

# Scammers worden slimmer in waar ze je targeten

## Nieuw onderzoek van Malwarebytes laat zien hoe verschillende scams worden afgestemd op verschillende platforms

Scammers gaan strategischer te werk bij het kiezen van waar ze mensen benaderen.

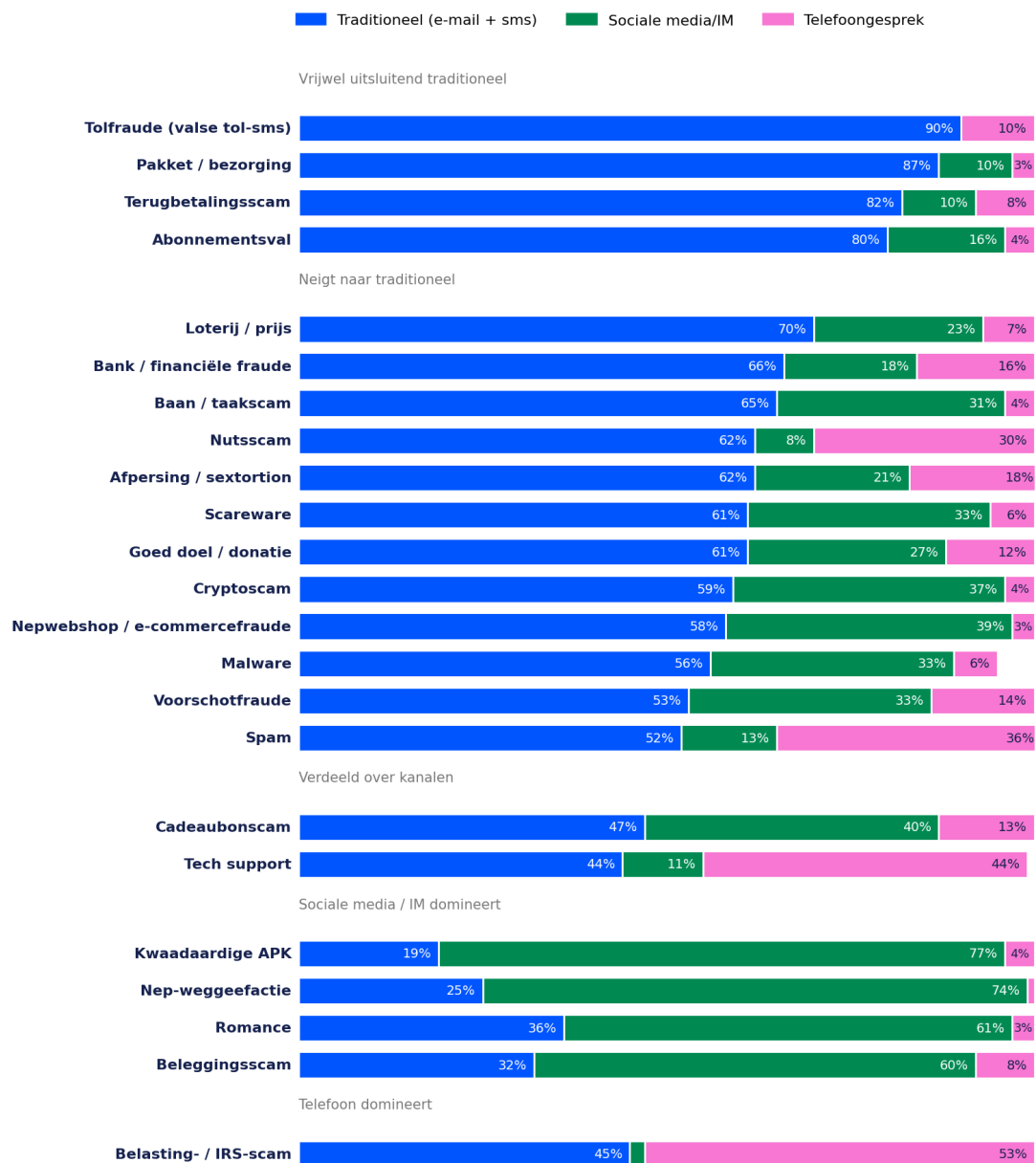
Negen van de tien gevallen van tolfraude – de valse sms'jes en e-mails over onbetaalde tol die dreigen met boetes of intrekking van je rijbewijs – komen binnen via e-mail of sms, terwijl ongeveer zes van de tien romance scams zich op sociale media afspelen. Dat is geen toeval. In plaats van overal hetzelfde bericht te verspreiden, stemmen criminelen verschillende scams af op de platforms waar ze de meeste kans van slagen hebben.

Deze bevinding komt uit de eigen threat-researchsystemen van Malwarebytes en is gebaseerd op wereldwijde gegevens van 15 april tot en met 14 juli 2026. Het onderzoek laat zien hoe scammers hun tactieken aanpassen en geeft nieuwe inzichten over waar ze opduiken, wanneer ze toeslaan en welke merken ze nabootsen.

Hieronder de belangrijkste bevindingen.

### Elke scam heeft een favoriet platform

Je krijgt veel eerder een nep-weggeefactie (giveaway-scam) te zien in je socialemediafeed dan via e-mail of sms. Aan de andere kant komt de helft van alle IRS-scams binnen via een telefoontje. Malwarebytes onderzocht meer dan 20 soorten scams, van tech support- en terugbetalingsscams tot sextortion en scareware, en ontdekte dat elke soort een bepaald platform verkiest. Vanzelfsprekend sluit het favoriete platform vaak aan bij de inhoud van de scam: vacaturescams komen meestal binnen via gebruikelijke werkkanalen zoals e-mail, romance scams meestal via sociale media, waar contact met vreemden het minst in twijfel wordt getrokken, en tech support-scams meestal via de telefoon. Het kanaal bepaalt ook hoe de scam aanvoelt: een DM voelt persoonlijk, terwijl een telefoongesprek druk legt om meteen te reageren. Eerder onderzoek laat bovendien zien dat scammers vaak herhalen wat werkt, wat zou kunnen verklaren waarom ze blijven doen wat ze tot nu toe deden.

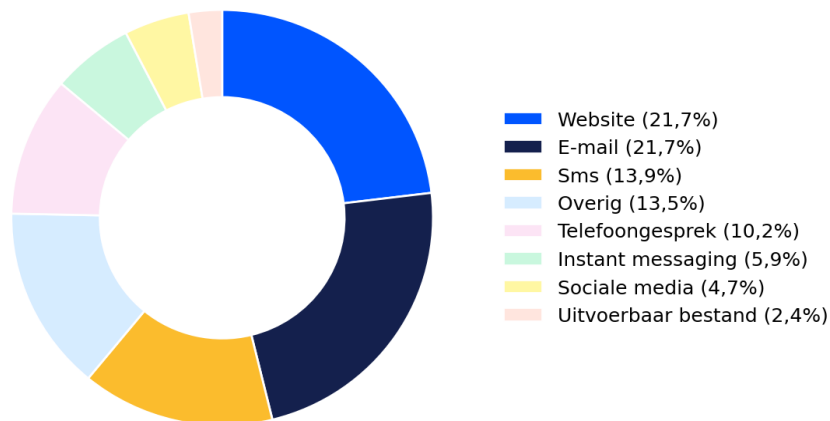


Elke scam heeft een favoriet platform (bron: Malwarebytes)

## Het web wint nog steeds

Ondanks de opkomst van sociale media en berichtenapps bereiken scams ons nog altijd vaker via het web dan via enig ander platform, gevolgd door e-mail en sms.

Het is geen verrassing dat het web de populairste toegangspoort is. Malwarebytes blokkeert ongeveer 500.000 phishingwebsites per dag.



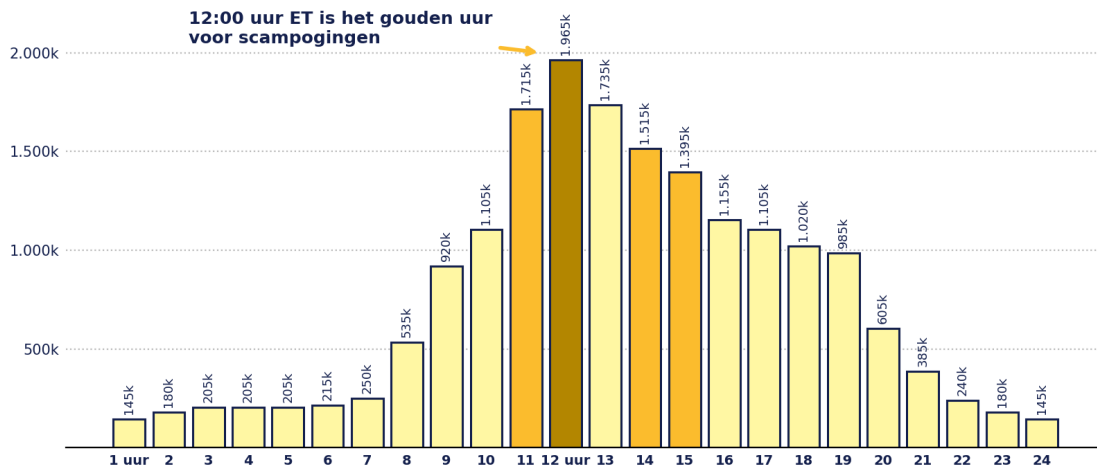
Kanalen waarlangs scams ons bereiken (bron: Malwarebytes)

### MrBeast verslaat Trump

Hij is al de populairste YouTuber ter wereld, beroemd om zijn online capriolen en extreme stunts, maar volgens de gegevens van Malwarebytes kan “MrBeast” daar nu “meest nagebootste persoon” aan toevoegen. Hij laat Elon Musk en Donald Trump (respectievelijk nummer twee en drie) ruimschoots achter zich. MrBeast, echte naam Jimmy Donaldson, is de favoriet van scammers die willen meeliften op zijn bekendheid: zijn gezicht wordt gebruikt in zo’n 30% van de nabootsingsscams, van cryptogiveaways tot oplichting met overboekingskosten. Bekende gezichten verlagen de waakzaamheid en maken scamberichten geloofwaardiger, en daarom werken ze zo goed. Dus als MrBeast de volgende keer in je feed opduikt en je vraagt geld te sturen als onderdeel van een verificatie: pas op.

### 12:00 uur ET is het “gouden uur” voor scammers die Amerikanen targeten

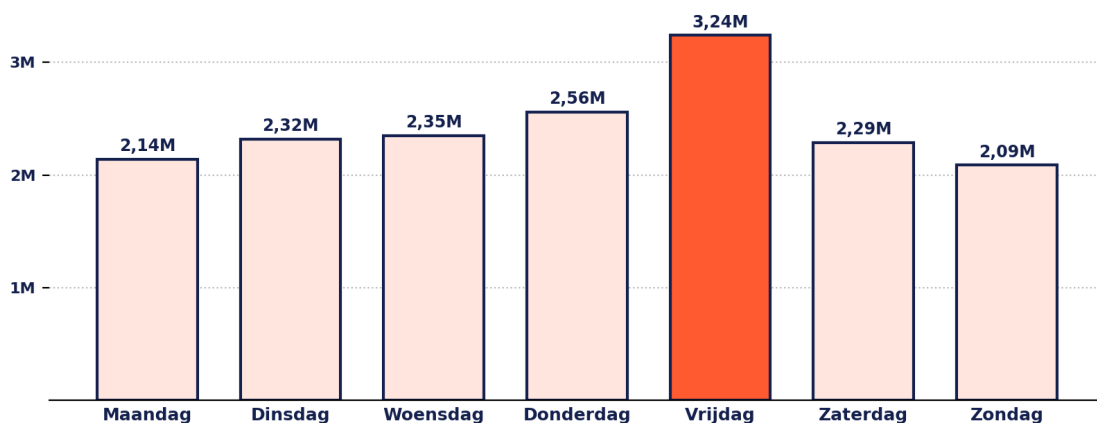
Als je aan de Amerikaanse oostkust woont, is lunchtijd ook scantijd. Volgens Malwarebytes is het 12:00 uur het gouden uur voor scamsms’jes en is het dan ruwweg 874% drukker dan op het rustigste moment, 1:00 uur ’s nachts ET.



Scampogingen per uur, ET (bron: Malwarebytes; waarden gemeten in de grafiek, bij benadering)

## Scamsms'jes pieken op vrijdag

Het aantal scamberichten op je telefoon neemt in de loop van de week toe. Vanaf een dieptepunt op zondag stijgt de frequentie gestaag tot een piek op vrijdag. Op het moment dat je van je werk vertrekt en je op het weekend voorbereidt, krijg je dus ongeveer 50% meer frauduleuze sms'jes te verwerken dan aan het begin van de week. De gegevens zeggen niet waarom, maar ze suggereren wel dat scammers hun campagnes bewust timen in plaats van willekeurig berichten te sturen.



Scampogingen per dag (bron: Malwarebytes; waarden gemeten in de grafiek, bij benadering)

## Grote merken zijn big business voor scammers

De grootste merken van de wereld zijn ook enkele van de nuttigste voor scammers. Ze zijn direct herkenbaar, worden door honderden miljoenen mensen gebruikt en maken al deel uit van ons dagelijks leven, waardoor ze zich lenen voor alles van nepaanbiedingen tot valse accountmeldingen. Op basis van meldingen van Malwarebytes-gebruikers zijn de vijf meest nagebootste merken:

- Google
- Microsoft
- Apple

- **Roblox**
- **Amazon**

Volgens Malwarebytes-gebruikers werd de merknaam van Google minstens twee keer zo vaak misbruikt als die van Amazon.

## Gaming wordt een groter doelwit

Scammers richten zich steeds vaker op gamingcommunity's. Volgens gegevens van Malwarebytes Scam Guard kan ongeveer de helft van alle gamingscams leiden tot een financieel verlies van \$1.000 of meer, wat Malwarebytes een "hoog-risico" noemt. De meest nagebootste gamingsites waren Roblox, Steam, Discord en Minecraft. Roblox zag van half juni tot half juli een stijging van 15% in scamactiviteit, Steam over dezelfde periode een stijging van 19%.

## Zo herken en stop je scams

De gegevens wijzen op een scameconomie die steeds meer gespecialiseerd raakt. In plaats van generieke campagnes stemmen criminelen scams af op de platforms die we dagelijks gebruiken, van e-mail en sms tot gamingcommunity's en sociale media. De tactieken kunnen veranderen, maar het doel blijft hetzelfde: lang genoeg je vertrouwen winnen om je geld of je gegevens te stelen. Als je weet hoe die tactieken per platform verschillen, zijn ze makkelijker te herkennen en dus makkelijker te vermijden.

### Algemeen:

- Klik niet op links en bel geen telefoonnummers uit ongevraagde e-mails, sms-berichten of DM's op sociale media.
- Controleer bij twijfel of een bericht echt is door rechtstreeks naar de officiële website van het bedrijf te gaan en er via officiële kanalen naar te vragen. Volg daarbij geen gesponsorde zoekresultaten; die kunnen scams zijn.
- Geef geen persoonlijke gegevens, pincodes, wachtwoorden, betaalgegevens of verificatiecodes door tijdens een ongevraagd telefoontje. Legitieme bedrijven vragen nooit telefonisch om wachtwoorden of verificatiecodes. Hang op en bel terug via het officiële telefoonnummer van de organisatie.
- Gebruik een browserextensie die scam- en phishingsites blokkeert, zoals Malwarebytes Browser Guard. Die kan een nepwebwinkel signaleren voordat je er belandt, ook als die nog niet eerder is gezien.
- Installeer een mobiel beveiligingsproduct zoals Malwarebytes Mobile Security, dat scam- en spamsms'jes uitfiltert.
- Controleer of een bericht legitiem is. Malwarebytes Scam Guard kan een bericht, telefoonnummer of link vergelijken met de uitgebreide threat intelligence-database om vast te stellen of het kwaadaardig of veilig is. Het geeft vervolgens informatie over waarschuwingssignalen en de vervolgstappen die je moet nemen. Scam Guard markeert ongeveer één op de vijf geanalyseerde sessies als hoog risico: situaties die kunnen leiden tot aanzienlijke financiële verliezen (\$1.000 of meer) of persoonlijke schade.

## Methodologie

De gegevens in dit rapport komen uit de eigen threat-researchsystemen van Malwarebytes en zijn verzameld tussen 15 april en 14 juli 2026. Alle gegevens zijn geanonimiseerd en geven weer wat Malwarebytes kan waarnemen via de eigen infrastructuur.

---

Nederlandse vertaling van het Malwarebytes Scam Report (september 2026). De grafieken zijn opnieuw getekend op basis van de oorspronkelijke grafieken; de percentages in de platformgrafiek en de cirkeldiagram komen uit het origineel. Het rapport noemt voor de uur- en daggrafiek zelf geen exacte aantallen; de weergegeven waarden zijn nauwkeurig gemeten in de vectorgrafiek (afwijking ruwweg 1%) en dus geen officiële cijfers van Malwarebytes.