



Nieuwsweek

Informatie voor alle ex-medewerkers van GM Belgium en GMASB

Nummer 5/2012

donderdag 15 maart 2012

Leuke tips ingestuurd door ex-collega's.

Rudy Puttenaers stuurde volgende leuke link door... Klik [HIER](#).

Patrick Beulens heeft een vraag voor de ex-collega's...

Beste collega's is het jullie ook al overkomen dat je solliciteert voor een bepaalde job en dat ze je dan uitnodigen op een interim-kantoor om je IN TE SCHRIJVEN en dat je daarna niets meer hoort ik begin stilaan te denken dat ze betaald worden om je IN TE SCHRIJVEN en daarna HOOR JE NIETS MEER.

Zijn er nog collega's die het ook hebben meegemaakt laat het me dan weten aub. Klik [HIER](#).

Marc Cleutjens stuurde onderstaande leerrijke info door...

Gelieve door te sturen? Niet doen! 8 manieren om nepberichten te herkennen.



Als in een mail staat dat je deze moet doorsturen naar x-aantal vrienden, dan is het 99,9% zeker dat het gaat om een nepbericht of 'hoax' in het Engels. Je stuurt de hoax best niét door. Of het nu gaat om een waarschuwing voor een nieuw virus of je een beloning wordt beloofd. Lees alles over de hoax. Alhoewel er nu een virusmelding is die niet nep blijkt te zijn.



Wat is een hoax?

De 'grap-mail' spoort je aan om de mail door te sturen om zoveel mogelijk mensen te informeren.

Een hoax is een e-mailbericht met een nepwaarschuwing (virus) dat zich via jou probeert te verspreiden als een kettingbrief. De 'grap-mail' spoort je aan om de mail door te sturen om zoveel mogelijk mensen te informeren.

Is een Hoax gevaarlijk?

De hoaxes -de valse geruchten, beweringen die niet waar zijn en per e-mail wijde verspreiding vinden-, zijn meestal tamelijk onschuldig. Maar hoaxes zorgen wel vaak voor een zware belasting van de mailservers en grote ergernis bij de mensen die ze ontvangen.

Bovendien kunnen spammers misbruik maken van de grote hoeveelheid geldige e-mailadressen

die ze in deze kettingmails vinden.

Bovendien kunnen spammers misbruik maken van de grote hoeveelheid geldige e-mailadressen die ze in deze kettingmails vinden. Want het aantal mailadressen in een enkel bericht is vaak zeer groot, omdat onervaren gebruikers vaak nalaten om met blind carbon copy (BCC) de ontvangers te anonimiseren.

Of misschien is het wel de bedoeling om spyware te installeren op je pc, een virus te verspreiden of een Trojaans paard binnen te brengen. Denk daaraan voor je een hoax verder doorstuurt.

Herken je deze soorten hoaxes?

1. Je krijgt geld

Het hoax-bericht belooft je geld. Een bekende Hoax is bijvoorbeeld de verdeling van het fortuin van Bill Gates. Hij zou zijn fortuin gaan verdelen en iedereen die de e-mail doorstuurde kreeg meer dan duizend euro, aldus het bericht. Er werd vermeld dat de mail nagekeken zou zijn door een jurist. In een paar doorgestuurde teksten stond dat de afzenders al geld hadden ontvangen.

2. Waarschuwingen voor virussen

In alle gevallen is de boodschap onjuist en kan de verwarring en ook schade enorm zijn.

Sommige berichten waarschuwen dat een bepaald bestand op je computer een virusbestand zou zijn. Het zet de gebruikers aan om belangrijke bestanden van hun computer te verwijderen. Zoals: -"Indien het bestand C:\windows\example.dll bestaat, verwijder dit dan onmiddellijk!". De bestanden die hierin genoemd worden zijn vaak bestanden die nodig zijn voor het goed functioneren van Windows of andere veel gebruikte software zoals Office.

Ook het bericht 'jdbmgr.exe' roept op tot het verwijderen van een Windows bestand. Een bestand dat zeker nodig is voor het gebruik van bepaalde onderdelen van Windows.

In alle gevallen is de boodschap onjuist en kan de verwarring en ook schade enorm zijn.

3. Je krijgt gratis geschenken

Bij sommige berichten wordt een bekend bedrijf betrokken dat je gratis producten belooft. Een bekend gsm-bedrijf gaat je bijvoorbeeld gratis de nieuwste gsm opsturen. Daarvoor

moet je dan wel het bericht naar het gsm-bedrijf terugsturen én doorzenden naar ten minste 10 personen. De auteur van dit bericht heeft eigenlijk de bedoeling de server van het gsm-bedrijf plat te leggen. Dat wordt veroorzaakt door de massale toezending van mails van mensen die zo'n gratis gsm wel zien zitten.

Maar die gsm kan je natuurlijk wel op je buik schrijven... Want dit soort mails zijn altijd bedrog en louter spam. Een bedrijf zal nooit een toestel gratis weggeven als je een e-mail doorstuurt naar een x-aantal vrienden. Als je toch twijfelt, check je best de officiële website van de fabrikant die in zo'n kettingmail wordt vermeld, voor je je adresboek ermee lastig valt.

Een waarschuwingsmail krijgen van een plaatselijke politiecommissaris over bijvoorbeeld de

allernieuwste, elektronische inbraakmethodes.

4. **Je krijgt een waarschuwing**

Je kan ook een waarschuwingsmail krijgen van een plaatselijke politiecommissaris over bijvoorbeeld de allernieuwste, elektronische inbraakmethodes. Je bent geschokt en stuurt de e-mail naar familie en vrienden. Eén telefoontje naar de bewuste politiedienst zal je echter leren dat het bericht volledig uit de lucht is gegrepen.

5. **Je krijgt een vraag om solidariteit**

Een ander soort mail die vaak voorkomt is de solidariteitsmail. Je krijgt de vraag of je een stel jonge hondjes aan een goede thuis wilt helpen. Een onweerstaanbaar schattige foto van die allerliefste puppy's overtuigt je wel.

De meeste doeltreffende solidariteitsmail is wel de vraag om een zwaar ziek kindje te steunen en bijvoorbeeld een operatie mogelijk te maken. Wie is daar nu niet gevoelig voor? En het kost je niets, gewoon het bericht verder sturen naar zoveel mogelijk personen. Een internetprovider sponsort immers het zieke kind met 1 euro per verstuurd bericht...

Dit is een wel erg flauwe grap. Maar met een grote vangst aan geldige e-mailadressen.

Wat je moet doen? Absoluut niets!

Al wat je moet doen, is deze mails negeren, verwijderen, en zeker niet doorsturen naar je adresboek.

Sommige hoaxes zijn al jaren in omloop. Vaak worden ze enkele keren opnieuw in omloop gebracht met een iets actuelere inhoud. Voor meer voorbeelden kan je een kijkje nemen op www.VirusAlert.nl.

Draag niet bij aan de verspreiding van hoaxes. Met deze 8 tips herken je ze!

8 tips om een hoax te herkennen

1. **Massaal doorsturen**

Een typisch kenmerk van een hoax is dat je gevraagd wordt om de mail zo snel mogelijk en naar zoveel mogelijk mensen door te sturen. Hiervoor doen de bedenkers van de hoax een beroep op typisch menselijke eigenschappen, zoals naastenliefde (voor een ziek klein meisje dat dringend een operatie nodig heeft), hebzucht (stuur deze mail naar x aantal personen en ontvang binnen de maand 10.000 euro) en angst (voor een super gevaarlijk virus dat nog maar pas ontdekt is en heel je pc kan wissen).

2. **SCHREEUWERIG!!!**

Net als bij veel spamberichten herken je in de hoax vaak hoofdletters, uitroeptekens en allerhande superlatieven waarmee de verspreider zijn boodschap kracht wil bijzetten. Een zin als "OPGELET!!! UITERST GEVAARLIJK VIRUS IN OMLOOP!!!" zou dus al meteen een belletje moeten doen rinkelen.

3. **Vage autoriteit**

Vaak worden internetproviders, gsm-operatoren of andere bekende bedrijven (IBM, Microsoft, Symantec) te pas en te onpas genoemd als referentie, om de dreiging of de belofte geloofwaardiger te maken.

Concrete gegevens, zoals een naam, een e-mailadres, een website of een link naar een persbericht waar je een en ander kan verifiëren, zal je niet snel aantreffen.

4. **Geen datum**

Om hun hoax zolang mogelijk in omloop te houden, zullen de verspreiders geen exacte datum in hun oorspronkelijke boodschap steken, maar deze eerder vaag houden.

Als je dus iets leest als "Ik hoorde het vanmorgen op CNN", "Microsoft liet gisteren weten dat..." of "Het virus is pas ontdekt", mag je er vrij zeker van zijn dat je met een hoax te maken hebt.

5. **Van wie komt de mail?**

Vaak krijg je dergelijke mails toegestuurd door een familielid, een collega of een vriend. En dan kan je je terecht afvragen: "Hoe komen zij in hemelsnaam aan deze informatie, terwijl er elders nog niks over te lezen of te horen valt?"

Als de dreiging echt zo groot zou zijn als wordt beweerd, zou de overheid hier wel over berichten, en zouden de media zich er massaal op storten. Komt de mail anderzijds van je kennis bij de Clickx-redactie, dan zou het wel eens waar kunnen zijn - al is dat ook geen garantie.

6. **Hoelang is de mail al in omloop?**

Wanneer mensen de hoax te goeder trouw doorsturen naar al hun contacten, plakken meestal ook de voorgaande mails er nog onder. Scroll je helemaal naar beneden, en zie je dat de oorspronkelijke mail al dateert van meer dan 6 maanden geleden, dan zal het allemaal wel niet zo dringend zijn als in de boodschap beweerd wordt.

7. **Verouderde informatie**

Sommige van deze nepmails durven na enkele jaren wel eens opnieuw opduiken, al dan niet in een licht gewijzigde vorm. Soms vergeten de verspreiders echter om de gegevens in de hoax te updaten, waardoor er verwezen wordt naar bedrijven die niet meer bestaan, of wordt er een toestel beloofd dat al lang uit de handel is.

8. **Gezond verstand**

Tot slot raden we je aan om je gezond verstand te gebruiken. Als er in de mail beloftes gedaan worden die te mooi lijken om waar te zijn, dan zijn ze in 99 % van de gevallen ook niet waar.

Toch zullen er altijd mensen zijn die hier met beiden voeten in trappen.

Activiteiten

Op woensdag 18 april komen de ex-collega's weer samen in Kapellen, alle verdere info vind je op de website.

Kaart,- & praatnamiddag te Brasschaat, donderdag 29/3/2012 om 13u00, meer info vind je op de website.

Nieuwe activiteit...

Wie heeft er nog een leuk idee om een activiteit te organiseren? Ik krijg meer en meer de vraag om eens iets te plannen voor alle ex-collega's. Voor alle zal wel niet lukken maar ik wil wel eens kijken hoeveel er zouden meedoen als er echt een leuk initiatief word aangeboden, dus degenen die een leuk voorstel hebben laat het me maar weten...
