Veilig internet

Internet

- Wie kan er nog zonder internet?
- Vrijwel alles gebeurt of kan gebeuren via internet
  - Bankieren
  - Winkelen
  - Gemeentelijke zaken
  - Belastingaangifte
  - Deel van sociaal leven
- Ook fraude en oplichting heeft zich verplaatst naar het internet

virus
trojan
hacker
infection
detection
spyware
internet
infected
firewall
cyber
phishing
malware
international
hackers
spam
hacking
intruder
attack
crime
computer
network
criminal
altering
target
service
needed
using
rooms
victim
people
access
defined
counts
included
technical
between
services
directly
infected
organized
networks
cyberspace
content
including
pornography
information
communications
terrorism
unauthorized
individuals
activities
system
crimes
child

Opbouw presentatie

- Malware
- Phishing
- Hulpvraagfraude (spear phishing/whaling)
- Helpdeskfraude
- Spoofing
- Contactfraude (datingfraude)
- Marktplaatsfraude
- Accounts beschermen

Malware

- Malware omvat alle ongewenste programma's op je computer
  - Computervirussen
  - Computerwormen
  - Trojaans paard
  - Adware
  - Spyware
  - Scareware
  - Ransomware
  - Backdoors

Bescherming tegen malware

- Haal programma's alleen van officiële websites
- Let bij installeren van programma's op dat je niets extra's installeert
- Open geen bijlagen van e-mails van onbekende afzenders
- Maak back-ups van bestanden op externe gegevensdragers
- Maak gebruik van goede antivirus software en firewall
- Update tijdig belangrijke software

Phishing

- Doel: verkrijgen van toegang tot accounts/bankrekening
- Via e-mail, WhatsApp, SMS
- Inzet massa-mails
- (Meestal) urgent karakter, wijzend op ernstige bedreiging
- Je wordt omgeleid naar een nepsite
- Dader krijgt daarmee gebruikersnaam en wachtwoord in handen of toegang tot bankrekening!

Herkennen van phishing

- Tekst bevat vaak spelfouten en grammaticale fouten
- Onpersoonlijke aanhef (geen naam)
- Vaak haast geboden
  - Dringende betaling nodig
  - Blokkade toegang van accounts
  - Werking software wordt beëindigd
  - Dreigen met deurwaarder/boete
- E-mail afkomst van vreemd uitziend adres
- Links naar vreemde webadressen

Gaat het echt om phishing?

- Kijk op website afzender
- Kijk op website SeniorWeb
  - https://www.seniorweb.nl/onderwerp/spam-en-phishing#/meldingen
- Google de titel van de e-mail
- Stuur de mail door naar een kennis die er verstand van heeft
- Kijk op veiliginternetten.nl
- Leden SeniorWeb kunnen mail door-sturen voor controle (Phishingchecker)
  - https://www.seniorweb.nl/phishing

Populair bij phishing

- Banken
- DigiD
- Kamer van Koophandel
- Virusscanners
- Aanbieders internet/telefoon
- Energiemaatschappij
- Cloudoplag
- Post

T · ·Mobile· · ·

Geachte klant,

U ontvangt deze e-mail, omdat uit onze administratie is gebleken dat het door u te betalen bedrag.
Voor de geleverde T-Mobile-internetdiensten van de maand **september** niet van uw rekening kon worden afgeschreven.

Bedrag en specificaties

Wij bieden u nod een laatste mogeliikheid aan om het openstaande factuur van **€ 103,50** alsnog binnen 2 tot 3 werkdagen te voldoen.
Door onderstaande stappen te volgen kunt u dit bedrag eenvoudig via onze nieuwe bitcoin (gekoppeld aan iDeal) betalingsmiddel te voldoen.

Zodra u het openstaande achterstand heeft betaald, zult u worden doorgeleid naar onze homepagina.

- klik hier om de betaling te voldoen
- gewenste aantal bitcoins: 0.15421
- bitcoinadres: 1NVhDeinNe6n75qd5Yppx1kZe1LhYpazLd
- Kies uw bank

T··Mobile

Er een storing is in jouw postcodegebied

Beste relatie,

We zien dat er een storing is in jouw postcodegebied. Hierdoor ervaar je mogelijk problemen met internetten, bellen en/of TV kijken. Er wordt hard gewerkt om dit zo snel mogelijk op te lossen.

Mijn account direct bijwerken
Om weer optimaal gebruik te kunnen maken van je T-Mobile account dien je je account gebruik opnieuw te verifieren via T-Mobile Beheer.

Voor meer informatie over onze veiligheid, ga naar t-mobile.nl/veiligheid-en-privacy

Met vriendelijke groeten,

T-Mobile

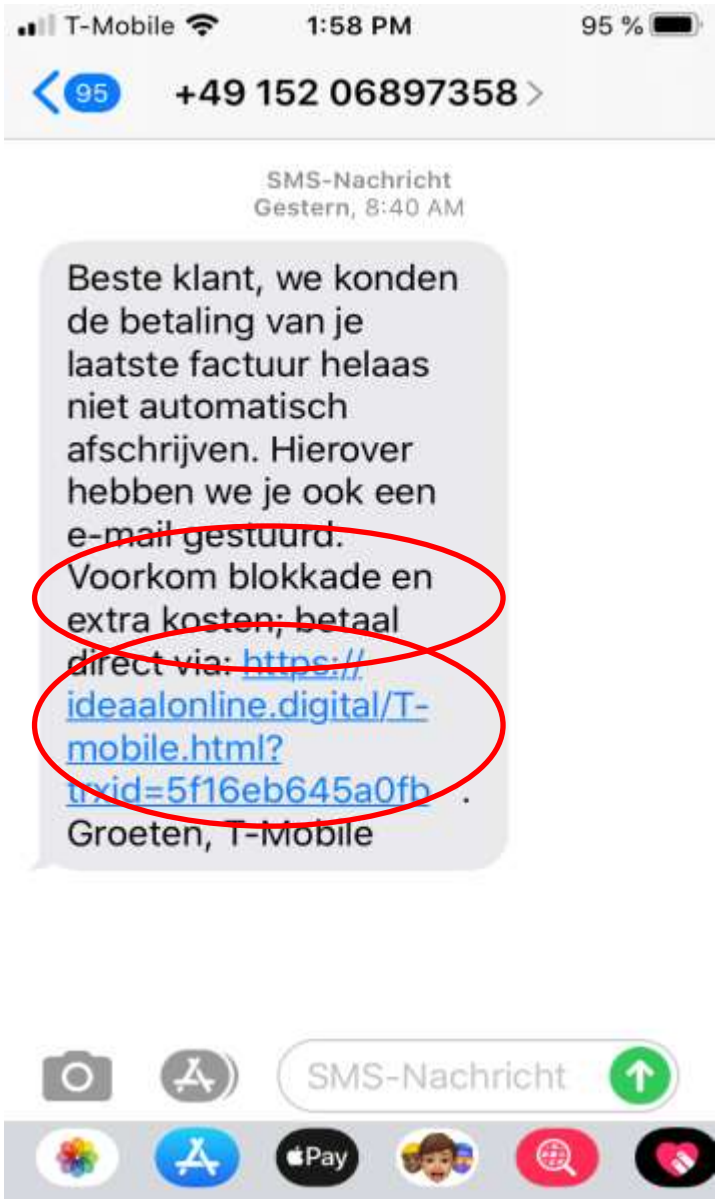
Uw betalingstermijn is verstreken

Wij stellen u thans nog eenmaal in de gelegenheid het verschuldigde bedrag van € 50,00 uiterlijk binnen een termijn van drie werkdagen te voldoen. Doordat het automatische incasso het bedrag niet van uw rekening kon afschrijven, verzoeken wij u te betalen met de zogeheten **CRYPTOBV**.

Het openstaande bedrag is momenteel **€ 53,32** (inclusief kosten).
Het bedrag zal worden verhoogd met buitengerechtelijke incassokosten ter hoogte van **€113,95** indien het niet binnen de door ons gestelde termijn is voldaan.

Klik hier op: online betalen om de factuur te voldoen, let op dat u de waarde van **€50,00** selecteert.

- Gebruik voor de betaling dit **E-mail adres:** tmprov0cryptopay@outlook.com zorg dat u het zorgvuldig overneemt



BESTE KLANT,

Uw zending Nr. [NL2022C49527] wacht nog op uw instructies. Bevestig de betaling van de verzendkosten.

Verzendkosten: 0,99 EURO

Hoe haal ik mijn pakket op?

We raden u echter aan het verlengingsformulier voor uw services handmatig in te vullen door de instructies in de onderstaande link te volgen.

Betaal verzendkosten door hier te klikken

Eerlijk,

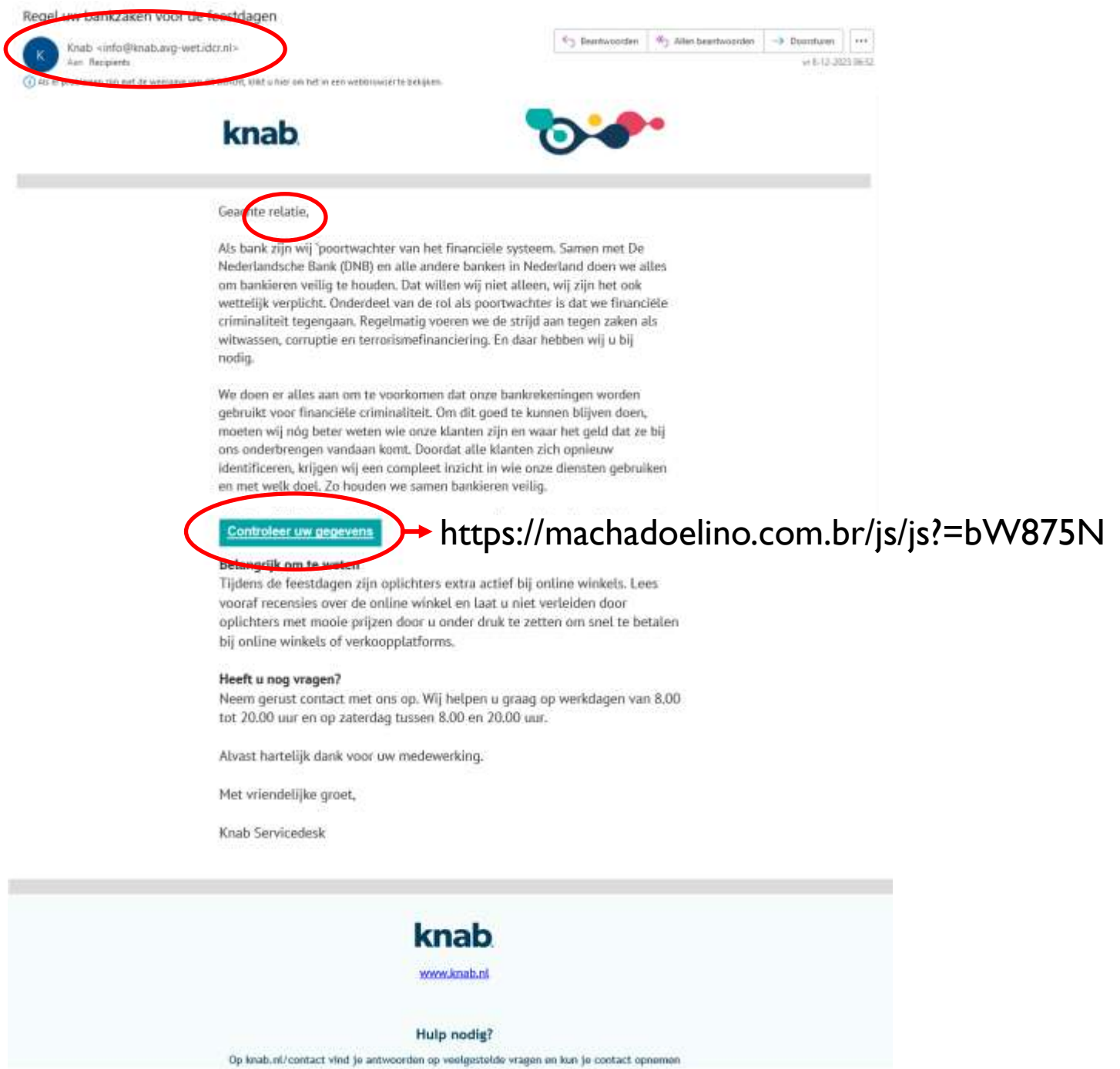
PostNL

POSTNL.NL | Neem contact op met POSTNL

Afzender mail = Knab (online bank, vrnl. voor zzp'ers)

Verwijzing naar https://punto23.com.pe

idcr.nl



Regel uw bankzaken voor de feestdagen

Knab <info@knab.avg-wet.idcr.nl>
Aan: Recipients

Beantwoorden | Allen beantwoorden | Doorsturen

knab

Geachte relatie,

Als bank zijn wij 'poortwachter van het financiële systeem. Samen met De Nederlandsche Bank (DNB) en alle andere banken in Nederland doen we alles om bankieren veilig te houden. Dat willen wij niet alleen, wij zijn het ook wettelijk verplicht. Onderdeel van de rol als poortwachter is dat we financiële criminaliteit tegengaan. Regelmatig voeren we de strijd aan tegen zaken als witwassen, corruptie en terrorismefinanciering. En daar hebben wij u bij nodig.

We doen er alles aan om te voorkomen dat onze bankrekeningen worden gebruikt voor financiële criminaliteit. Om dit goed te kunnen blijven doen, moeten wij nóg beter weten wie onze klanten zijn en waar het geld dat ze bij ons onderbrengen vandaan komt. Doordat alle klanten zich opnieuw identificeren, krijgen wij een compleet inzicht in wie onze diensten gebruiken en met welk doel. Zo houden we samen bankieren veilig.

Controleer uw gegevens → https://machadoelino.com.br/js/js?=bW875N

Belangrijk om te weten
Tijdens de feestdagen zijn oplichters extra actief bij online winkels. Lees vooraf recensies over de online winkel en laat u niet verleiden door oplichters met mooie prijzen door u onder druk te zetten om snel te betalen bij online winkels of verkoopplatforms.

Heeft u nog vragen?
Neem gerust contact met ons op. Wij helpen u graag op werkdagen van 8.00 tot 20.00 uur en op zaterdag tussen 8.00 en 20.00 uur.

Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groet,

Knab Servicedesk

knab

www.knab.nl

Hulp nodig?

Op knab.nl/contact vind je antwoorden op veelgestelde vragen en kun je contact opnemen

Hulpvraagfraude (spear phishing/whaling)

- Vaak via WhatsApp
- Aanval gericht op individu
- Bericht van “bekende”
- Boodschap: nieuwe telefoon en/of nieuw nummer
- Zit in nood en/of heeft dringend geld nodig


14:26
40%
1
+31 6
laatst gez. vandaag om 14:26
Vandaag
Berichten en gesprekken worden end-to-end versleuteld. Niemand buiten deze chat kan ze lezen of beluisteren, zelfs WhatsApp niet. Tik voor meer informatie.
Ik ben het! En ik heb een nieuw nummer 14:24
Sla je m'n nieuwe nummer meteen op? 14:24
Andere vraag: kan je me even helpen? Kun je een rekening voor me betalen? 14:25
Ik moet vandaag betalen maar ik kan niet bij mijn bankrekening komen 14:25
De afzender komt niet voor in uw contacten
Blokkeer
Rapporteer
Voeg toe aan contacten


Berichten en oproepen in deze chat zijn nu beveiligd met end-to-end encryptie. Tik voor meer informatie.
Hey Papa met Alex. Dit is me nieuwe nummer mijn oude nummer kan weg ❤️😘 16:33
Alles goed ? 16:34
Ben je druk... 16:35
Zit te chillen.. Jij? 16:35
Ik ben onderweg naar huis 16:36
Ik zit met een klein probleem sinds vanochtend 😓 16:36
Wat.. 16:36
Ik kan sinds vanochtend niet overmaken heb jij ook storing bij de ing ?

Wat te doen?

- Wees altijd alert als geld gevraagd wordt
- Wees altijd alert als iets snel moet gebeuren → Tijdsdwang
- Wees er op bedacht dat ze informatie uit sociale media kunnen gebruiken!
- Bel persoon terug op bij jou bekend nummer
- Controleer het opgegeven rekeningnummer
- Scherm zo nodig eigen sociale media af (telefoonnummers, familierelaties, e.d.)

Meer hulpvraagfraude

- Oplichter probeert toegang te krijgen tot jouw WhatsApp account
- Gebruikt dat om contacten op te lichten
- Hoe?
  - Installeert WhatsApp op eigen telefoon
  - Gebruikt jouw telefoonnummer
  - Vraagt bij WhatsApp verificatiecode aan
  - Neemt met jou contact op voor code
- Stuur nooit codes door!
- Stel tweetrapsverificatie in!

Helpdeskfraude

- Medewerker van helpdesk belt: pribleem met je computer
- Vraagt om toegang tot computer via internet om probleem op te lossen
- Installeert malware
- Vraagt daarna bv. betaling voor dienst en kijkt mee hoe je inlogt bij de bank

Wat te doen

- Gebeld door een helpdesk zonder aanleiding? Hang op. Geen enkele bedrijf gaat je via die route benaderen
- Geef nooit onbekenden die je ongevraagd bellen toegang tot je computer
- Geef geen persoonlijke gegevens door
- Bel nooit telefoonnummers die door dergelijke personen gegeven worden

Bank belt

- Telefoontje van bank dat criminelen proberen geld weg te sluizen van je bankrekening
- Telefoonnummer op scherm kan van de bank zijn (spoofing)!
- Willen wel helpen om geld in een veilige “kluisrekening” te parkeren tot dreiging weg is
- Soms gecombineerd met verzoek om pinpas in te leveren bij bankmedewerker die langs komt.

Wat te doen

- Banken vragen nooit om geld over te maken naar een andere rekening
- Banken vragen nooit om een pincode of inleveren pinpas
- Bel desnoods naar de bank met het bij jou bekende telefoonnummer

Spoofing

- Vervalsen e-mailadres of telefoonnummer
- Weergave bekend e-mailadres of telefoonnummer geeft vertrouwen
- Kan voorkomen bij verschillende vormen van phishing en helpdeskfraude

- Weergegeven telefoonnr. of e-mailadres hoeft niet juist te zijn! Wees alert!

Contactfraude (datingfraude)

- Maakt contact met mensen via sociale media, datingsites of –apps
- Doelwit vooral mensen die een relatie zoeken
- Bouwt vertrouwensband op
- Begint om geld te vragen (noodgeval, om elkaar te ontmoeten, e.d.)

Wat te doen?

- Maak nooit geld over aan iemand die je nooit ontmoet hebt
- Controleer iemand zijn foto eens via bv Google Image of TinEye
- Blijf communiceren via het ontmoetingsplatform
- Blijf altijd alert, hoe betrouwbaar iemand ook overkomt in dit soort gevallen

Marktplaatsfraude

- Verschillende vormen van fraude
- Verkoopfraude
  - Nadat je geld overgemaakt hebt, krijg je geen product
- Aankoopfraude
  - Doel: geld van je rekening halen
  - Oplichter doet een goed bod om iets te kopen
  - Wil graag dat jij je betrouwbaarheid bewijst
  - Stuur een link voor een iDealbetaling van 1 cent
  - Via de link kom je op een nepsite en verdwijnt er een veel groter bedrag van je rekening!
- Gelijk oversteekfraude
  - Koper en verkoper spreken af 'gelijk oversteken' te gebruiken
  - Verkoper krijgt een nep-SMS dat er betaald is, en dat hij kan opsturen

Wat te doen?

- Wees terughoudend met (grote) bedragen overmaken
- Kijk naar de betrouwbaarheid van de persoon
- Blijf communiceren via het Marktplaats-platform
- Kijk eens hoe ze reageren als je zegt dat je het product ook wel wilt ophalen
- Let bij gelijk oversteken op de status op de website van Marktplaats

Accounts beschermen

- Toegang tot een persoonlijke dienst of afgeschermde informatie.
  - Bank, online winkels, verzekeraars, e-mail, toegang tot eigen computer / tablet / smartphone
  - Wordt beveiligd met een gebruikersnaam en wachtwoord

Veilig wachtwoord

- Lang
- Geen bekende woorden / namen / datums
- Gebruik kleine letters, hoofdletters, cijfers EN leestekens
- Moeilijk te onthouden
  - Gwd@5sd34$9Hbg
- Wachtzin
  - IkGaPerenPlukkenOp25Nov!

Alternatieven voor wachtwoorden

(Onveilige) wachtwoorden zijn het grootste veiligheidsrisico!

- Pincode
- Patroon tekenen
- Gezichtsherkenning
- Vingerafdruk

Tweestapsverificatie

- Op meerdere manieren identiteit bewijzen
  - Wat iemand weet
    - Naam en wachtwoord
  - Wat iemand heeft
    - Telefoon (sms, verificatie-app)
  - Wat iemand is
    - Vingerafdruk, gezichtsscan

Google authenticator

Conclusie

- Oplichting is zowel in het echte leven als via internet een probleem
- Het is onmogelijk in te gaan op alle mogelijkheden tot oplichting en er zullen nieuwe methodes ontwikkeld worden
- Internet is een mooie en zinvolle ontwikkeling die veel goeds heeft gebracht, maar:
  - Wees alert op iets wat afwijkt van 'normaal'
  - Wees alert zodra er geld in het spel is
  - Wees alert als er druk wordt uitgeoefend
  - Neem de tijd om via een andere route te bevestigen dat er geen sprake van oplichting is