dat is gereserveerd voor persoonlijke informatie, en moet hij de widget « *Abonnementen* » kiezen. Dan gaat hij naar « *Parameters* » en schakelt hij « *Abonnees* » uit.



Facebook vormt een middel voor spambots en oplichters om meer abonnees te verkrijgen. Het kopiëren van de functionaliteiten van Twitter kan zich eveneens vertalen in het importeren van zwendelpraktijken van het scamtype.

9. Zijn naam terugvinden in zoekmachines

Tot slot raden wij de gebruikers aan om hun naam regelmatig in te tikken in de zoekmachine van Facebook om te weten wat er over hen wordt gezegd op het sociale netwerk. Naast accounts die zich onrechtmatig hun identiteit toeëigenen, zouden ze ook fanpages op het spoor kunnen komen of groepen die hun naam vermelden. Bitdefender adviseert de gebruikers overigens om hun naam regelmatig op te zoeken via uiteenlopende zoekmachines, want de resultaten kunnen verschillen van de ene machine tot de andere, en om de pagina's te bezoeken waar hun naam duidelijk voorkomt.

Bij ongepaste resultaten stelt de CNIL aan iedereen een gids ter beschikking om digitale vingerafdrukken van het doek te vegen.

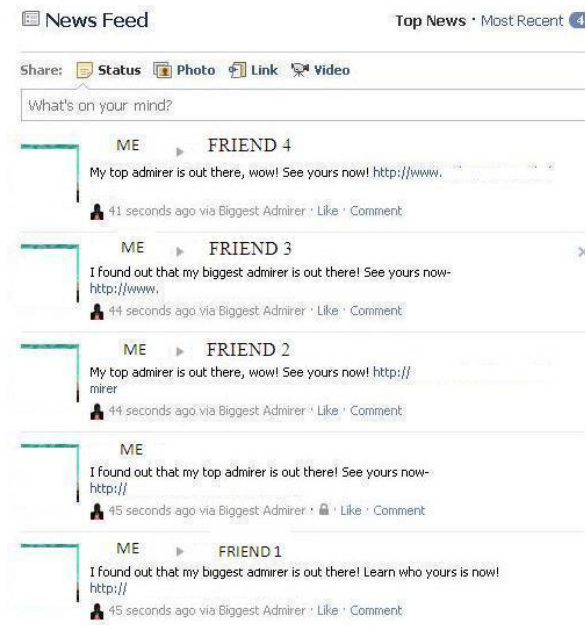
Om de verwijdering van content te vragen, moet men enkel de verantwoordelijke van de site contacteren, zodat deze de verwijzingen in kwestie weghaalt. De contactgegevens van die persoon zijn terug te vinden in de juridische vermeldingen, die verplicht beschikbaar zijn op de site. Om de content te kunnen laten verwijderen, moet men kunnen aantonen dat deze schadelijk is voor zijn reputatie. De CNIL stelt aan iedereen een e-mailmodel ter beschikking om dit procédé te vergemakkelijken. De webmaster krijgt twee maanden om te antwoorden. Bij gebrek aan een antwoord van hem of in het geval van een onbevredigend antwoord, kan men overwegen om een online klacht in te dienen bij de CNIL.

10. Sociale scams, vernietigend voor een reputatie

1) Twijfelachtige toepassingen

Facebook hangt niet af van een specifiek platform, de site kan functioneren op om het even welke computer en op alle belangrijke mobiele platformen: iOS, Android, Symbian en Windows. De site bezit zijn eigen beveiligde cloud waarin de persoonlijke gegevens van de gebruikers worden bewaard. Heel wat ongecontroleerde toepassingen van derden hebben toegang tot deze vertrouwelijke informatie (zodra de gebruiker er de toelating voor geeft tijdens de installatie van de toepassing), die dan wordt opgeslagen in de eigen cloud van deze toepassingen. Er bestaat geen enkele manier om te controleren wat er gebeurt met de gegevens zodra ze zich bevinden in de privécloud van een toepassing.

Als de gebruiker dus een toepassing installeert die kwaadaardig blijkt te zijn, kan deze toepassing geïnfecteerde berichten en links posten in zijn dagboek en de dagboeken van zijn vrienden. Iets wat nog vervelender is op het vlak van *personal branding* als het Facebook-account deel uitmaakt van de professionele strategie. Een typisch voorbeeld van dit soort oplichterij: « Wie bekijkt uw



profiel? » :

2) Kaping van muisklikken of clickjacking

Nadat er werd geklikt op een link om de inhoud van een video met een vaak aanstootgevende of schokkende titel te zien, wordt er automatisch een bericht gepost op de wall van het slachtoffer, met de mededeling I LIKE IT. Hoe is dit mogelijk ? Een Java-script installeert een onzichtbare like-knop onder de knop *Video bekijken*. De gebruiker klikt om de video te bekijken zonder zich er rekenschap van te geven dat hij met die klik zegt "I like it". Deze bedreiging heeft zich op een interessante wijze ontwikkeld. In het begin bestond het « like-mechanisme » op Facebook uit één regel onder de titel "Recente activiteit" van de profielpagina van de gebruiker. Nadien heeft het platform het virale mechanisme van deze knop verbeterd, door het resultaat ervan vergelijkbaar te maken met dat van de functie "Share". Anders gezegd, alle « likes » worden nu op de wall getoond met een label en een korte (vaak onbetamelijke) beschrijving :



Dit type van scam heeft enkele specifieke afleidingen gekend binnen de oorspronkelijke functies van Facebook: tagjacking, eventjacking en commentjacking. Door de tagmachtigingen te programmeren kan de gebruiker een einde maken aan elke poging tot tagjacking. Maar voor andere vormen van oplichterij is er de toepassing Bitdefender Safego. Deze toepassing is bedoeld om scams af te stoppen die de (professionele) geloofwaardigheid van de gebruiker in het gedrang kunnen brengen.

Ter herinnering: clickjacking heeft een bijzonder uitgebreide virale reikwijdte omdat een Facebook-gebruiker ongeveer 200 vrienden heeft die potentieel worden blootgesteld.

Besluit

In deze tijden waarin sociale netwerken de overhand krijgen op het professionele en persoonlijke visitekaartje, is het voor mensen moeilijk om te controleren wat er over hen wordt gezegd. Bovendien blijft het in een virtuele wereld waarin informatie wordt uitgewisseld via verschillende platformen, lastig om alle middelen te kennen waarmee de identiteit kan worden beschermd. Dat is de reden waarom er nieuwe aanpassingen werden aangekondigd door Facebook, die de aanwezigheid van toepassingen en hun werking erg zichtbaar zullen maken binnen het profiel van de gebruikers. Sociale zwendelpraktijken zullen er doeltreffender dan ooit tevoren door kunnen worden. Zo kan een afbeelding van een gebruiker worden beschadigd naar aanleiding van een slechte programmering van vertrouwelijke informatie die openbaar zou worden gemaakt.

De ingebruikneming van de Timeline zal, in navolging van eerdere updates van Facebook, wellicht vergezeld gaan van foute toepassingen of add-ons die het herstel van de oude opmaak beloven. Bitdefender raadt aan om dit soort berichten te wantrouwen: in de sociale wereld zal de toekomst in het teken van malware en manipulatie staan, wat inhoudt dat mensen zullen worden overtuigd om zichzelf te “infecteren” door toepassingen te installeren die hun opdracht op de achtergrond uitoefenen. Door de 10 adviezen, die uitvoerig aan bod komen in dit document, te volgen, maakt de reputatie van de gebruiker veel kans om ongeschonden te blijven op Facebook.

Bitdefender, uitgever van veiligheidssoftware, beschermt meer dan 400 miljoen mensen in de hele wereld en benut deze ervaring om onophoudelijk nieuwe toepassingen te ontwikkelen, zoals Bitdefender Safego, dat is gewijd aan de bescherming van de gebruikers van sociale netwerken. Identiteitsdiefstal, diefstal van vertrouwelijke gegevens, infecties, onvreemde wachtwoorden, clickjacking... Bitdefender Safego beveiligt het sociale leven van de gebruikers tegen alle soorten van e-bedreigingen en vrijwaart tevens hun e-reputatie.

Als u meer wilt weten over zwendelpraktijken op sociale netwerken, kunt u ons witboek lezen: *Vrienden, vijanden en Facebook: de nieuwe strijd tegen oplichterij*.