

Ransomware

Waarom?

Ransomware is helaas aan de orde van de dag. Wij zien echter met de dag een toename in het aantal pogingen tot verspreiding hiervan. En helaas neemt dus ook het aantal besmettingen hiermee toe. Met deze pagina willen wij u proberen zo goed mogelijk te waarschuwen. Neem dan ook even 5 minuten om dit aandachtig te bekijken, dit kan u een grote schadepost schelen.

Wat is Ransomware?

Ransomware is een vorm van malware welke bestanden op de computer gijzelt. Het kan hierbij gaan om bestanden op de computer zelf, maar ook op het netwerk en externe disks als usb en in de cloud. Het doel hiervan is dat er vervolgens geld moeten worden betaald om een sleutel te verkrijgen om deze bestanden weer 'schoon' te maken.

De besmetting vindt plaats via verschillende manieren. Het grootste deel komt binnen via e-mail waarin een bijlage zit of een link naar een website waar vervolgens automatisch een stukje software wordt gedownload. We zullen op deze pagina proberen wat meer duidelijkheid te geven om zo de signalen van 'foute boel' te herkennen.

Voorbeeld e-mail

Besmetting verloopt meestal via besmette bestanden, bijvoorbeeld een e-mailbijlage of via een lek op de pc door niet-geüpdatete software. Hieronder is e-mail dat voor een recente infectie heeft gezorgd.

Middels deze e-mail willen ze op de "Download Factuur" URL-snelkoppeling laten klikken dat uw browser naar een malafide website zal laten doorsturen. De malafide website serveert u vervolgens één van de volgende bestanden:

- Een .ZIP bestand
 - Hier zit meestal een uitvoerbaar bestand in dat voor de uiteindelijke infectie zorgt. Vaak heeft het uitvoerbaar bestand het volgende logo:

- Een .RAR bestand
- Een .EXE bestand
- Een .XLSX bestand
- Een .DOC bestand

Voorbeeld mail Centraal Justitieel Incassobureau (CJIB)



Centraal Justitieel Incassobureau
Ministerie van Veiligheid en Justitie

AFZ: POSTBUS 1794, 8901 CB, LEEUWARDEN

CJIB-nummer
6714 9293 8517 3894

Verstuurd op
12-08-2017

verkeersboete aanmaning

Direct door u te betalen
€ 90,00

Dit bedrag is inclusief €9,00
administratiekosten.

Als u niet op tijd betaalt,
wordt de boete hoger.

Bedrag na 1e verhoging	€ 126,00
Bedrag na 2e verhoging	€ 231,00

Geachte Marleen Oldenhave,

Er is met uw voertuig een verkeersvoorschrift overtreden. Hiervoor is een administratieve sanctie opgelegd. Het kenteken staat volgens het kentekenregister op uw naam of u was op het moment van de overtreding de huurder van het voertuig. Ondanks de eerder verstuurde beschikking hebben wij geen betaling ontvangen. U ontvangt daarom deze aanmaning.

Informatie over de overtreding en de opgelegde administratieve sanctie:

Feltoede:	VA010
Gemeente:	Nieuwegein
Plaats:	Nieuwegein
Locatie:	STRUCTUURBAAN
Datum:	11-07-2017
Tijdstip:	17:10 uur
Toegestane snelheid:	50 km/h
Gemeten snelheid:	65 km/h
Gecorrigeerde snelheid:	62 km/h
Fotofilmnummer:	10084700584

Het volledige bedrag van € 90,00 moet uiterlijk 04-09-2017 zijn bijgeschreven op rekeningnummer van het Centraal Justitieel Incassobureau (CJIB).

U kunt de administratieve sanctie direct betalen via iDeal. Klik hiervoor op de onderstaande knop:



Direct betalen via iDeal →

Als u het niet eens bent met de opgelegde sanctie dan kunt u schriftelijk beroep instellen bij de officier van justitie. U bent niet verplicht het volledige bedrag te betalen, zolang uw beroepschrift in behandeling is. De beroepstermijn eindigt op 04-09-2017. Stuur uw beroepschrift voor deze datum naar: Postbus 1794, 8901 CB, Leeuwarden.

Hoogachtend,

Centraal Justitieel Incassobureau

Voorbeeld mail T-Mobile

Van: "T-mobile" <bestreserver@skallionhotel.com>

Datum: 1 november 2016 11:07:06 CET

Aan:

Onderwerp: Uw nieuwe factuur



Uw nieuwe factuur

Uw nieuwe factuur staat klaar op My T-Mobile.

Het factuurbedrag is € 258,56.

Bijzonderheden bij deze factuur

- ✓ U heeft op 15/09/2016 gebeld naar een servicenummer. Op deze factuur betaalt u daarvoor € 55,15 (exclusief BTW) gebruikskosten. Het gesprek naar dit servicenummer viel voor een deel of volledig buiten uw bundel/tegoed. Meer weten over servicenummers op uw factuur? [Ga naar onze website](#) >
- ✓ U heeft uw abonnement gebruikt in het buitenland. Op deze factuur betaalt u daarvoor in totaal € 191,33 (inclusief BTW). Meer details over de gesprekken en sms'jes ziet u op uw specificatie. Zie ook t-mobile.nl/buitenland voor informatie over de tarieven.
- ✓ Op deze factuur zijn gebruikskosten in rekening gebracht voor de datum 15/09/2016. Deze kosten hadden eigenlijk al op een eerdere factuur moeten staan, maar wij konden ze pas later verwerken in onze systemen. Onze excuses voor de onduidelijkheid.

Uw gespecificeerde factuur kunt u bekijken op My T-Mobile.

[Bekijk uw factuur](#)

Heeft u nog geen My T-Mobile account? Dan kunt u zich via onderstaande link registreren.

[Registreer voor My T-Mobile](#) >

Afschrijving

Het bedrag van € 258,56 wordt omstreeks **01/11/2016** van uw rekening afgeschreven.

Voor vragen over uw factuur, ga naar t-mobile.nl/facturen.

Met vriendelijke groeten,

T-Mobile

Heb je nog vragen?

Je kan ons ook bereiken via de onderstaande kanalen.

[Twitter](#) [Facebook](#) [Google+](#) [Forum](#) [Over T-Mobile](#)

N.B.: op (de inhoud van) deze e-mail is een DISCLAIMER met belangrijke VOORBEHOUDEN van toepassing: zie <http://www.t-mobile.nl/disclaimer>

This e-mail and its contents are subject to a DISCLAIMER with important RESERVATIONS: see <http://www.t-mobile.nl/disclaimer>

Voorbeeld mail Ziggo

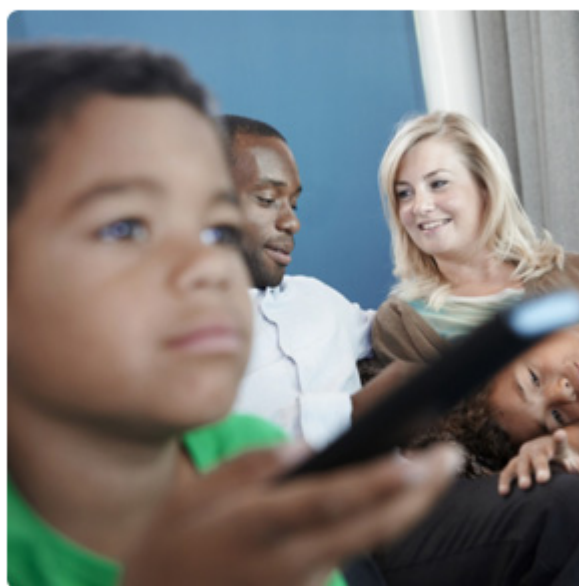


Je nieuwe factuur staat klaar

Totaalbedrag:

€ 127,27

[Factuur bekijken](#)



Je nieuwe factuur staat klaar in [Mijn Ziggo](#). Het gaat om een bedrag van € 127,27. Betaal je via automatische incasso? Dan schrijven wij dit bedrag aan het eind van de maand van je rekening af. Als je nog een bedrag tegoed hebt van Ziggo, dan verrekenen wij dit voordat we van je rekening afschrijven. De automatische incasso is dan voor een lager bedrag dan het totaalbedrag van de factuur. Je hoeft niets te doen, wij regelen dat voor jou.

Alle antwoorden op een rij

Is het factuurbedrag hoger dan verwacht? Of wil je je wachtwoord voor Mijn Ziggo opvragen? Wij hebben de antwoorden op een aantal veelgestelde vragen voor je op een rij gezet.

[Veelgestelde vragen](#)



Kies voor Mijn Ziggo

Meer dan 90% van onze klanten kiest voor Mijn Ziggo. Ook het gemak van Mijn Ziggo ervaren? Met een paar muisklikken vraag je [toegang](#) aan. Houd hiervoor je klantnummer 97372782 bij de hand.

Nog een vraag?

Wij staan [online](#) dag en nacht voor je klaar met handige oplossingen op maat en slimme stappenplannen voor bijvoorbeeld installaties. Daarna nog een vraag? Of bel je liever? [Bekijk](#) onze contactgegevens en openingstijden.

Fijne dag,

Ruben Uppelschoten

Diensten Klantenopvang

Voorbeeld mail KPN



Geachte [REDACTED]

Deze maand is uw factuur in totaal € 581,27. De specificaties van de factuur vindt u in de bijlage.

[Downloaden Factuur](#)

[Overzicht van al uw facturen in MijnKPN](#)

Wilt u een overzicht van al uw facturen of uw persoonlijke instellingen bekijken? Klik dan [hier](#) om naar MijnKPN te gaan. Dit is uw persoonlijke en beveiligde KPN omgeving.

[Uitleg van uw factuur](#)

Klik [hier](#) voor uitleg over uw factuur.

[Veelgestelde vragen](#)

Hebt u nog vragen over uw factuur en de betaling ervan, kijk dan op kpn.com/factuur. Hier vindt u informatie over veelgestelde vragen zoals: de opbouw van de factuur, de betalingsmogelijkheden, de factuur online bekijken en hoe u wijzigingen doorgeeft.

Met vriendelijke groet,

Bob Mols

Directeur Klantenservice

N.B. dit is een automatisch verzonden e-mail, het is niet mogelijk deze e-mail te beantwoorden.

Kent u KPN Compleet al? Hoe meer u combineert, hoe meer voordelen u krijgt. Kijk voor meer informatie op kpn.com/krijgmeer

De KPN Compleet voordelen zijn:



Voorbeeld mail ICS Visa Card Services

Geachte ICS klant,

Dit is uw officiële mededeling dat de hieronder vermelde dienst (en) worden gedeactiveerd en verwijderd als je profiel niet wordt geverifieerd. vorige mededelingen zijn verstuurd naar de contactpersoon van uw toegewezen account.

U bent verplicht om onze online validatie formulier in te vullen door te klikken op de volgende link.

[Klik hier om het online formulier te openen](#)

Opmerking: deze beveiligingsmaatregel is bedoeld om uw persoonlijke informatie te beschermen tegen onrechtmatig gebruik door anderen.

Gelieve alle gegevens correct in te vullen om blokkering van uw rekening te voorkomen.

Hoogachtend,

Gert-Jan Pieters
Directeur ICS Klantenservice

International Card Services BV
Wisselwerking 32
1112 XP Diemen
Postbus 23225
1100 DS Diemen

Bevestiging blokkade

Geachte kaarthouder,

Hierbij bevestigen wij dat uw huidige kaart uitgegeven door de International Card Services BV tijdelijk geblokkeerd is.

Wij hebben uw kaart geblokkeerd, omdat wij een nieuwe beveiligingssoftware (CCS) hebben ingevoerd. Met deze nieuwe beveiligingssoftware willen wij misbruik van creditcards bestrijden.

Om de blokkering op te heffen dient u de onderstaande stappen te hanteren.

1. [Direct inloggen op Mijn ICS](#)
2. Vul uw gegevens nauwkeurig in.
3. Bevestig de verificatie met de gegevens die bij ons bekend staan.

Let op! Uw kaart zal niet bruikbaar zijn voor o.a. transacties en/of geld opnames, totdat deze weer geverifieerd is.

Met vriendelijke groet,
International Card Services BV

Uw creditcard wordt uitgegeven door International Card Services BV (ICS).

Let op! Ga voorzichtig om met uw persoonlijke gegevens. Medewerkers van ICS zullen nooit naar uw gebruikersnaam, wachtwoord en/of pincode vragen. Niet via e-mail, telefoon of op welke andere manier dan ook.

Dit bericht is verzonden door International Card Services BV, gevestigd aan de Wisselwerking 32 te (1112 XP) Diemen, ingeschreven in het Handelsregister Amsterdam onder nummer 33.200.596.

This message has been sent by International Card Services BV, which has its seat at Wisselwerking 32 (1112 XP) Diemen, the Netherlands, and is registered in the Commercial Register of Amsterdam under number 33.200.596.

Wat als eerste opvalt is dat de tweede alinea een taalfout bevat. Dit moet al argwaan wekken. Verder kunt u zien dat de link naar een vreemde site leidt. Dit kunt u zien in de onderstaande screenshot. Het is van belang dat u **NOOIT** klikt op zo'n link.

Geachte ICS klant,

Dit is uw officiële mededeling dat de hieronder vermelde dienst (en) worden gedeactiveerd en verwijderd als je profiel niet wordt geverifieerd. vorige mededelingen zijn verstuurd naar de contactpersoon van uw toegewezen a

U bent verplicht om onze online validatie te klikken op de volgende link.

<http://xtwfluaeqr.conectarsediariosustentable.com/international/ics/>
Click to follow link

[Klik hier om het online formulier te openen](#)

Opmerking: deze beveiligingsmaatregel is bedoeld om uw persoonlijke informatie te beschermen tegen onrechtmatig gebruik door anderen.

Poging tot online betaling met uw Card

Geachte heer/mevrouw,

Hiermee willen wij u vermelden dat er mogelijk is geprobeerd een online betaling te verrichten met uw Card.

Tevens is deze betaling niet gelukt omdat enkele gegevens onjuist waren. Hierdoor hebben wij uw creditcard rekening & Mijn Card Online tijdelijk in een beperkte omgeving geplaatst. Dit doen wij voor uw veiligheid, totdat u uw gegevens heeft geverifieerd kunt u geen betalingen verrichten met uw huidige Card.

Als uw gegevens correct zijn geverifieerd zullen wij alle gezette beperkingen opheffen. ICS wil haar cliënt erop attenderen haar gegevens zo spoedig mogelijk te verifiëren om weer volledig gebruik te kunnen maken van alle diensten die International Card Services BV verleent.

U dient op de gegeven link te klikken om deze verificatie te starten: > [Mijn Card activatie procedure](#) <

Met vriendelijke groet,

International Card Services BV

Uw Card wordt uitgegeven door International Card Services BV (ICS).

Let op! Ga voorzichtig om met uw persoonlijke gegevens. Medewerkers van ICS zullen nooit naar uw gebruikersnaam, wachtwoord en/of pincode vragen. Niet via de e-mail of telefoon.

Dit bericht is verzonden door International Card Services BV, statutair gevestigd aan de Wisselwerking 32 te (1112 XP) Diemen, ingeschreven in het Handelsregister Amsterdam onder nummer 33.200.596.

This message has been sent by International Card Services BV, which has its seat at Wisselwerking 32 (1112 XP) Diemen, the Netherlands, and is registered in the Commercial Register of Amsterdam under number 33.200.596.

----- Oorspronkelijk bericht -----

Van: "ICS.nl" <zangaram@duq.edu>

Datum: 09-12-16 09:42 (GMT+01:00)

Aan:

Onderwerp: Vernieuwde Update Mijn ICS



INTERNATIONAL CARD SERVICES

Geachte heer/mevrouw,

Uw Mijn ICS is momenteel op non-actief gesteld omdat er inactiviteit werd geconstateerd.

U kunt momenteel niet inloggen op uw Mijn ICS.

[Klik hier om uw Mijn ICS actief te maken](#)

Hoogachtend

International Card Services | Bond van de Nederlandse Banken

Voorbeeld mail ING Bank

Van: ING <noreply@ing.email.nl>
Datum: 8 augustus 2016 01:40:17 CEST
Aan: [REDACTED]
Onderwerp: Nieuwe betaalpas aanvragen
Antwoord aan: <noreply@ing.email.nl>



Er staat een nieuwe betaalpas voor u klaar.
Uw betaalpas word per 10 augustus geblokkeerd.

Geachte klant,

Hierbij willen wij u de nieuwe betaalpas introduceren. De nieuwe betaalpas is beter beveiligd tegen frauduleuze praktijken en voldoet zich aan de Europese veiligheidsvoorschriften betreffend bankzaken. Wij bieden onze klanten een zo veilig mogelijke virtuele omgeving aan om bankzaken te doen met maximaal gebruiksgemak. Onze oude betaalpas speelt hierbij een belangrijke rol, maar biedt niet altijd de flexibiliteit en gebruiksvriendelijkheid aan die we voor onze klanten nastreven.

Onze nieuwe betaalpas maakt gebruik van nieuwe technologie en biedt nu en in de toekomst meer mogelijkheden. Op dit moment is skimming en misbruik van betaalpassen een groot probleem voor het ING. De schade van de opgenoemde onderwerpen is op dit moment heel hoog. Wij als bank willen dit probleem oplossen door middel van verschillende nieuwe functies. Op dit moment is dat alleen mogelijk met een nieuwe betaalpas die hier wel tegen gewapend is. De chip van onze nieuwe betaalpas bevat een AES-256 encryptie en NFC-2 chip die het skimming probleem volledig oplost. dit is in een nieuwe omgeving ontwikkeld die samen met het contactloos betalen werkt. Deze omgeving is volledig beveiligd tegen frauduleuze transacties en zal in uw nieuwe betaalpas worden inbegrepen.

De nieuwe Mijn ING omgeving functioneert alleen op de nieuwe betaalpas. U kunt hieronder de aanvraag voor deze nieuwe betaalpas voltooien, deze aanvraag is tot **10 augustus** volledig gratis. U kunt hieronder de aanvraag voor de nieuwe betaalpas voltooien. Via het onderstaande formulier moet u uw gegevens bevestigen, nadat u dit heeft gedaan zal de aanvraag voor uw nieuwe betaalpas gestart worden. Na het voltooien van uw aanvraag, ontvangt u uw nieuwe betaalpas met de bovengenoemde functies binnen 2 tot 3 werkdagen thuis. Vanwege de vele aanmeldingen kan het zo zijn dat uw nieuwe betaalpas vertraging oploopt met de bezorging.

Vervang uw bankpas

Wij vertrouwen erop u hiermee voldoen te hebben geïnformeerd en van dienst te zijn geweest. Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groeten,

Willem van Trotshoud
ING Groep N.V.

Voorbeeld mail PostNL

Van: PostNL <jouw-postnl@t-online.de>
Verzonden: dinsdag 6 september 2016 10:10
Aan: [afgeleverd]
Onderwerp: De levering van een pakket op uw adres is mislukt



Geachte klant,

Onze pakketbezorger heeft op 03-09-2016 om 13:00 op uw adres een pakket geprobeerd af te geven. Er was helaas niemand aanwezig om het pakket in ontvangst te kunnen nemen.

Het pakket afhalen op het postkantoor

<http://urls.nycker.net/udG81>
Ctrl+klik of tik om de koppeling te volgen

Het aangetekende pakket ligt klaar op het postkantoor. [Klik hier](#) om uw track & trace informatie te downloaden. Print deze uit en neem deze mee naar het postkantoor. Vergeet niet om een geldig identiteitsbewijs mee te nemen. Uw pakket wordt 14 dagen na dagtekening terug naar de afzender gestuurd.

Met vriendelijke groet,
PostNL Klantenservice

Voorbeeld mail ABN AMRO

Van: ABN AMRO [mailto:kbc@kbc-mailing.be]

Verzonden: dinsdag 9 augustus 2016 14:40

Aan:

Onderwerp: ABN AMRO Bankkaart beveiliging



ABN·AMRO Bank

Geachte ABN AMRO Klant,

We hebben onlangs een melding ontvangen waaruit blijkt dat er is geprobeerd in te loggen met een buitenlandse IP op uw bankrekening.

Hierom hebben wij de benodigde maatregelen genomen om uw betaalrekening optimaal beveiligen, en gaan wij uw oude bankkaart vervangen met een nieuwe beveiligde bankkaart.

Dat gaat als volgt:

1 Uw dient uw oude bankkaart(en) op te sturen naar

Tnv: ABN AMRO Recycle-Punt

Adres: NOLENSSTR 43

1067 JW AMSTERDAM

2 Om het proces af te ronden dient u op de onderstaande link te klikken

[Aanvraag afronden](#)

Vervanging bankkaart is geheel gratis.

U bankkaart wordt milieuvriendelijk vervangen.

Voor 18:00 uur op de post. Ontvangt u uw nieuwe bankkaart de eerstvolgende werkdag. (na ontvangst van u oude bankkaart)

Let op: Na 15 augustus 2016 kunt u geen gebruik maken van uw oude bankkaart.

Indien u vanaf de genoemde datum nog steeds uw oude bankkaart in bezit heeft wordt ook uw ABN AMRO-Online Internetbankieren geblokkeerd.

Met vriendelijke groet,

ABN AMRO Fraudehulpdesk

Voorkomen beter dan genezen

Wellicht is dit iets waarvan u denkt dat dit voor de hand ligt. Maar toch is het eerste **Gebruik uw gezond verstand.**

- Verwacht u e-mail van deze partij?
- Is deze manier van communicatie gebruikelijk voor de partij waarmee u zaken doet?
- Komt de mail vanuit de quarantaine, behandel deze dan ook als 'verdacht'. Ga hier extra voorzichtig te werk.

Als er een link in een bestand zit controleer deze dan eerst voor hier gelijk op te klikken.

Een link bestaat uit 2 delen.

- De display tekst. Dit is de naam die u ziet staan. In ons voorbeeld is dit <http://www.google.nl>
- De link. Dit is de daadwerkelijke website waar je naartoe gaat wanneer je hier op klikt

Deze kan dus verschillen.

Hoe kun je dit zien?

- Ga met uw muis op de link staan en klik hier dus **NIET**
- Vervolgens zal de daadwerkelijke link zichtbaar worden
- Wat je zult zien is dat deze verwijst naar een compleet andere website als de tekst welke zichtbaar is

Hieronder een plaatje wat u ziet wanneer u dit doet.



<http://www.infotheek.com/services>
Click to follow link

Klik hier voor uw factuur <http://www.google.nl>

Wanneer u nu op deze link zou klikken wordt u dus daadwerkelijk naar de site van Centralpoint gestuurd in plaats van de te verwachten google.nl

Bij twijfel vraag uw collega om mee te kijken, vraag de versturende partij of het correct is of neem contact op met de servicedesk van Centralpoint.

Preventieve maatregelen

Indien u ondanks dit alles toch wordt getroffen is eigenlijk de enige juiste methode om uw data terug te krijgen een restore vanuit de back-up. Dus het eerste punt:

Zorg voor een goed werkende back-up

De overige punten kunnen helpen om het buiten de deur te houden:

- Spamfilter, deze scant uw e-mail voordat dat deze bij u aankomt en verwijderd de op dat moment bekende Spam / Ransomware mails
- Firewall, op verschillende lagen wordt het verkeer geïnspecteerd en waar nodig geblokkeerd
- Anti-virus, zorg voor een goedwerkende anti-virus.
- Updates, zorg er voor dat u altijd bij bent met de beveiligings updates van Microsoft.

Dit alles samen zorgt voor een zo optimaal mogelijke beveiliging. Hou hierbij in gedachten dat 100% tegengaan een illusie is. De preventie loopt altijd achter de maker aan.

Toch besmet?

Als u onverhoopt toch besmet raakt, twijfel geen seconde en haal de bron pc gelijk los van het netwerk of schakel hem gelijk uit en neem contact op met de Servicedesk van Centralpoint.

Hoe eerder dit gedaan is, hoe kleiner de schade zal zijn.

Voorbeelden

Hieronder proberen we voorbeelden te blijven plaatsen van foute berichten.

Afzender: La Tulipe Bv, Fanfan,

Mailadres: j-skroblin@t-online.de

Beste support,

Dit is een vriendelijke herinnering over uw openstaande saldo , wat binnenkortverschuldigd is. Raadpleeg de bijgevoegde factuur voor meer details.

Ordernummer: **#J100391724**

Vervaldatum: **10-jun-16**

Totale order: **1,998.00 €**

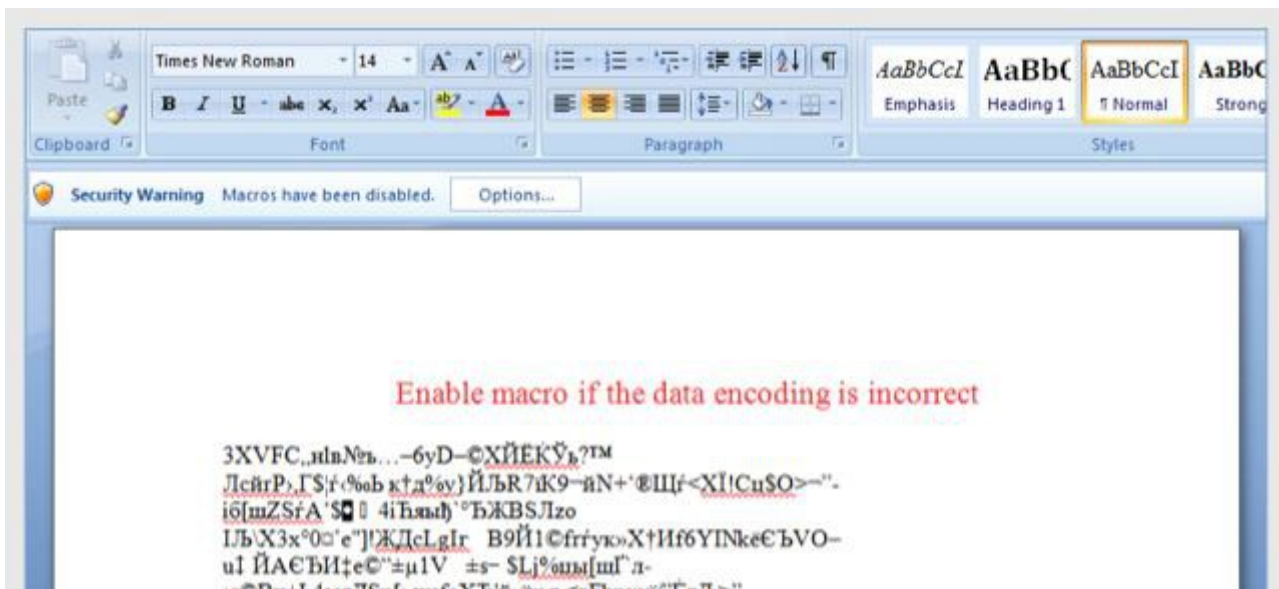
We doen graag zaken met u! La Tulipe Bv, Fanfan, VUYK ENGINEERING. Borneostraat 9 Baarn 3742 DA Baarn 3742 DA +31183449030

Bijlagen :

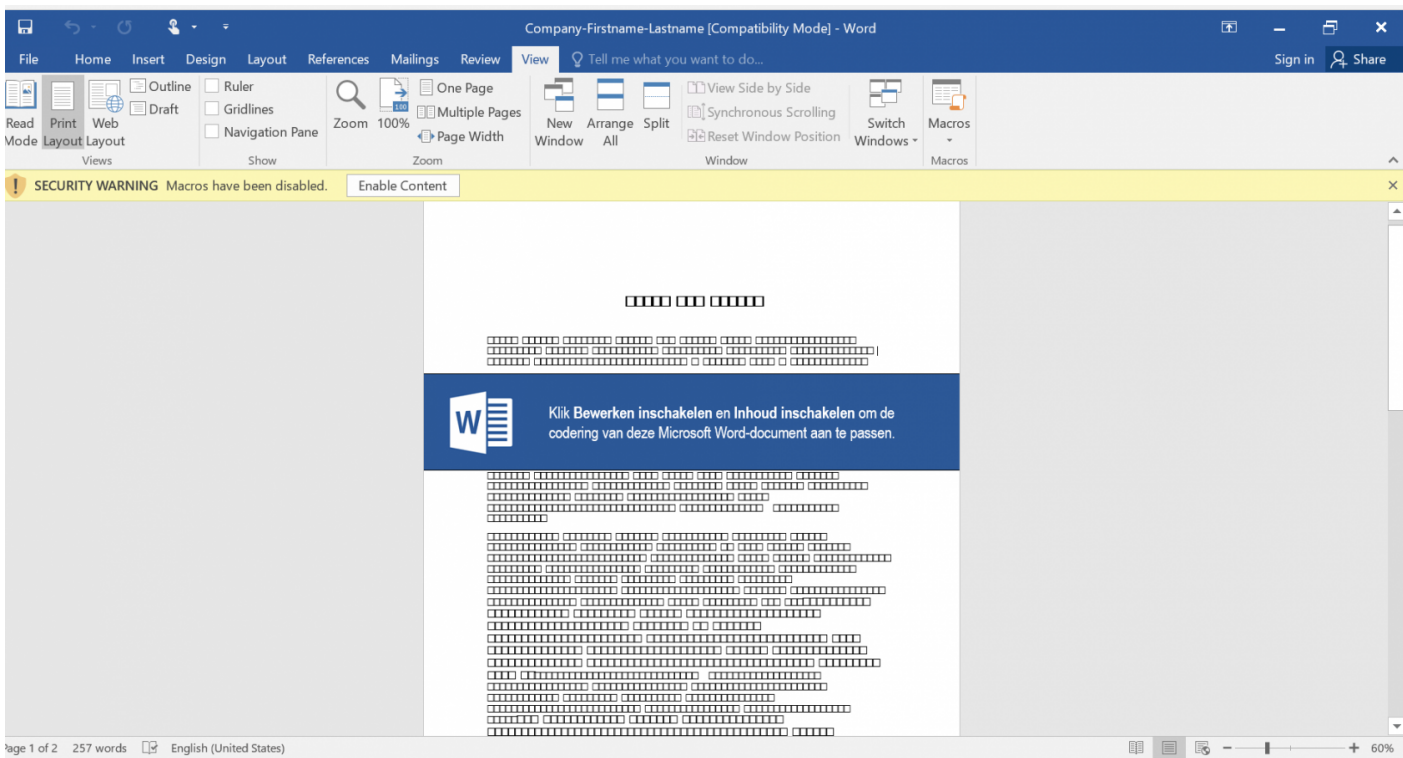
 support_factuur(vs9705).doc (65.80 KB)

Hier ook een voorbeeld van hoe een word document er uit ziet. Schakel dus **NIET!!** de macro's in!

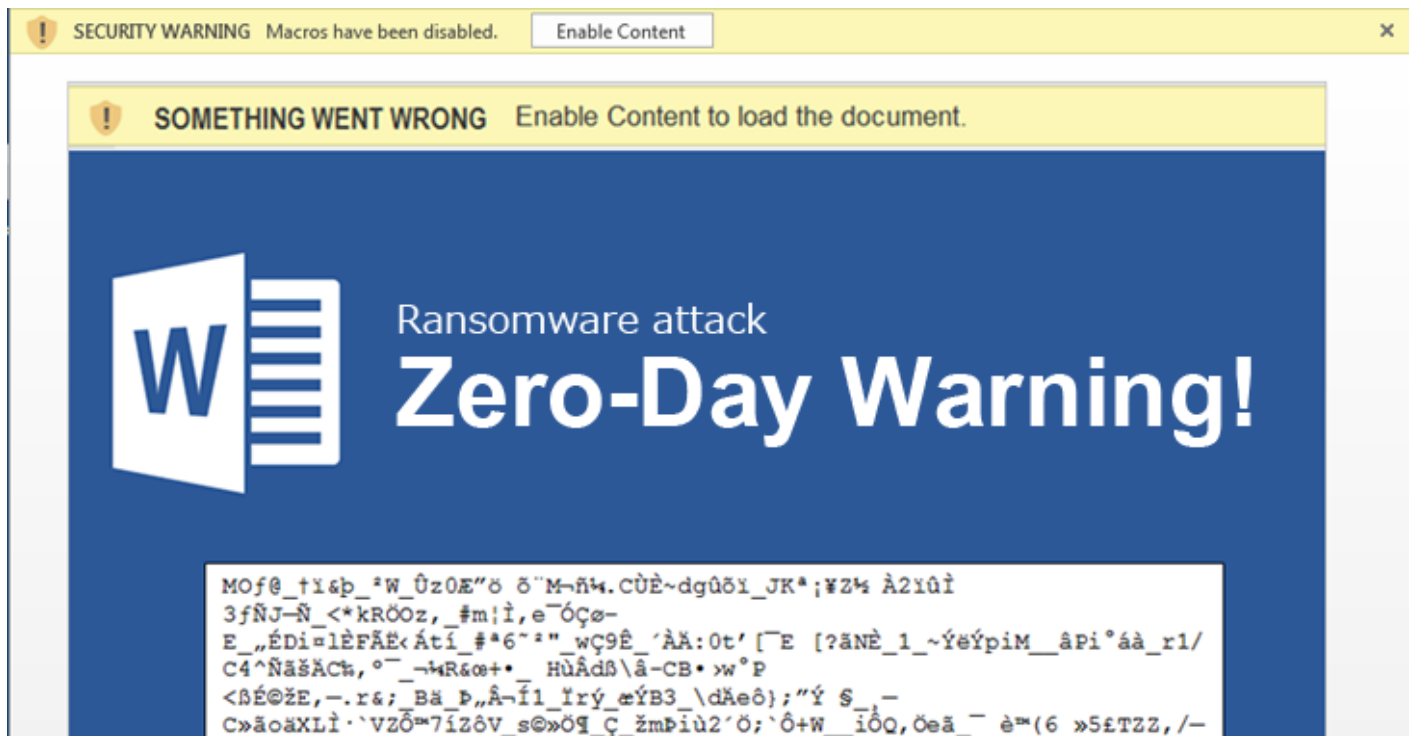
Doe je dit wel, neem dan direct contact op. Op dat moment wordt het proces gestart welke de bestanden versleuteld of bankgegevens verzameld.



NL versie:



Hier een voorbeeld van een mail welke voornamelijk gericht is op Office365 gebruikers:



Revision #3

Created 26 September 2019 08:42:43 by Servicedesk

Updated 11 October 2019 10:57:46 by Servicedesk