

# Spam herkennen

en tips om spam te stoppen en te verwijderen



# Wat is spam ?

- Spam zijn **ongevraagde berichten** vaak in de vorm van e-mails of sms'jes, die massaal worden verzonden.
- Als bedrijven dat doen onder de vorm van **reclame** hebben ze jou toestemming nodig, maar je geeft die meestal onbewust bij het ondertekenen van een klantenkaart of bij je aankopen op het internet.
- **Ongewenste berichten** (reclame) zijn niet gevaarlijk maar wel irritant. Als hackers dit doen is dat wel gevaarlijk.

# Waarom is spam gevaarlijk ?

- Het is gevaarlijk als je je door een spambericht laat verleiden gevoelige gegevens prijs te geven (**phishing**), of door op een link, of QR-code te klikken waardoor ongeoorloofd malware op je apparaat kan gedownload worden (**hacking**).
- **Malware** (malicious software) is kwaadaardige software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen.
- **Quishing** is een samentrekking van QR-code en phishing en is een nieuwe vorm van oplichting waarbij fraudeurs hun slachtoffers aanmoedigen om kwaadaardige QR-codes te scannen.

# Hoe herken je spam ?

- **Beloften** die te mooi zijn om waar te zijn. Als dure producten spotgoedkoop zijn, je een droomreis gewonnen hebt... kun je zeggen dat het spam is.
- Berichten en onderwerpen waarbij je **snel moet reageren**. Bijvoorbeeld dat je snel moet betalen of dat je een boete zal krijgen.
- **Ken je de afzender ?** Komt het e-mailadres overeen met de naam ?
- Word je **persoonlijk** aangesproken ? Dan kun je het beter vertrouwen dan als vaag met e-mailadres als aanspreking
- Als er **bijlagen** in het bericht zitten. De kans is groot dat die malware bevat.

Tik op het adres  
MediaMarkt - Afdeling

Geen persoonlijke  
aanspreektitel

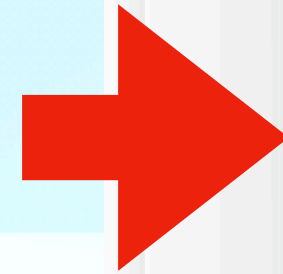
Snelle actie gevraagd



Beloften die te mooi  
zijn om waar te zijn

Link waarbij je  
doorverwezen wordt naar  
malafide adres

Hier zie je dat het e-mailadres niet klopt



Van: MediaMarkt - Afdeling >  
Aan: Papa 🐱 >

Je... nen id#sWI

**MA**

MediaMarkt  
- Afdeling

bericht bel video e-mail

Pro die op je wacht!

nende beloning is alleen zichtbaar  
nebt voltooid!

andere  
UFZ0GwX0nWy4URJwhY@naha...

Voeg toe aan vip

Blokkeer deze contactpersoon

Zoek in e-mail naar contact

Verstuur bericht

Deel contact

Maak nieuw contact

Zet in bestaand contact

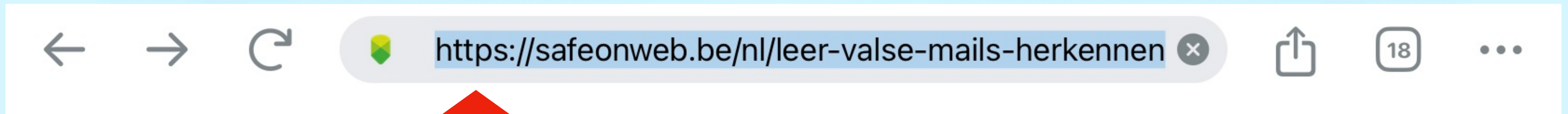
**Beloning:**  
**iPhone 15 Pro**

**Bevestig hier**

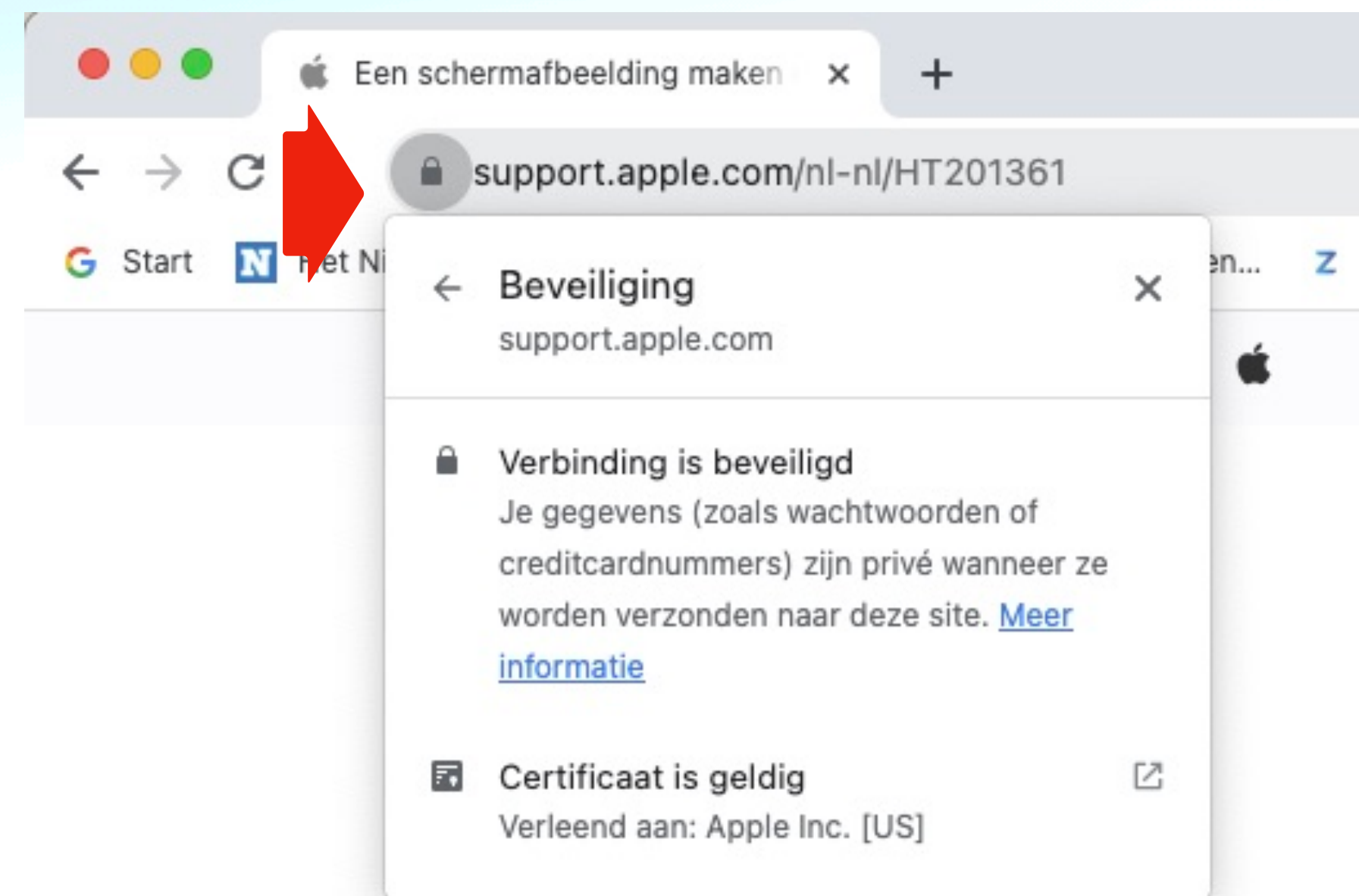
**Handtekening: FRDEVOS**

kenheid vereist om deze geweldige beloning  
en! 📣

- Kijk bij e-mails naar de url of het http:// (hyper text transfer protocol = onbeveiligd webadres) of https:// waar de beveiliging scherper is omdat gegevens versleuteld worden verstuurd



Druk op het molslotje



- **Spellingsfouten.** Meestal kennen spammers onze taal niet. Maar pas op de hackers worden ook steeds slimmer met minder taalfouten
- Is het **onverwacht**? Je kocht niets... niet vertrouwen
- **Vind je de vraag vreemd?** Een officiële instantie zal je nooit via e-mail, sms of telefoon vragen om je wachtwoord, bankgegevens of persoonlijke gegevens.
- **Naar waar leidt de link** waar je moet op klikken? Zweef met je muis over de link. Is de domeinnaam, het woord voor .be, .com, .eu, .org, ... en voor de allereerste slash ”/“, ook echt de naam van de organisatie ?
- Bijvoorbeeld: bij de link [www.safeonweb.be/tips](http://www.safeonweb.be/tips) is het domein safeonweb. Bij de link [www.safeonweb.tips.be/safeonweb](http://www.safeonweb.tips.be/safeonweb) is tips het domein en word je naar een andere website geleid.



- Probeert iemand jou **nieuwsgierig** te maken ? Kijk wat ik over jou las... of ben jij dit op de foto ? Niet vertrouwen
- Als er gevraagd wordt om een **betaling** uit te voeren die je niet verwacht, moet je altijd voorzichtig zijn.

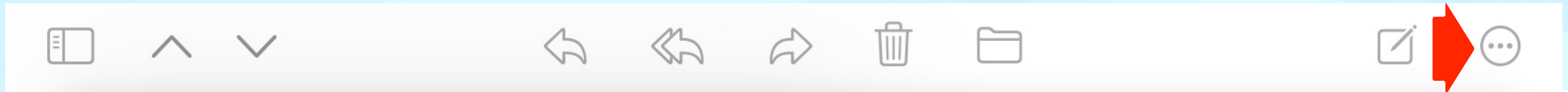
# Tips om spam te stoppen

# Verberg mijn e-mailadres gebruiken

## Enkel met een iCloud+ abonnement

'Verberg mijn e-mailadres' genereert unieke, willekeurige e-mailadressen die automatisch doorverwijzen naar je persoonlijke postbus 'Inkomend'. Elk adres is uniek voor jou. Je kunt e-mails die worden verzonden naar deze adressen, lezen en rechtstreeks beantwoorden; je persoonlijke e-mailadres blijft privé.

- **Rapporteer** spam voordat je het verwijdert. Je kunt een e-mail in Gmail als spam rapporteren door naast beantwoorden op de drie puntjes te drukken en voor “spam melden” te kiezen. Hierna kan je de spam verwijderen.



- Spam **blokkeren**, maar niet afmelden. Spam mail stoppen doe je door de afzender van het bericht te blokkeren. Soms vind je “afmelden” of “unsubscribe” link in de e-mail, pas op! deze kan je naar een website leiden die vol malware zit. Beter nog: Mail verplaatsen naar **spamfolder**, zodat hij de volgende keer in de spam map verdwijnt.

**P** **Post**  
confirm Now

📁 Ongewen...lame - Google 13 oktober 2023 23:01

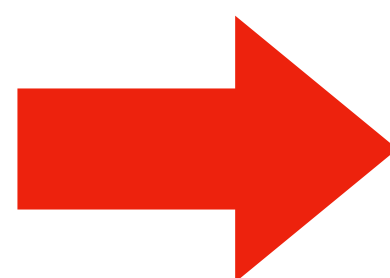
## POST

### Track your Packages Anytime, Anywhere

**We konden uw pakket niet bezorgen, omdat er niemand aanwezig was om voor de bezorging te tekenen.**

**We informeren hierbij dat we een adresbevestiging nodig hebben om de pakketverzending opnieuw te bevestigen.**

**HIER CONTROLEREN**



unsub [here](#)

# Wat te doen als je een verdacht bericht krijgt?

- **Klik niet op de link** in een verdacht bericht, open de bijlages niet en download geen applicaties als daar om gevraagd wordt.
- Verdachte e-mails kan je doorsturen naar [verdacht@safeonweb.be](mailto:verdacht@safeonweb.be)
- Verdachte sms'jes kan je ook doorsturen. Maak een **screenshot** en verstuur die naar [verdacht@safeonweb.be](mailto:verdacht@safeonweb.be). De inhoud wordt dan automatisch verwerkt.

# Heb je op een verdachte link geklikt?

- Als je wel geklikt hebt, vul de velden verder niet in en **breek elke interactie af**.
- Geef NOOIT **persoonlijke gegevens** of **codes** door.
- Als je een wachtwoord hebt doorgegeven dat je ook op andere plaatsen gebruikt, **verander** het dan onmiddellijk.
- Als je op een link hebt geklikt die opent in een website waar je bankgegevens moet indienen, **controleer** dan eerst of dit de echte website van je bank is. Bij de minste twijfel voer je geen betaling uit

# ... en tot slot

- Merk je dat er **namens jou** rare berichten verstuurd worden? Waarschuw jou contacten dat je hen een vals bericht hebt doorgestuurd.
- Installeer de **safeonweb extensie** in je browser. Deze zal je waarschuwen als je een onveilige website bezoekt en wanneer het gevaarlijk is om je gegevens in te voeren.
- In de App Store kan je de Safeonweb **app** downloaden. Daar vind je informatie over veel voorkomende verdachte berichten. Zo ben je snel op de hoogte wanneer verdachte berichten de ronde doen.
- Een laatste tip: Neem 10 minuten de tijd en leer verdachte berichten herkennen door eens naar [surfenzonderzorgen.safeonweb.be](https://surfenzonderzorgen.safeonweb.be) e-learning te surfen.



# Einde

- Bronnen:
- Nord VPN
- Seniorweb
- Safeonweb
- Appletips