**Persbericht**

**Enkele onmiskenbare tips voor ‘Black Friday’ en ‘Cyber Monday’**

Brussel, 25 november 2016 – **Vandaag is het Black Friday! Een traditie die uit de Verenigde Staten naar Europa is overgewaaid en nu ook in België de kop opsteekt. Wie vandaag de deur uitgaat, op jacht naar allerlei koopjes, doet er goed aan enkele belangrijke *security tips* in acht te nemen… Wie vandaag niet meer tot in de winkels geraakt, kan online zijn slag proberen slaan op ‘Cyber Monday’.**

**Tip #1 - Hou je kredietkaart onder controle**

Indien je over een pinkaart beschikt, zorg er dan voor dat je ook die pin gebruikt, en niet zomaar je kredietkaart zijdelings door het toestel haalt… Pinnen is niet perfect, maar het zorgt er wel voor dat je data niet zomaar kan worden gekopieerd. Dit is iets wat met het *swipen* wel degelijk gebeurt. De magneetstrip wordt dan helemaal gelezen, telkens je de kredietkaart zijdelings door het betaaltoestel schuift. Dan komen we bij skimming terecht, wanneer oplichters een niet-rechtmatige copy maken van de data op je kaart. Bijvoorbeeld aan de hand van een ultradunne magneetstrip die in het betaaltoestel zit verborgen. Vergeet ook niet om je hand te bedekken telkens je de pincode ingeeft. Zo vermijd je dat de persoon na jou meekijkt, en dat je pin kan worden opgenomen door goed geplaatste videocamera’s.

**Tip #2 - Check goed je betaalticket**

Wanner je inkopen doet voor eindejaar, eindig je wellicht met een heleboel grote en kleine transacties. Ook al hou je vinger aan de pols over je uitgaven, op het eind van de dag kan het totaalbedrag ferm oplopen. Je doet er dan ook goed aan om telkens opnieuw je betaalticket goed na te kijken. Want er is een groot verschil tussen 9 en 99 euro. Ga dus zorgvuldig door je betaalticket en bekijk of je wel degelijk alles hebt aangekocht wat op het betaalformulier staat. Sommige banken versturen ook sms’jes bij elke transactie. Indien jouw bank ook over deze service beschikt, vink die dan zeker aan. Zo word je op de hoogte gehouden, telkens er een aankoop gebeurt met jouw kaart. Indien iemand misbruik heeft gemaakt van jouw betaalkaart, dan kom je dat op deze manier snel te weten…

**Tip #3 - Wees voorzichtig met location services**

De meeste mensen laten hun *location services* op elk moment geactiveerd op hun telefoon. Zo kan je jezelf snel terugvinden op een kaart, vooral handig wanneer je winkelt in een nieuwe buurt en je verloren loopt, of een nieuwe route naar je bestemming wilt. De moderne telefoons maken cocktails van die signalen om precies te weten waar je bent en geven die ook door aan Apple, Google, Microsoft en verschillende app verkopers. WIFI en Bluetooth kunnen je positie niet berekenen maar met behulp van andere draadloze apparaten in de buurt weten ze wel dat je in de omgeving bent.

Bijvoorbeeld indien Google Street View de exacte locatie van de Starbucks koffieshop heeft opgenomen, dan weten ze dat je je daar in de buurt bevindt. Zo kunnen ook Bluetooth bakens van Apple en Google je indirect tracken, aangezien ze unieke identificaties uitsturen die je telefoon oppikt. Wees er dan ook van bewust dat de winkels die bakens oppikken, en zo precies weten wanneer je wat deed toen je voorbij de winkel passeerde. En zo gebeurt het dat je dikwijls bepaalde acties op je telefoon ontvangt, telkens je in de buurt bent van een of andere winkel. Tijdens de drukke winkeldagen kan je er eventueel voor kiezen om die *location services* uit te zetten, om zo ongestoord te kunnen winkelen en je privacy te verbeteren. Of misschien wil je ze wel net aanzetten om geen enkele actie van je favoriete shop te missen!

**Tip #4 - Hou je spam-standaarden**

Wellicht kreeg je heel wat speciale aanbiedingen in je mailbox, waaronder heel wat mails van bedrijven waar je nog nooit van hebt gehoord… Uitgerekend die bedrijven prijzen producten aan die je wél goed kent. Let hiermee op! Vooral bij overvolle mailboxen kunnen oplichters toeslaan omdat ze handig gebruik maken van het feit dat er heel wat gelijkaardige mails worden uitgestuurd. Net dan ben je vatbaarder om die beste prijs eruit te kiezen en daarmee net iets sneller op een mail te klikken die je anders gegarandeerd als spam zou beschouwen. Denk dus goed na vooraleer je klikt!

**Tip #5 - Geef niet meer gegevens dan nodig**

Sommige websites vragen veel meer (persoonlijke) gegevens dan nodig: naam, adres, geboortedatum, geslacht, telefoonnummer, hobby’s, inkomsten, etc. Let ook hiermee op! Beslis vooraf hoeveel informatie je wenst prijs te geven zodat je niet voor voldongen feiten komt te staan. Hou er rekening mee dat er altijd een risico bestaat dat jouw data ergens terechtkomt waar je het zelf liever niet ziet verschijnen.

**Tip #6 - Laat je niet misleiden**

Er bestaan websites die mensen lokken met een goede deal om ze dan verder te misleiden voor compleet andere (veel minder goede) deals. Zorg ervoor dat je niet in deze val trapt en enkel ingaat op die aanbiedingen waar je echt voor open staat. Sta er ook bij stil dat sommige deals worden aangeprezen via een vertrouwde bron, maar dat het wel zou kunnen dat net die vertrouwde bron met malware is besmet…

**Onthoud vooral: Cyberveiligheid is voor het leven, niet alleen rond de feestdagen**

Sophos zegt dit niet alleen vandaag, maar ook telkens opnieuw rond de feestdagen, bij grote sportevenementen, enzovoort. De tips die Sophos geeft om speciale aandacht te geven aan cyberveiligheid verliest zijn waarde niet wanneer het feest voorbij is. Net nu Black Friday en Cyber Monday ook in onze contreien ingang hebben gevonden, laat het dan ook een extra reden zijn om nog zorgvuldiger om te springen met cyberveiligheid.

**Connect with Sophos**

[Twitter](http://soph.so/CfuKd)

[LinkedIn](http://soph.so/Cfv36)

[Facebook](http://soph.so/CfvaA)

[Google+](https://plus.google.com/%2Bsophos)

[Spiceworks](http://soph.so/Cgbwa%20)

[YouTube](http://www.youtube.com/user/sophoslabs)

[Sophos Blog](http://blogs.sophos.com/)

[Naked Security News](http://nakedsecurity.sophos.com/)

**Over Sophos**

Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com/).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**

Square Egg, Sandra Van Hauwaert, Sandra@square-egg.be, 0032 497 251816