

shopping
tomorrow



ShoppingTomorrow



Secure e-commerce

Ketenveiligheid in digital commerce

Uitdagingen in e-commerce

- Consumenten kopen steeds meer online
- Gevolg:
 - Toename digitale fraude
 - Toename nepwebshops
 - Toename phishing aanvallen
 - Toename datalekken



thuiswinkel
.org

**Wat kunnen we doen om de
weerbaarheid van e-commerce
bedrijven in Nederland tegen
cyberaanvallen te vergroten?**

Secure e-commerce expertgroep

shopping
tomorrow



Roland van Kortenhop
Manager Operations & ICT
Thuiswinkel.org



Nicole Mallens
Senior beleidssecretaris
VNO-NCW & MKB-Nederland



Gunther Cleijn
Cyber Security Officer
PostNL Pakketten Benelux BV



Hans Minten
Master Security Analyst
Wehkamp.nl



Gerrie de Jonge
CIO Parcel & Delivery
PostNL Pakketten Benelux BV



Diederik Perk
Threat Intelligence Advisor
Fox-IT



Raymond Bierens
Researcher
T.U. Delft



Dennis Pieterse
Senior Security Advisor
T-Systems Nederland B.V.



thuiswinkel
.org

Secure e-commerce expertgroep

shopping
tomorrow



Nick Pinto
Teamleider Fraude
Wehkamp Finance



Michel Teuwen
Senior Information Security Consultant
Jumbo Groep Holding B.V.



Thomas Stols
Cybersecurity specialist
Computest



Raymond van den Hoek
IT Security manager
Bol.com



thuiswinkel
.org

Speerpunten

- Cybersecurity informatie uitwisseling
 - Hoe kunnen we zorgen dat informatie over cyberdreigingen tijdig wordt gedeeld binnen de keten?
- Secure interfacing
 - Waar dient u op te letten bij het uitwisselen van (persoons)gegevens met partners, afnemers, leveranciers en klanten?
- Phishing
 - Welke technische en organisatorische maatregelen kunt u nemen om uw organisatie te beschermen tegen phishing aanvallen?

Er ontbreekt een specifiek platform waar informatie over cyberdreigingen en handelsperspectief wordt gedeeld voor bedrijven uit de e-commerceketen.

Cybersecurity informatieuitwisseling

- Oprichten van een e-commerce ISAC (Information Sharing and Analysis Center)
 - Grote e-commerce organisaties (PostNL, Jumbo, Bol.com, Wehkamp)
- Branchevereniging (bv Thuiswinkel.org) kan een e-commerce specifiek platform oprichten voor informatiedeling
 - Middelgrote en kleinere e-commercebedrijven



thuiswinkel
.org

**Er is teveel onduidelijkheid en
te weinig standardizatie voor
veilige informatieuitwisseling.**

Secure interfacing

- Ook wanneer ICT-gerelateerde zaken zijn uitbesteed blijft de onderneming zelf nog steeds aansprakelijk voor de correcte informatieverwerking.
- Het is als ondernemer belangrijk om goede afspraken te maken op het gebied van beveiliging.



thuiswinkel
.org

Checklist veilige gegevensuitwisseling

- Vragenlijst voor de ondernemer + leverancier/partner
- Behandelt de belangrijkste punten voor veilige gegevensuitwisseling
- Maakt inzichtelijk waar de risico's en verbeterpunten zitten
- Opgesteld door de Secure E-commerce expertgroep

Bluepaper downloaden?

- Ga naar www.shoppingtomorrow.nl/resultaten
 - Jaar 2018
 - Secure ecommerce
-

**Phishing is een groot
probleem in de e-commerce
branche.**

Phishing

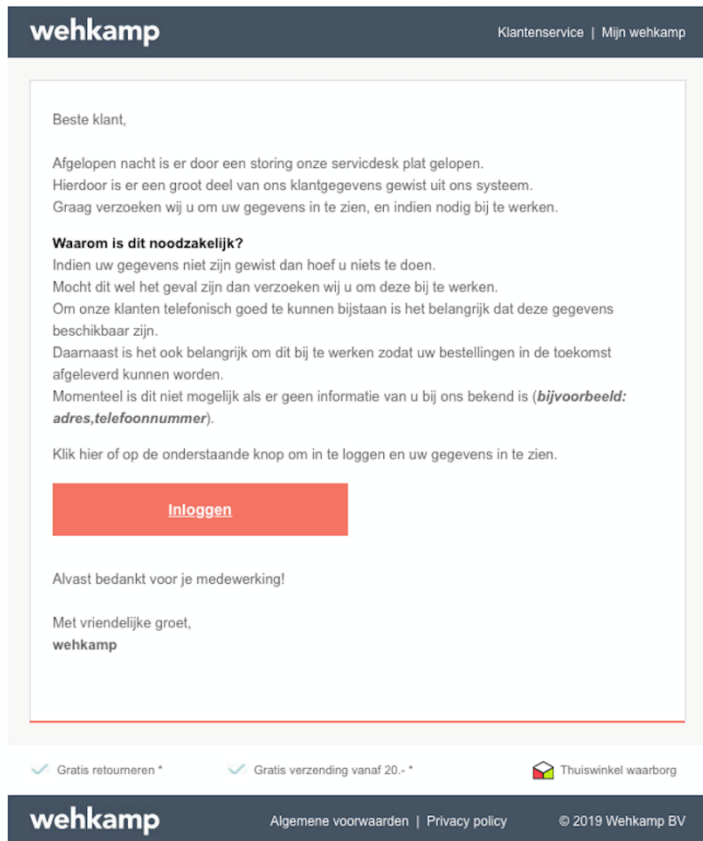
- 76% van alle organisaties (vanuit hun merknaam) wereldwijd heeft te maken gehad met phishing*
- Fraudeschade door phishing neemt toe
- In eerste halfjaar van 2018 meer dan in 2017 (1.34 mln vs 1.05 mln)
- Meest voorkomende soorten phishing
 - Deceptive phishing (inloggegevens stelen door een legitieme website te imiteren)
 - Spear phishing (gerichte aanval op een organisatie of individu)
 - CEO fraude

* Bron: <https://www.wombatsecurity.com/state-of-the-phish>



thuiswinkel
.org

Deceptive phishing



bol.com

Uw blokkade opheffen



Welkom
bij bol.com

Geachte heer/mevrouw,

Uw account is geblokkeerd vanwege misbruik. Wij vermoeden dat derden toegang hebben tot uw account en gegevens. Wij willen eventuele misbruik van uw gegevens voorkomen. Daarom hebben wij een blokkade op uw account moeten plaatsen.

U kunt de blokkade simpelweg opheffen door [hier te klikken](#) en uw gegevens te verifiëren.

Bol.com bedankt alvast al haar cliënten.

Met vriendelijke groet,
bol.com

bol.com vraagt nooit om je gegevens te verifiëren



thuiswinkel
.org

Deceptive phishing

shopping
tomorrow

gratis bezorging vanaf 20.-*

voor 23:59 uur besteld, morgen in huis*

gratis retour



veilige verbinding

Inloggen

e-mailadres

wachtwoord

toon

log in

[wachtwoord vergeten?](#)

[nieuw bij wehkamp?](#)

[maak een account](#)

wehkamp

thuiswinkel waarborg | [algemene voorwaarden](#) | [privacy](#) | [cookies](#) | [service & contact](#) | © 2018 wehkamp b.v.



thuiswinkel
.org

© ShoppingTomorrow

Deceptive phishing

shopping
tomorrow

✓ gratis bezorging vanaf 20.-* ✓ voor 23:59 uur besteld, morgen in huis* ✓ gratis retour



 veilige verbinding

Inloggen

e-mailadres

wachtwoord

log in

[wachtwoord vergeten?](#)

[nieuw bij wehkamp?](#)

maak een account

wehkamp

 thuiswinkel waarborg | [algemene voorwaarden](#) | [privacy](#) | [cookies](#) | [service & contact](#) | © 2019 wehkamp b.v.



thuiswinkel
.org

© ShoppingTomorrow

Deceptive SMS (smishing) / Whatsapp

zondag • 17:24

Uw ING is in de quarantaine zone geplaatst en dient opnieuw te worden geverifieerd. Voorkom Blokkade en volg de stappen op : <https://mijn.ing-quarantaine.nl>

Log in bij Mijn ING - ING Bankieren

Sorry, we kunnen je nu geen hulp-opties laten zien. We doen ons
mijn.ing-quarantaine.nl

zo 17:24



thuiswinkel
.org

Ik heb een nieuw nummer sinds vandaag

21:48

Ik stuur iedereen even een appje met mijn nieuwe nummer 👍

21:48

Ik wou iets verkopen via marktplaats, de koper vroeg of ik 1 cent wilde overmaken naar zijn rekening om mijn gegevens te controleren. Op een of andere manier hebben ze me hele rekening leeg geplunderd

18:41

Ik ben naar de politie gegaan en heb aangiften gedaan dus nu hopen dat ik het geld terug zie

18:42

Ohh nee. Heb zoiets een keer op het nieuws gelezen. Heb je aangifte gedaan

18:42 ✓✓

SPF



SPF voorkomt dat iemand in naam van uw organisatie een e-mail kan sturen. SPF controleert de afzender van een e-mail op echtheid.

DKIM



DKIM voorkomt vervalsing van e-mails. Als iemand knoeit met de inhoud van een e-mail, detecteert DKIM dat.

DMARC



DMARC vertelt uw mailserver wat hij moet doen als hij een verdachte e-mail ontvangt. Ook zorgt DMARC ervoor dat een organisatie informatie krijgt over vervalste e-mail die in z'n naam verstuurd is.

STARTTLS en DANE



STARTTLS zorgt voor een beveiligde verbinding tussen verzendende en ontvangende mailserver. DANE dwingt STARTTLS af en geeft zekerheid over de identiteit van de ontvangende mailserver. DNSSEC waarborgt in deze keten de echtheid van DANE



Internet.nl

IS JOUW INTERNET UP-TO-DATE?



thuiswinkel
.org

Vragen?