**Blijf ook tijdens de kerstperiode veilig online**

*12 gouden tips voor een zorgeloze decembermaand*

**Nu Sinterklaas zijn hielen heeft gelicht, is het tijd om de kerstversiering af te stoffen en een mooie boom in huis te halen! En laten we de cadeaus niet vergeten: ook dit jaar zullen we met z'n allen onze creditcard trekken en online onze kerstinkopen doen. Want e-commerce blijft booming business.**

**Volgens BeCommerce.be, de Belgische vereniging van de bedrijven actief in verkoop op afstand, via internet, en dus alle vormen van e-commerce, zijn er in totaal 6,8 miljoen Belgen die online winkelen. Dat is 73% van de Belgische bevolking en 3% meer dan vorig jaar. Opvallend ook is dat de online aankopen via smartphones met 33% stijgen. En we mogen ervan uitgaan dat deze stijging zich in de komende weken verderzet.**

Gezien het alsmaar toenemend aandeel van online aankopen - en de veiligheidsrisico’s die daarmee hand in hand gaan - geeft Sophos een 12-tal tips waar iedereen rekening mee kan houden wanneer hij/zij op het internet een kerstcadeau voor zijn familie of vriend(in) wil kopen.

**1) Wijzig wachtwoorden voordat je begint met winkelen**

Gebruik niet hetzelfde wachtwoord op meer dan één website. Als cybercriminelen één wachtwoord te pakken krijgen, zullen ze deze onmiddellijk proberen op al je andere accounts. Maak daarom wachtwoorden zo lang en ingewikkeld als mogelijk. Het beste is om een wachtwoord manager te gebruiken, dat automatisch een uniek wachtwoord voor elke website genereert.

**2) Update je apparaten**

Patches herstellen beveiligingszwakheden die de ‘boeven’ reeds kennen of hier snel achter zullen komen. Stel beveiligingsupdates niet uit en volg ons advies: patch vroeg, patch vaak.

**3) Maak een back-up van bestanden**

Of je je laptop meeneemt met vakantie of gewoon thuis bent: vergeet niet regelmatig een back-up van onvervangbare documenten te maken. Mochten deze namelijk onverhoopt door bijvoorbeeld ransomware worden versleuteld, kun je met je back-up nog steeds alle waardevolle gegevens terugkrijgen.

**4) Kijk uit voor ‘rare’ geldautomaten**

Kijk uit voor geldautomaten wanneer je in deze maand geld opneemt. Oplichters zijn heel gehaaid en halen diverse trucs uit om zo achter de data en de PIN-code van een creditcard te komen. Als een geldautomaat er verdacht uitziet, meld dit bij de bank of politie.

**5) Pas op login koppelingen in e-mails**

De decembermaand is een populaire tijd voor cybercriminelen om 'phishing' e-mails te gebruiken om consumenten te verleiden tot het intikken van persoonsgegevens. Wanneer je in een e-mail verzocht wordt om te klikken op een link en vervolgens in te loggen op je account met een wachtwoord, is het mogelijk dat boeven je proberen te verleiden. Trap hier niet in. Wanneer je zelf een transactie wilt controleren op een van je accounts, open dan de browser en ga naar de betreffende website.

**6) Let op het ‘hangslot’ in de URL-balk**

Een hangslot in de adresbalk en een URL die begint met 'https' wil zeggen dat de website een beveiligde verbinding gebruikt. Bij sites die om persoonlijke informatie vragen maar geen hangslot hebben, kun je er zeker van zijn dat dit nepsites zijn!

**7) Kijk uit voor mails van ‘koeriers’**

Door online bestellingen in de decembermaand is het aannemelijk dat je een mail van een koeriersbedrijf ontvangt met de status van je bestelling. Oplichters weten dit en sturen mails over zogenaamde leveringsproblemen in de hoop personen naar hun website te trekken. Wanneer je echt contact wilt opnemen met een koeriersbedrijf, bel of mail ze dan zelf.

**8) Mail nooit je creditcardgegevens**

Soms weigert een creditcard bij een online betaling. Te goeder trouw kan een call center medewerker vragen de creditcardgegevens te mailen. Maar zo’n mail zou kunnen eindigen in de handen van cybercriminelen, zelfs als de verkoper met alle zorg met uw gegevens is omgegaan.

**9) Zet Flash uit**

Wil je één handeling uitvoeren om de veiligheid voor nu en voor altijd te verbeteren? Schakel Flash uit (of verwijder het helemaal). Booby-trapped Flash-bestanden zijn nog steeds een populaire manier van malwareverspreiding. En met steeds minder en minder sites die Flash vereisen, is het veiliger om helemaal zonder Flash door het leven te gaan.

**10) Pas standaardwachtwoorden aan**

Of het nu om een nieuwe babyfoon of een andere ‘internetcamera’ gaat: ze hebben allemaal een standaard (fabrieks)wachtwoord. Wordt dit wachtwoord niet aangepast, is het voor cybercriminelen makkelijk binnenkomen en zo te zien wat je aan het filmen bent. Dat kan van alles zijn: je huis, je baby of iets anders wat je liever voor jezelf houdt.

**11) Denk na voordat je deelt op sociale media**

Oversharing op social media is een slecht idee: of het nu om foto’s gaat van anderen, creditcardgegevens of een feestje waar je naartoe gaat: denk na voor je deelt. Zodra het online staat, zul je nooit in staat zijn het terug te nemen.

**12) Upgrade software van elk nieuw apparaat voor gebruik**

Zelfs ‘nieuwe’ computers en andere apparaten hebben meteen updates nodig. Tussen het moment waarop ze werden gefabriceerd en het eerste gebruik hebben cybercriminelen alle tijd (gehad) om nieuwe gaten in de beveiliging aan te vallen. Wanneer je nieuwe apparaten wilt beschermen, patch deze alvorens ze te gebruiken.

Tot slot: zorg ervoor dat thuiscomputers veilig zijn. Sophos Home is gratis en beschermt maximaal tien Windows- en Mac-computers tegen malware, ransomware, phishing en nog veel meer. Het is een eenvoudig te gebruiken oplossing die enkele minuten duurt om te downloaden voordat het kan worden gebruikt.

En onthoud: deze security tips nog zijn in 2017 ook nog steeds van toepassing.

Fijne feestagen gewenst!