



WELKOM



Huis en veiligheid

Programma

- Welkom door Yvonne Schouten
- Wat doe jij bij brand door Susanna Mastenbroek?
- Oplichters via internet door Michel Hogendoorn
- WAS: veiligheid in de wijken door Amber Hagebeek
- Pauze
- Discussie in groepjes
- Afsluiting door Yvonne Schouten



Susanna Mastenbroek



Programma;

- Oorzaken van brand, wat is brand
 - Veilig laden, telefoon/e-bike
 - Belang van rookmelders en waar hang ik ze op
 - Wat te doen bij brand > vluchten
 - Alarmeren hoe doe je dat
 - Scootmobielen
 - Koolmonoxide (als er nog tijd is)
 - Vragen
- 

Oorzaken van brand:



=



Vlam in de pan, tips:

- Gebruik NOOIT water om te blussen!
- Warmtebron uitschakelen (gas/elektra/keramisch/inductie)
- Afzuigkap uitzetten
- Leg een passende deksel, van u af, op de pan
- Pan minstens een uur laten staan om af te koelen
- Brandweer bellen

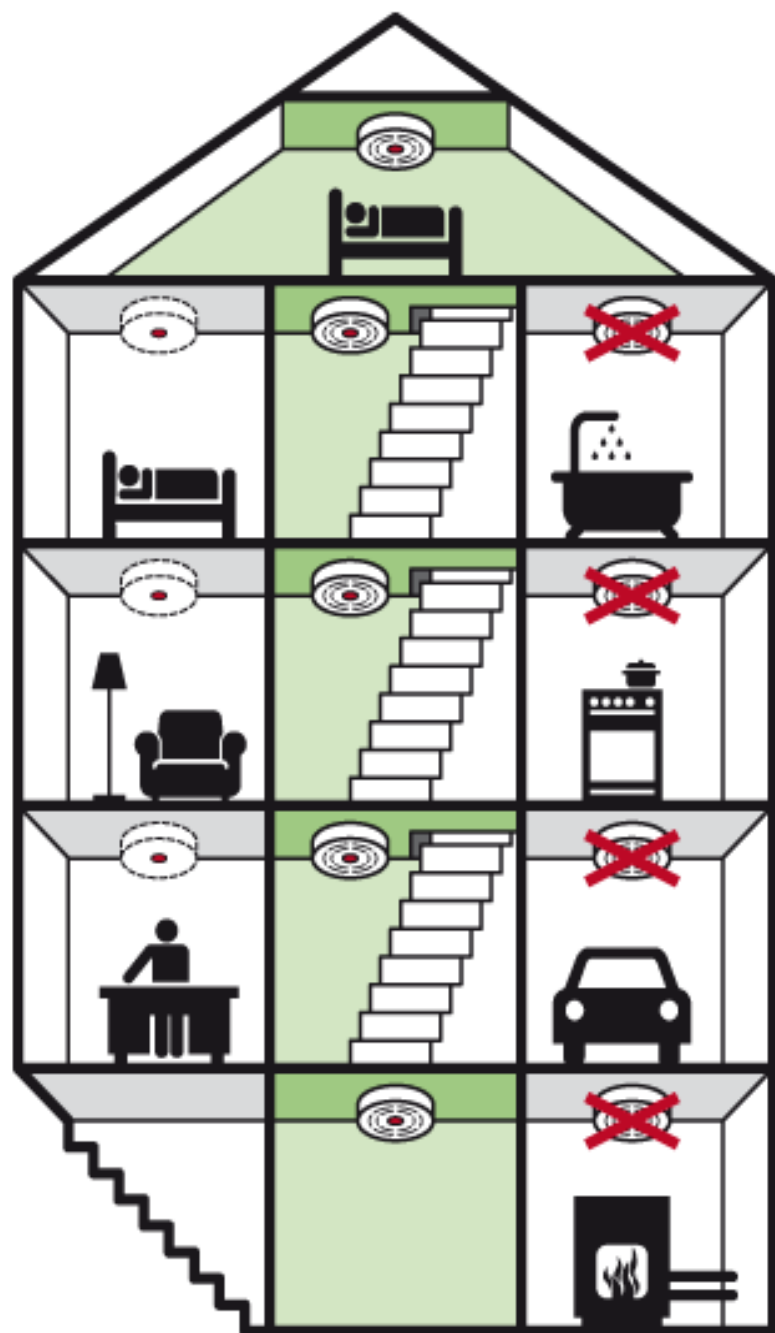




- Lees de handleiding
- Gebruik alleen de originele oplader
- Laad het apparaat bij voorkeur overdag op
- Haal de stekker uit het stopcontact als de batterij of accu vol is
- Opladen op een stabiele, onbrandbare plaats en in een ruimte met een rookmelder
- Beschadigingen: laten controleren

Veilig opladen





Alleen begane grond:



-  Minimale bescherming
-  Maximale bescherming
-  Nooit hier!

- Stikgevaar (door giftige stoffen)
- Je ziet niets
- Desoriëntatie
- Hitte



3 Minuten





Veilig vluchten



3 minuten

2 vluchtwegen



Ken de vluchtweg!



Vluchtwegaanduiding openbare gebouwen



Bij brand in uw woning

- Verlaat zo snel mogelijk uw woning
- Doe ALTIJD elke deur achter u dicht, dus ook de buitendeur
- Probeer uw burenen te waarschuwen
- Ga, indien mogelijk, naar het dichtstbijzijnde trappenhuis. Pak **nooit** de lift !!
- Ga naar beneden of wacht op hulp
- Bel zo snel mogelijk het alarmnummer 1-1-2



Alternatief vluchtplan

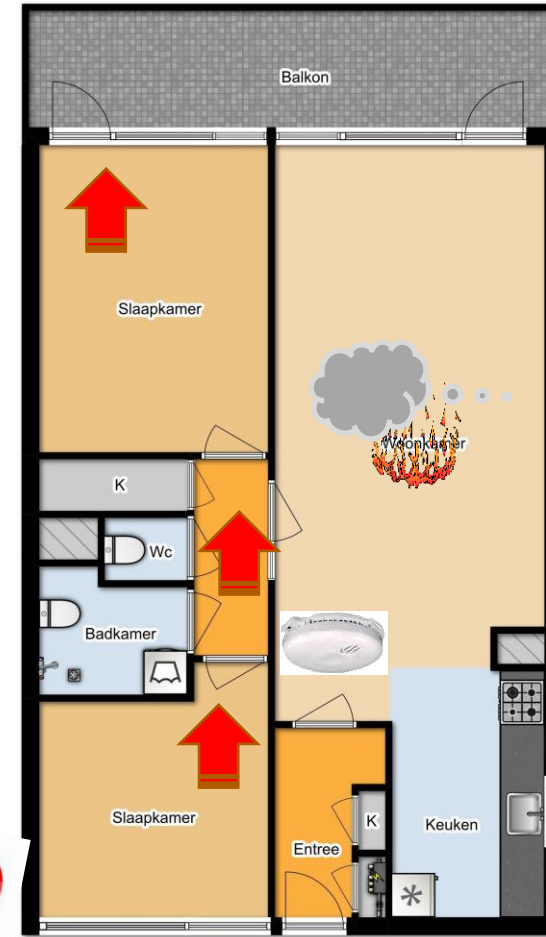
Ga bij voorkeur
naar een kamer
aan de
straatzijde



Sluit deur en
dek de
kier/plint af



Open kamerraam



Bij brand in het gebouw

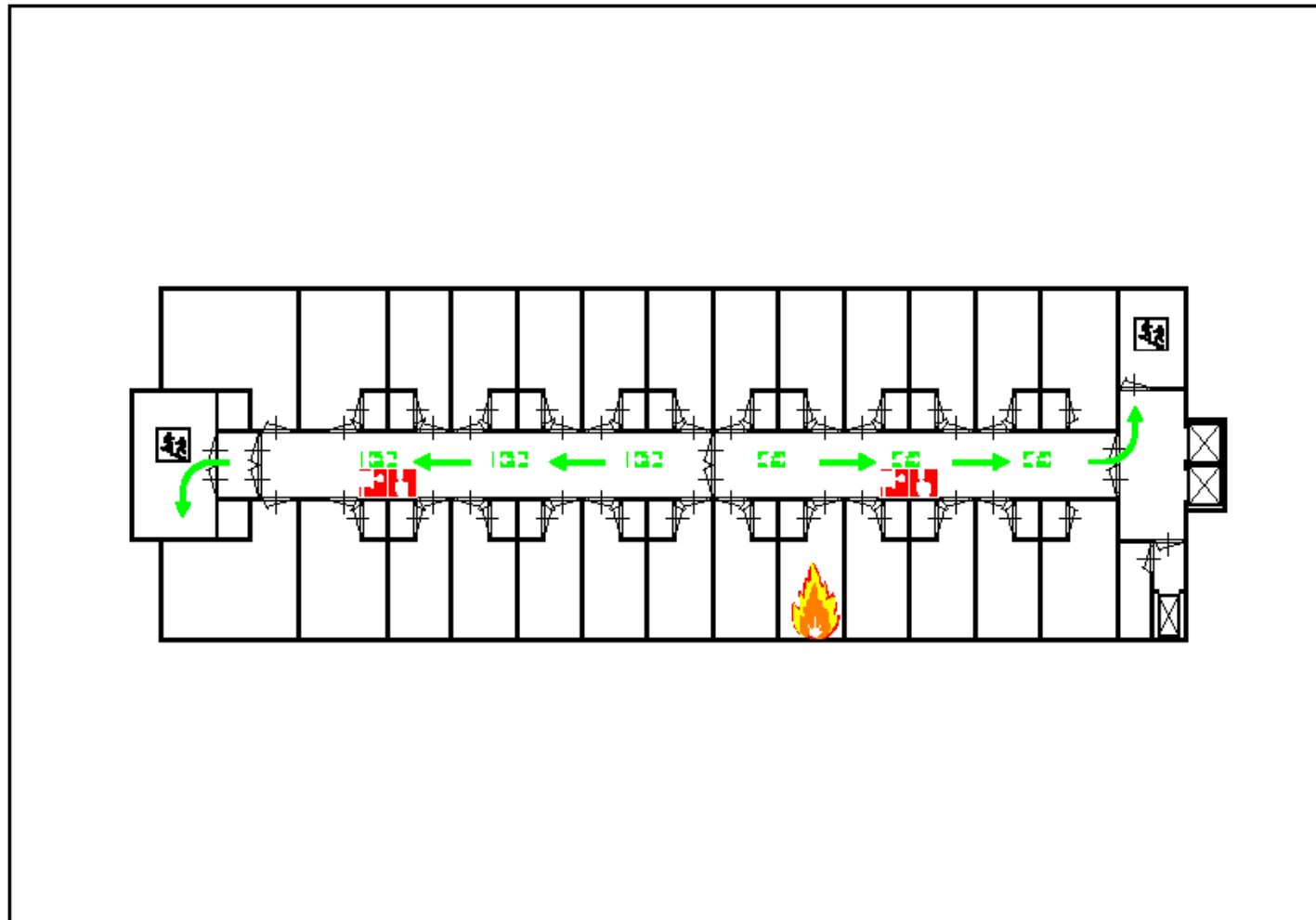
- Blijf rustig!
- In uw woning bent u minimaal 30 minuten veilig voor brand
- Zijn trappenhuizen bij brand niet bereikbaar vanuit uw woning....wacht dan **IN** uw woning of op het balkon tot de brandweer arriveert
- Zorg dat er geen rook in uw woning komt!



Fasen van ontruiming



Hoe gaan we ontruimen



Brandweer bellen via 1-1-2

Bel **BUITEN**

De 1-1-2 telefonist vraagt welke hulp je nodig hebt:
politie, brandweer of ambulanceen in welke stad

Je wordt doorverbonden

De meldkamer van de hulpdienst vraagt

Wat is het **adres** van het noodgeval?

Op welk **telefoonnummer** kan ik u terugbellen?

Wat is uw **naam**?

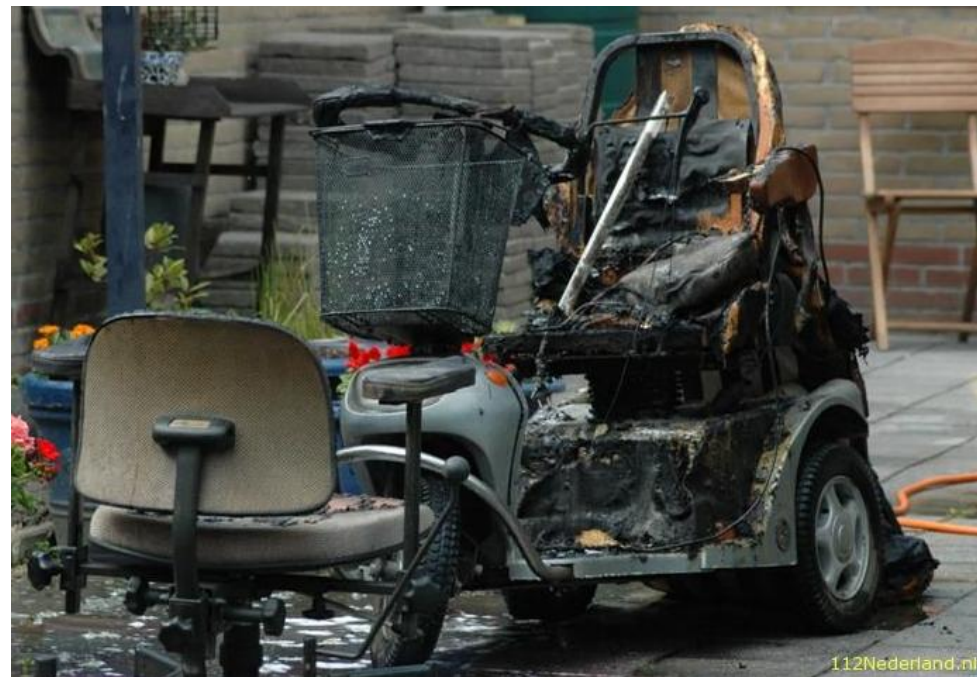
Vertel mij **precies** wat er gebeurd is

Bevindt u zich **op die locatie**



Scootmobielen

- ca. 400.000 scootmobielen in Nederland
 - Verwachting in 2030 is 600.000
- Kans op brand :
 - door slijtage (regelmatig onderhoud)
 - bij opladen accu (oververhitting)
 - kortsluiting
- Stallen van een scootmobiel:
 - in huis (niet in de vluchtroute)
 - in woongebouw (oudere gebouwen niet op berekend)
 - bij voorkeur in garage of aparte ruimte (scootmobielbox)



Zijn er vragen ?



Dank voor uw aandacht



Koolmonoxide

Gevaren koolmonoxide

Wanneer er koolmonoxide in huis is:

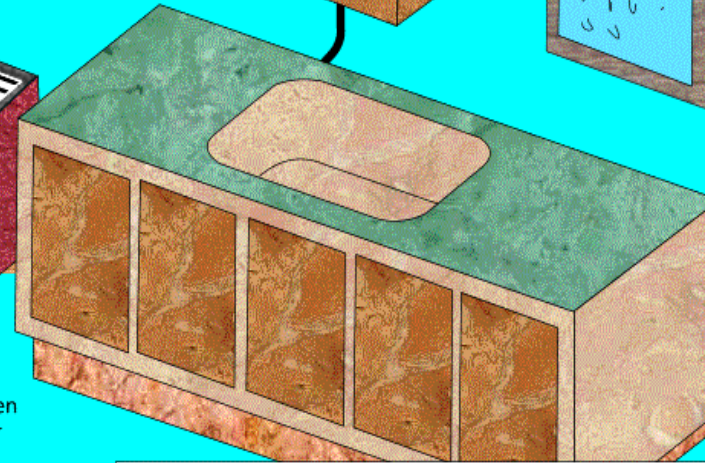
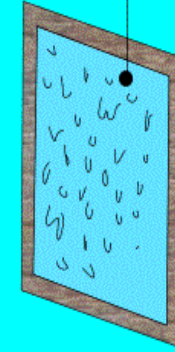
Niet voldoende lucht, er ontstaat condens op de ramen.



Bij een verstopte schoorsteen komen verbrandingsstoffen de woonkamer in.

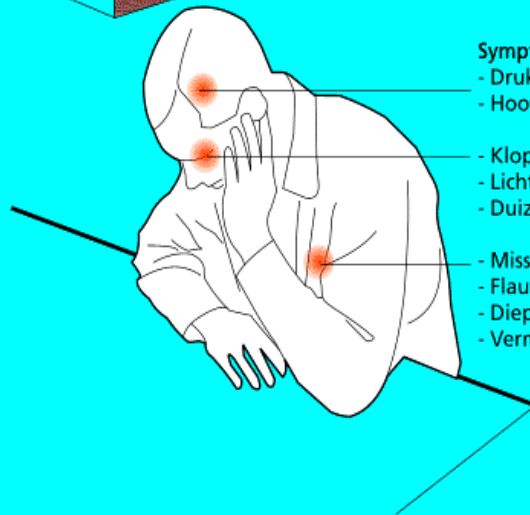


De vlam in de geiser en kachel is oranje van kleur en brandt hoger dan normaal.

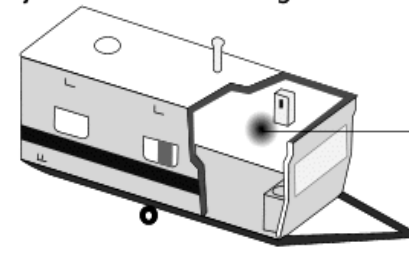


Symptomen:

- Druk boven voorhoofd
- Hoofdpijn
- Kloppende pijn in slapen
- Lichtrode gezichtskleur
- Duizeligheid
- Misselijkheid
- Flauwvallen
- Diep bewusteloosheid
- Vermindering hartfunctie



Bij caravans en woonwagens is kans op vergiftiging groter.



De ruimte is kleiner waardoor de concentratie koolmonoxide sneller oploopt.





Oplichters via internet
door Michel Hogendoorn



seniorweb

Consumenten
bond

seniorweb.nl

Wie speelt de grootste rol als het gaat om digitale veiligheid ?

A => De overheid

B => De provider

C => De gebruiker zelf

Gedrag !!

Wat is het belangrijkste onderdeel om veilig te kunnen internetten?

A => Zorgen dat je een veilige verbinding hebt

B => Zorgen dat je veilige wachtwoorden gebruikt

C => Zorgen dat je nepberichten kunt herkennen

D => Zorgen dat je andere vormen van fraude pogingen kunt herkennen

Diverse vormen van nepberichten

- Phishing
 - Vissen naar (stelen van) jouw gegevens
 - Zie ook consumentenbond <https://www.consumentenbond.nl/veilig-internetten/voorbeelden-phishing-nepmails>
 - Spoofing (je doet je voor als iemand anders)
 - WhatsAppfraude
 - Telefoon
 - Helpdesk
 - Website
 - QR-code-fraude: tips en risico's
-
- Het zijn allemaal fraude berichten

Maar eerst !

- Het kan ons allemaal overkomen
- Steeds geraffineerder
 - Steeds minder taalfouten !!
 - Spelen in op de actualiteit
- Speelt in op de menselijke emoties
 - Hebzucht
 - Aanbod is te mooi om waar te zijn
 - Uw teruggave staat voor u klaar
 - Angst
 - Uw rekening wordt binnenkort geblokkeerd
 - Betaal en voorkom snel oplopende incassokosten
 - Uw computer heeft een virus
 - Familie
 - Whatsapp => Hè pap/mam - berichtjes

Wat is phishing?



- Phishingberichten hengelen ('vissen') naar je geld en je gegevens. Met een dringend bericht proberen ze je vaak naar een valse website te leiden. Soms ziet die er precies hetzelfde uit als de officiële website. Alleen het webadres wijkt altijd af.
- Nepmails zijn ook nog steeds een belangrijke manier om virussen te verspreiden. Vooral ransomware die je persoonlijke bestanden versleutelt is gevaarlijk.
- Gegevens die je invult op de phishing-website kunnen criminelen gebruiken om bijvoorbeeld je rekening te plunderen.
- De schaal waarop phishingmails worden verstuurd is enorm. Google verwijdt er dagelijks al ruim 100 miljoen. Veel valse e-mails worden verstuurd uit naam van banken, pakketverzendende, incassobureau Intrum Justitia, het CJIB en internetproviders. Nep-winacties, die je mooie prijzen voorspiegelen, komen uit naam van bijna alle bekende merken voor.

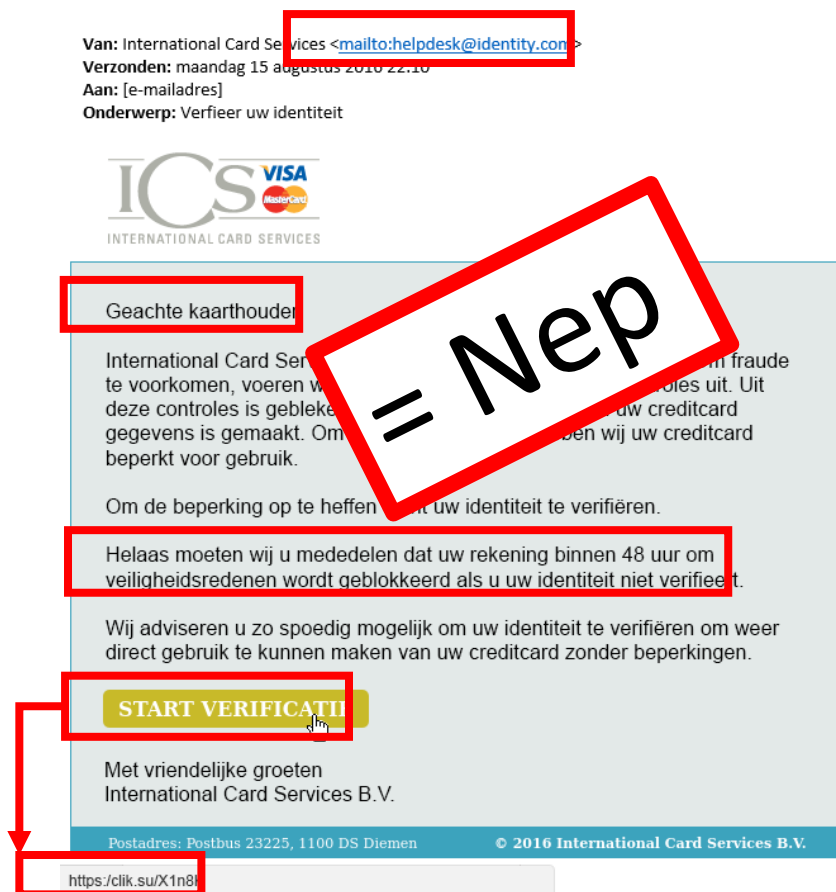
Phishing – waar moet ik op letten?



1. Verdacht mailadres als afzender
2. Urgentie en snelle actie is nodig
3. Verdachte onderwerpen bv. Beveiligingsproblemen, KVK
4. Te mooi om waar te zijn
5. Willen ze iets van je weten (persoonlijke gegevens)
6. Onpersoonlijk aanhef bij iets wat persoonlijk is (bv. Jouw kaart)
7. Check de [DIT IS EEN LINKJE](#) waar ze willen dat je op klikt (mouse-over)
8. Bijlagen (wat voor soort bijlage is het (de bestand extensie))
9. Wachttijden / -melding bij bankwebsites
10. Taalfouten (Jammer: Criminelen wordt steeds taalvaardiger)
11. Fout rekeningnummer (bij betalingen)
12. Niet alleen via e-mail

13. Bij twijfel => niet klikken maar checken

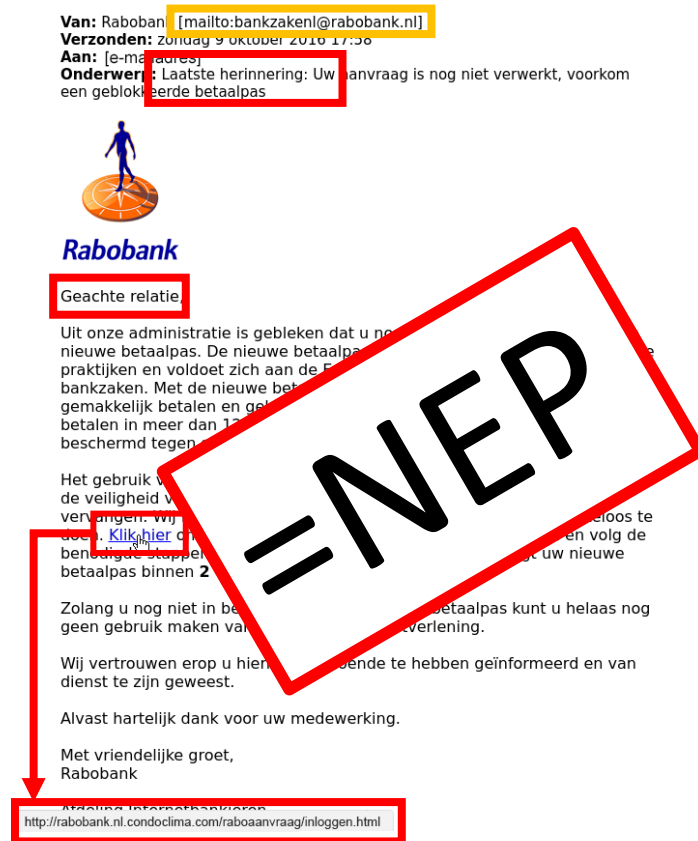
Voorbeelden phishingmails



Wat moet ik op letten ?

1. Email adres?
2. Aanhef ?
3. Is er haast bij?
4. Moet ik betalen of persoonlijk gegevens delen?
5. Gaat het om een juiste link?
6. Conclusie?

Voorbeelden phishingmails



Wat moet ik op letten ?

1. Email adres?
2. Aanhef ?
3. Is er haast bij?
4. Moet ik betalen of persoonlijk gegevens delen?
5. Gaat het om een juiste link?
6. Conclusie?

Voorbeelden phishingmails

Van: PostNL - [mailto:noreply@notificatie.postnl.nl]
Verzonden: dinsdag 9 juli 2016 16:45
Aan: [e-mailadres]
Onderwerp: Uw PostNL Pakket



Pakketten

=Echt

Beste heer/mevrouw,

Vandaag bezorg ik bij u een pakket van LIGGO, met barcode 33260 15269 1526. Kijk op [PostNL](#) hoe laat ik bij u langskom.

Mocht u niet thuis zijn dan ontvangt u een bericht met een 'Niet-thuis-code'. Met deze code kunt u vandaag voor 22.00 uur een keuze maken voor een tweede bezorgafspraak.

Maakt u geen keuze, dan kom ik morgen nog een keer bij u langs (m.u.v. zon- en feestdagen).

Met vriendelijke groet,

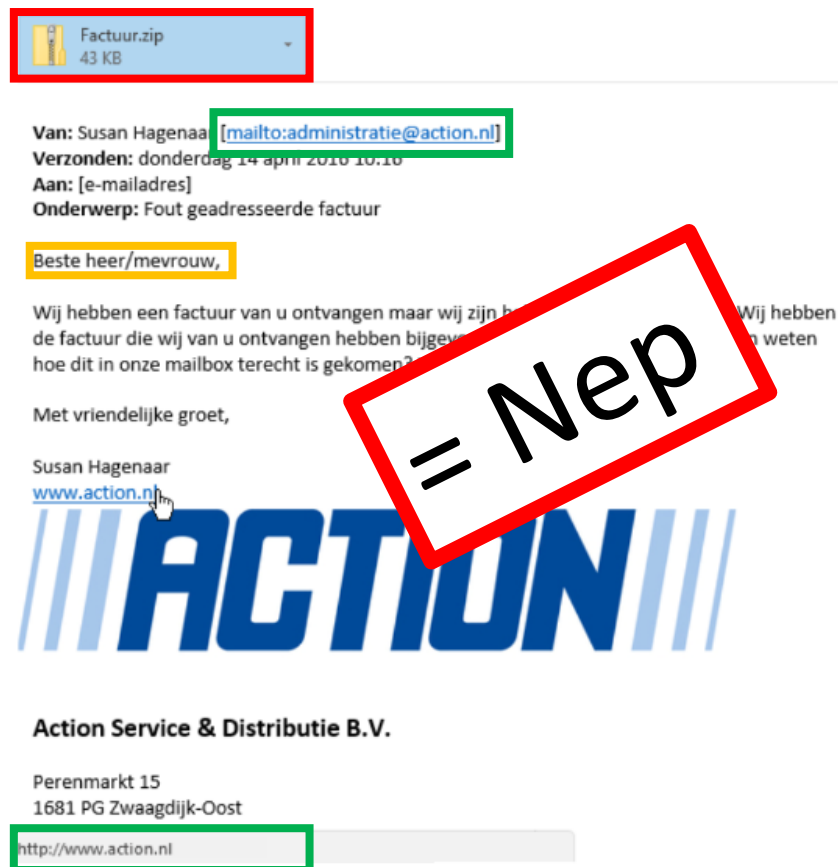
Uw PostNL Pakketbezorger

<https://p.notificatie.postnl.nl/public/r/qdgl8bhena1jfpfqczkg/keyptzfnpmvketzugfsa/gvgbj6p1auh7gesqepouna>

Wat moet ik op letten ?

1. Email adres?
2. Aanhef ?
3. Is er haast bij?
4. Moet ik betalen of persoonlijk gegevens delen?
5. Gaat het om een juiste link?
6. Conclusie?

Voorbeelden phishingmails



Wat moet ik op letten ?

1. Email adres?
2. Aanhef ?
3. Is er haast bij?
4. Moet ik betalen of persoonlijk gegevens delen?
5. Gaat het om een juiste link?
6. Conclusie?
 1. Let bij bijlagen ook op verdachte bestandsformaten



2. Eindconclusie?

Voorbeelden phishingmails

Van: Dlguide [mailto:info@djguides.nl]

Verzonden: woensdag 14 april 2016 11:14

Aan: [e-mailadres]

Onderwerp: Gratis e-ticket Armin van Buuren Kingsday Leiden

GRATIS E-TICKET ARMIN VAN BUUREN KINGSDAY LEIDEN



Armin van Buuren presents Kingsday Leiden

Armin van Buuren treedt dit jaar weer op in Leiden op Koningsdag. Na het grote succes van vorig jaar vindt het feest 'Armin van Buuren presents Kingsday Leiden' dit jaar weer plaats op de Garenmarkt in de binnenstad van Leiden en jij kan er **GRATIS** bij zijn.

Op dinsdag 27 april vanaf 15.00 uur tot 22.00 uur kunnen oranje fans genieten van diverse optredens met als hoogtepunt een optreden van Leidenaar Armin van Buuren.

Ook dit jaar zal Armin van Buuren de oranjekoorts 'zijn stad' naar ongekende hoogte laten stijgen. Al 13 jaar lang treedt Van Buuren, één van de beroemdste DJ's ter wereld, op tijdens Koningsdag in Leiden. Dit is het hoogtepunt van het feest 'Armin van Buuren presents Kingsday Leiden', dat dit jaar weer plaatsvindt op de Garenmarkt. Iedereen vanaf 16 jaar en ouder kan hier genieten van het ultieme Koningsdagfeest!

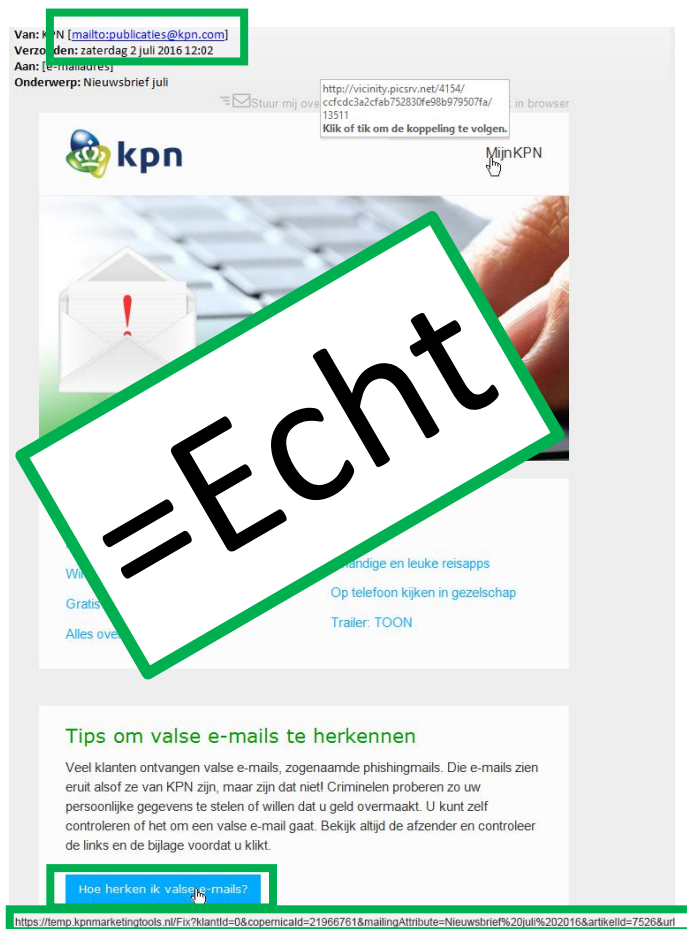
[DOWNLOAD HIER JOU GRATIS TICKET](#)

<http://www.djguides.nl/gratis-ticket>

Wat moet ik op letten ?

1. Email adres?
2. Aanhef ?
3. Is er haast bij?
4. Moet ik betalen of persoonlijk gegevens delen?
5. Gaat het om een juiste link?
6. Conclusie?
 1. Alles lijkt OK
 2. 1^E Alarmbel: Te mooi om waar te zijn
 3. Spelfout in de link
 4. HTTP ipv HTTPS
 5. Eindconclusie

Voorbeelden phishingmails



Wat moet ik op letten ?

1. Email adres?
2. Aanhef ?
3. Is er haast bij?
4. Moet ik betalen of persoonlijk gegevens delen?
5. Gaat het om een juiste link?
6. Conclusie?

Voorbeelden phishingmails

Belangrijke mededeling

KVK <webseitenre@mrccida.mx>
18-8-2023 02:51

Aan: nrijghogandoorn@oliggo.nl

KVK

= Nep

Belangrijke Mededeling: Correcte Persoonsgegevens

Geachte heer/mevrouw,

Wij willen u vriendelijk herinneren aan het belang van het aanleveren van de juiste persoonsgegevens. Accurate informatie is essentieel voor een vlotte afhandeling van onze diensten.

Verifieer alstublieft uw persoonsgegevens op uw account om er zeker van te zijn dat alles up-to-date en correct is. Ga naar uw profielpagina en controleer zorgvuldig of uw naam, adres, contactgegevens en andere relevante informatie accuraat zijn.

Scan de onderstaande QR code om naar uw profielpagina te gaan.



Bedankt voor uw medewerking en tijdige aandacht voor dit belangrijke aspect. Wij stellen uw samenwerking op prijs en kijken ernaar uit om u verder van dienst te zijn.

Met vriendelijke groet,

KvK

Mijn laatste phishing mail.

Of ik even mijn profielgegevens bij de kamer van Koophandel wil bijwerken door op de QR code te klikken.

Phishing - belangrijk

- Belangrijke tips



- Gebruik geen telefoonnummers uit het bericht zelf
- Gebruik goede virusscanner en browser
- Bij twijfel, niet doen !!

Phishing - vraag

Toon antwoord

Je hebt ondanks je twijfel toch op een linkje geklikt. Wat kun je dan het beste doen?

A => Check alsnog de website (bv 'slotje' en bij <https://www.checkjelinkje.nl/>)

B => Ik bel 112 wegens oplichting

C => Vul geen persoonlijke gegevens in



Phishing - vraag

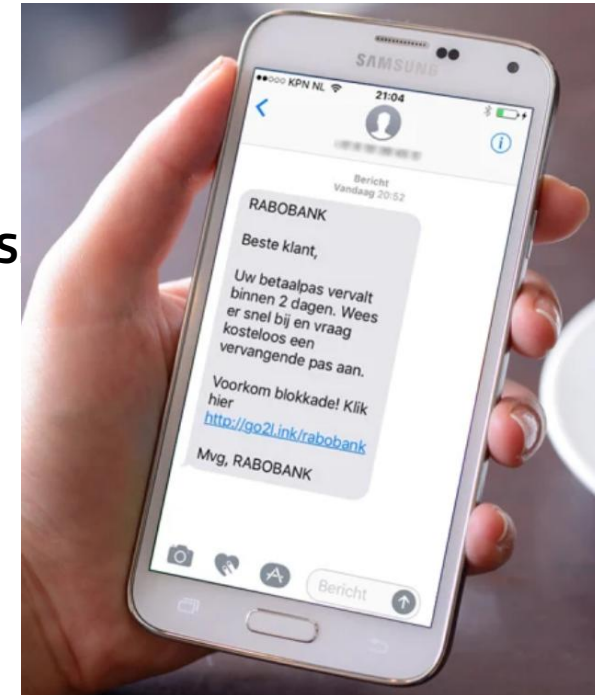
Toon antwoord

Je hebt via SMS het volgende bericht ontvangen. Wat doe je?

A => Ik doe de zelfde controle regels als bij phishing email toepassen. Ik klik niet.

B => Phishing is alleen via e-mail en social media maar niet via SMS. Ik kan gewoon doen wat de bank in het bericht van me vraagt.

C => SMS heeft een ander veiligheidsprotocol. In de link staat Rabobank en dan is het goed.



Voor meer info over phishing via SMS:

<https://www.consumentenbond.nl/veilig-internetten/phishing-via-sms>

Spoofing – Whatsapp fraude

Toon antwoord

Wat doe je?

A => Ik help natuurlijk mijn zoon even uit de brand

B => Ik bel hem even terug met Whatsapp

C => Ik bel hem even terug op zijn oude nummer



Spoofing – Whatsapp fraude

- WhatsApp-fraude zorgt voor veel schade: gemiddeld duizenden euro's per slachtoffer. Bij de nieuwste variant doen oplichters niet alleen bekenden na, maar kapen ze ook WhatsApp-accounts.



Maak contact via het oude nummer

Voer een duidelijk gesprek

Bij twijfel niet betalen

Doe aangifte bij de politie

Stel tweefactorauthenticatie in

Bespreek het met bekenden



Spoofin



Een medewerker van de afdeling beveiliging van jouw bank belt je op met de mededeling dat ze frauduleuze transacties op jouw rekening hebben gezien. Uit voorzorg vraagt de medewerker aan jou om je geld naar een veilige tussenrekening over te maken.

A => Ik volg zijn instructies zodat mijn geld buiten het bereik van fraudeurs blijft

B => Ik vraag hem om mij de instructies per mail toe te toesturen.

C => Ik beëindig het gesprek direct. De bank benaderd klanten nooit direct met dit soort vragen!



Wat doe je nog meer nadat de poging tot oplichting doorhad.

A => Ik was de fraudeur te slim af dus geen verdere stappen zijn nodig

B => Ik doe aangifte bij de politie van POGING tot oplichting

C => Ik bel/benader mijn bank via de telefoon/website en maak melding van de poging tot oplichting



Ik krijg een email van de Rijksoverheid dat in het kader van een nieuwe koopkracht herstel maatregel van de regering, ik in aanmerking kom voor een aanzienlijke korting op de OZB belasting voor mijn huis.

In de mail staat een QR code om deze OZB korting aan te vragen.

A => Ik bel telefoon nummer in de mail om te checken of wel echt waar is.

B => QR code kunnen oplichters NIET namaken en is daarom altijd veilig. Ik kan de korting gewoon aanvragen.

C => QR code kunnen oplichters OOK namaken. Ook bij QR codes moet je daarom blijven opletten. Verder klinkt de meevaller als 'te mooi om waar te zijn'. Niet klikken.



Wat als toch geklikt ??



Gelukkig kan het meestal niet zo veel kwaad als je per ongeluk klikt op een phishinglinkje.

- Het gaat pas echt fout als je iets invult op of downloadt van de nepwebsite waar je op terecht komt.
- Of als je een foute bijlage opent.

Heb je al bepaalde gegevens prijsgegeven aan een fraudeur?
Trek dan direct aan de bel bij de betrokken bedrijven of instanties.



- Waarschuw direct je bank als het om bankgegevens gaat.
Volgens de banken kom je alleen in dat geval in aanmerking voor compensatie van de schade.
- Heb je een wachtwoord ingevuld op een nepwebsite?
Verander dit wachtwoord dan meteen in een nieuw sterk wachtwoord.
Gebruik je dit wachtwoord ook elders? Pas het ook daar aan.
- Criminelen kunnen persoonlijke gegevens ook gebruiken voor bijvoorbeeld [bank spoofing](#) of andere oplichting.
- Kun je bestanden niet meer openen?
En zijn ze versleuteld door gijzelsoftware?
Dan is er niet altijd een oplossing, maar in sommige gevallen wel.
Lees hoe je deze zogenoemde [ransomware kunt verwijderen](#).
- Heb je je mobiele nummer ingevuld?
Meld je dan meteen af voor ongewenste (sms) betaaldiensten via [Payinfo.nl](#).
- Ben je geld kwijtgeraakt?
Doe aangifte.
Je kunt ook proberen je geld terug te krijgen door [gegevens van de oplichter](#) op te vragen.

Cookies

https://www.youtube.com/watch?v=f_CPNB8ASR4

1. Wat zijn cookies ? => Bestandjes met jouw activiteit op internet die achterblijven op jouw computer nadat je een website hebt bezocht.
2. Soorten cookies
 1. Noodzakelijke (essentiële) cookies
 1. **Functionele cookies**
 2. **Analytische cookies**
 2. Niet noodzakelijke cookies
 1. **Tracking cookies**
 2. **Cookies van derden**
3. Moet de website toestemming vragen om deze cookies te gebruiken (c.q. op jouw computer achter te laten)??
 1. Noodzakelijke cookies => **Nee**
 2. Niet noodzakelijke cookies => **Ja**

Cookies – hoe mee om te gaan

1. Noodzakelijke cookies => niet te voorkomen
2. Niet noodzakelijke cookies bij vraag voor toestemming
 1. Accepteren
 2. Weigeren
 3. Zelf instellen
3. Wat kun je nog meer zelf doen
 1. Regelmatig cookies verwijderen
 2. Bij de browser instellingen kun je aangeven dat je cookies allemaal verwijderd moeten worden na afloop van jouw sessie

Alles accepteren

Zelf instellen

Weigeren





WAS

Veiligheid in de wijken

Wijk en Agent Samen

Bijeenkomst JongSenioren ZM



Wat is WAS?

- Teams
- Betrokken inwoners
- Doel
- Rol



**Wat doet
WAS?**

Oren en ogen

Loopronde

Themakalender

Melden

Projecten en campagnes

Samenwerkingspartners



gemeente
Zoetermeer



gemeente
Zoetermeer

Historie en in de praktijk





gemeente
Zoetermeer

Bedankt!

buurtpreventie@zoetermeer.nl





Pauze



Steun JongSeniorenZM met een donatie





Discussie in groepjes



Afsluiting
door
Yvonne schouten