



Geloof jij in Sinterklaas? Als het te mooi lijkt om waar te zijn ...

(Vrij gebaseerd op het artikel van KrebsOnSecurity "How to shop like a Security Pro")

De eindejaarsperiode is naast een periode van feesten, warmte en gezelligheid ook voor (cyber)criminelen het ideale moment om een slag binnen te halen! Nog snel een pakje online bestellen, vlug een last minute aanbieding meepikken, ... Daarom een paar tips.

In deze periode laten zelfs de meest doorwinterde experts wel eens een steek vallen, als ze holderdebolder nog snel een cadeautje nodig hebben, of als een superaanbieding nog maar slechts een uur geldig is ...

Met deze tips proberen we je veilig(er) doorheen de komende weken te loodsen. Want simpelweg voor de goedkoopste online aanbieding gaan, kan wel eens fout uitpakken.

Als je twijfelt, kijk dan eens wat verder

In deze tijd schieten online winkels als paddenstoelen uit de grond, ook de valse. Als je je aankopen doet bij een onbekende webwinkel die nog maar pas het daglicht gezien heeft, is het risico dat er een addertje onder het gras zit aanzienlijk hoger.

Hebben ze toch net dat ene hebbedingetje aan een echt nooit geziene prijs, neem dan toch even de tijd om wat onderzoek te doen naar online ervaringen van medekopers. Twijfel je nog steeds, dan kan je op <https://www.dnsbelgium.be> ook opzoeken sinds wanneer het internetadres, de domeinnaam zoals dat heet, geregistreerd is. Als die pas een paar weken bestaat ... pas dan op!

dnsbelgium Domeinnaam Producten Kennisbank Over ons

Home > Whois

DOMAIN NAME [welzijnsregio.be](#)

DOMAIN	
Name	welzijnsregio.be
Status	REGISTERED
Registered	October 29, 2003 11:23 AM CET
Last update	October 14, 2015 9:15 AM CEST

Gebruik liever een kredietkaart dan je debetkaart

Het artikel geeft aan dat je iets meer kans hebt om de schade te beperken met een kredietkaart (VISA, Master Card, enz.) dan met een debetkaart (je gewone bankkaart: Maestro, MisterCash). De kredietkaart is meestal voorzien van een paar limieten en de aankopen met die kaart worden gebundeld. Als criminelen er met je bankkaart vandoor kunnen gaan, zouden ze meer schade kunnen aanrichten op je bankrekening. Verder geven ze ook aan dat, mocht je rekening leeggeplunderd worden, de nalatigheidskosten voor je lening, verzekering, enz. voor jou zijn, ook al kan je achteraf je centen recupereren. Met een kredietkaart bouw je daar nog een stapje tussen.

To slotje of not to slotje

 bol.com bv [NL] | <https://www.bol.com/nl/>

We vertellen al jarenlang dat het belangrijk is dat een website een slotje heeft naast het adres, maar de laatste tijd zegt dat minder over de veiligheid dan vroeger. Het blijft wel zo dat als een website geen slotje heeft langs zijn adres, of het adres begint met <http://> in plaats van met <https://>, dan kan je maar beter een andere winkel zoeken.

De s in <https://> staat voor secure (of beveiligd) en vroeger kon je er vanuit gaan dat als een site zo een adres had en er stond een slotje bij, dat deze site dan legitiem was. Tegenwoordig is dat niet meer zo en duidt het slotje er vooral op dat de gegevens die je naar de website stuurt en/of omgekeerd niet zomaar af te luisteren zijn. We zeggen dan dat de gegevens *versleuteld* verstuurd worden.

 Niet beveiligd | www.vvsg.be/Pages/Home.aspx

De website van de VVSG is dus niet 'onveilig', maar de gegevens die je invoert in bijvoorbeeld formulieren worden leesbaar over het internet gestuurd en kunnen dus door iedereen die meeluistert gelezen worden. Voor login- of bankgegevens wil je dat zeker niet.

Een website die eruit ziet als bol.com maar eigenlijk vals is, kan dus ook een slotje hebben. Vertrouw dus niet op het slotje om in te schatten of een website veilig is of niet. Net zo min je moet vertrouwen op keurmerken zoals AVG-proof, Hacker-safe, enz.

Verzendkosten

Vaak lijkt het alsof iets veel goedkoper is bij de ene aanbieder dan bij de andere. Vergelijk echter niet alleen de prijs van het product, maar vooral de prijs wanneer je gaat afrekenen. Er zijn aanbieders die een product goedkoper aanbieden, maar via de verzendkosten een deel terug proberen te krijgen.

Wees ook aandachtig voor de verzendtermijnen (toch fijn als je het cadeautje met Kerstmis zelf kan afgeven) en voor het retourbeleid.

Laat je niet phoppen



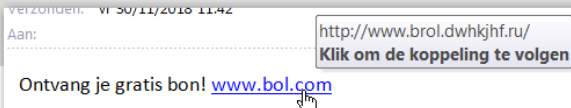
Phishingmails zijn er het hele jaar door, maar rond de Kerstperiode zijn ze specifieker. Ze lijken echt te zijn, maar hebben alleen maar slechte bedoelingen.

Wees daarom deze periode extra voorzichtig, zeker met mails die lijken te komen van grote leveranciers als bol.com, Amazon, bpost, PostNL, UPS, enz. Vooral in deze periode zien we veel mails waarin aangegeven wordt dat er een probleem is met je pakje! Oh nee! Het is verloren geraakt door de staking van bpost, we konden het niet leveren, enz.

Bedenk eerst of je effectief een pakje verwacht. Als dat echt het geval is, surf dan eerst eens rechtstreeks naar de website van de leverancier of bezorgdienst en klik zeker

niet op de links in de mail. Op de echte website kan je ook de status zien van je pakje, of kan je een trackingnummer invoeren. Links in een phishing e-mail kunnen je naar websites sturen die gegevens proberen te stelen of die je proberen te besmetten met een virus. Voor je op een link klinkt, kijk eerst even naar het webadres als je met je muis erover gaat!

Herinner je ook dat een link op een website of in een e-mail uit twee delen bestaat: de tekst die je kan zien en de effectieve link. Om de effectieve link in een e-mail te kunnen zien, ga je met je muiscursor over de link staan **zonder te klikken**. Er verschijnt dan een vakje waarin de echte link weergegeven wordt. Als de tekst 'www.bol.com' is, maar de link gaat naar 'www.brol.dwhkjhf.ru', dan klik je beter niet!



Het gebeurt ook dat men je een compensatie aanbiedt voor de overlast en je moet enkel maar de administratiekosten van een paar cent betalen! Niet doen. En open ook nooit zomaar verdachte bijlages bij een e-mail die je al niet vertrouwt.

Hou je bankrekening in de gaten

Het kan in deze periode geen kwaad om je bankrekeninguittrek eens extra in detail te bekijken. Omdat er rond de Kerst vaak meer uitgaves de revue passeren, kleine en grote bedragen, is het de ideale periode voor criminelen om ongezien een uitgave te kunnen doen in jouw naam. Mochten ze eerder al jouw gegevens te pakken gekregen hebben, dan is het voor hen zeker interessant om daar in deze periode gebruik van te maken.



Mocht je toch iets vreemd opmerken, dan kan je daar best zo snel mogelijk een melding van maken bij je bank en stuur het door naar verdacht@safeonweb.be of indien je effectief geld bent verloren geraakt, doe een aangifte bij de politie.

Meer info en tips kan je ook vinden op <https://www.safeonweb.be>.

"Mooiweervandaag", de stoute neef van het paard van Sinterklaas



Het is geen nieuw fenomeen maar er zijn nog steeds mensen die zich voor de kar van criminelen laten spannen als 'money mule' of 'geldezel'. Zogenaamde 'recruiters' zoeken op social media, via scholen, enz. naar mensen die hun bankrekening, bankkaart en PIN code even willen uitlenen. Deze worden dan gebruikt om crimineel geld door te sluizen.

Ze doen dat meestal in ruil voor geld of luxe-artikelen, waardoor het misschien allemaal nog wat aantrekkelijker lijkt om in het verhaal mee te gaan.

Weet dat de pakkans als 'money mule' erg groot is, omdat de rekening langs waar het geld passeert, op jouw naam geregistreerd is. De politie zal je dus altijd weten te vinden. En er is meer, want als 'moneymule' draai je op voor het volledige bedrag dat langs jouw bankrekening is gepasseerd.

Een gouden raad: laat je nooit overhalen om 'money mule' te worden en geef een onbekende ook nooit toegang tot je bankrekening.

(Via Politiezone Regio Turnhout)

Zorg voor je medemensen

Ook al ben je geen expert, praat ook eens met de oudere generaties in je familie over informatieveiligheid. Wijs hen ook op de mogelijke gevaren van phishing, Microsoft medewerkers met een slecht accent die je opbellen, enz.

Qua inleving kan het zeker ook tellen om je eens in de positie van de veiligheidsconsulent te plaatsen en hen iets te vertellen over wachtwoorden en hoe belangrijk het is om tenminste voor de belangrijke accounts, toch een ander wachtwoord te gebruiken.

Zo kunnen jullie alvast veilig het nieuwe jaar in gaan!

We wensen jullie alvast hele fijne en veilige feesten en een schitterend 2019!

De enige echte privacy Sint!

