Memo

Van : Programma Digitale Veiligheid en Cybercrime
Aan : Politie, OM en Gemeenten (Communicatie)
Datum : 5 november 2024
Onderwerp : Standaard tekstblokken aankoopfraude in aanloop van Black Friday en Cyber Monday

Aanleiding

De toenemende populariteit van Black Friday en Cyber Monday brengt jaarlijks een piek in online aankopen, maar ook in online fraude, wat aankoopfraude tot de meest voorkomende vorm van gedigitaliseerde criminaliteit maakt (CBS, 2023). Dit biedt ons als overheid de gelegenheid om gezamenlijk te communiceren om inwoners bewust te maken en handelingsperspectief te bieden tegen deze vorm van criminaliteit. Zo voorkomen we slachtofferschap.

Doel

Het doel van deze memo is om partners te ondersteunen bij de communicatie over aankoopfraude, met een nadruk op het voorkomen van slachtofferschap. Door bewustwording en praktisch advies te bieden, vergroten we de weerbaarheid van inwoners en verkleinen we de kans dat zij slachtoffer worden.

De memo biedt:

- Een overzicht van het doel en de doelgroep
- Tips voor een integrale communicatieaanpak
- Drie voorbeeldberichten om via diverse kanalen te delen

Doelgroepen

Uit gegevens blijkt dat voornamelijk 25- tot 65-jarigen het vaakst slachtoffer zijn van aankoopfraude (CBS, 2023). Deze memo richt zich daarom op deze groep en nodigt hen uit om bewust en alert te blijven bij online aankopen.

Integraal communiceren

Gedigitaliseerde criminaliteit zoals aankoopfraude is aantrekkelijk voor daders vanwege de geringe pakkans en de mogelijkheid om vanaf een scherm grote aantallen potentiële slachtoffers te bereiken. Onze kernboodschap is dat wij als gezamenlijke overheid alles in het werk stellen om fraudeurs op te sporen en te vervolgen.

Voorbeeldberichten

Om te communiceren via eigen middelen en lokale pers over aankoopfraude hebben we enkele voorbeeldberichten toegevoegd die naar eigen inzicht kunnen worden aangepast:

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl

VARIANT 1:

Black Friday; kijk uit voor nepwebshops

29 november is het weer Black Friday; een dag waarop veel consumenten hun slag slaan. Zowel in gewone winkels als online staat vaak de hele week in het teken van de beste aanbiedingen en kortingen. Je zou eigenlijk wel gek zijn als je al dat moois liet lopen, toch? Maar pas op; online pikken criminelen graag een graantje mee van de aankoopgekte. Schimmige websites en oplichtingspraktijken komen rond deze populaire koopdag helaas steeds vaker voor.

Wil je veilig winkelen? Check dan deze tips:

1. **Controleer de website**: Zorg dat je koopt bij bekende en betrouwbare webwinkels. Kijk naar beoordelingen en controleer of de website veilig is. De politie biedt een handige online tool: Check de Verkoper, waarmee je kunt zien of een verkoper bekend is bij de politie.
2. **Een aanbieding die te mooi is om waar te zijn, is dat waarschijnlijk ook. Is de prijs veel lager dan d**e marktprijs? Wees dan voorzichtig. Heb je nog maar een uur om te beslissen of zijn er nog maar twee stuks van een artikel beschikbaar? Dit soort praktijken zijn vaak verboden en bedoeld om je onder druk te zetten om snel een aankoop te doen.
3. **Gebruik veilige betalingsmethoden**: Vermijd het gebruik van bankoverschrijvingen en kies voor veilige betaalmethoden zoals iDEAL of creditcard.
4. **Wees voorzichtig met persoonlijke gegevens**: Geef niet meer informatie prijs dan nodig is. Vertrouw websites die om onnodige gegevens vragen niet.
5. **Controleer de retourvoorwaarden en contactmogelijkheden**: Een betrouwbare webshop heeft duidelijke retour- en verzendvoorwaarden. Kan je de contactgegevens niet vinden of alleen in het buitenland? Let dan extra op.
6. **Een mooie aanbieding in je mailbox? Kijk uit:** Criminelen proberen niet alleen hun slag te slaan via nepwebshops, ook het aantal phishingmails neemt vanaf half november enorm toe. Let altijd goed op wie de afzender is en klik niet op een link als je de mail niet vertrouwt.

Maar shoppen is toch vooral leuk?
Zeker! Maar laat je niet misleiden door (te) mooie aanbiedingen. Door met gezond verstand en bovenstaande tips in het achterhoofd online te shoppen, zorgen we ervoor dat Black Friday een prettige en vooral veilige dag voor iedereen is!

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl

VARIANT 2:

Black Friday; mooie aankoop of financiële puinhoop?

Wil jij Black Friday 29 november online je slag slaan? Kijk dan uit voor oplichters. Ieder jaar rond deze datum neemt het aantal nepwebshops enorm toe. Door de vele aanbiedingen valt die ene aanbieding die écht te mooi is om waar te zijn, waarschijnlijk niet meer zo snel op. Check daarom extra of je met een betrouwbare website te maken hebt. Lees de tips op de site van **de politie**.

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl

VARIANT 3: REFERENTIE AAN LANDELIJKE CAMPAGNE 'LAAT JE NIET INTERNEPPEN'

Aanbieding te goed om waar te zijn? Laat je niet interneppen. Check de afzender en bij twijfel: klik weg!

Rondom de feestdagen vliegen de aanbiedingen je om de oren. Criminelen, ofwel interneppers maken daar ook graag gebruik van. Ze doen zich voor als een bekende of een winkelmedewerkers en schotelen je een prachtige korting voor van maar liefst 60 procent! Moet je wel binnen een uur reageren en even op een link van ze klikken. Laat je niet interneppen, check altijd de afzender en als je twijfelt: klik weg.

Mensen kopen steeds meer en vaker online. Verkopers proberen jou op allerlei manieren te verleiden tot impulsaankopen. Vooral rondom de feestdagen maken criminelen, ofwel interneppers daar ook graag gebruik van. Door zich voor te doen als iemand anders en jou via e-mail, sms of WhatsApp te benaderen met een goede deal, krijgen criminelen het voor elkaar om je op het verkeerde been te zetten. Een internepper maakt daarbij gebruik van 'Social Engineering'. Dit is een term voor wisselende trucjes waarmee mensen online worden bedrogen.

Hoe herken je nepberichten?
• Je krijgt weinig bedenktijd: de internepper geeft je geen tijd om na te denken, dringt constant aan, blijft vriendelijk en benadrukt dat je direct moet handelen.
• Het bericht heeft een dwingende toon: de zogenaamde 'bekende' of 'instantie' verwacht dat je iets betaalt, je wordt gevraagd om op een link te klikken, of je wordt aangespoord om iets te downloaden.
• De situatie loopt uit de hand: je krijgt een aanbieding die te mooi is om waar te zijn, je bent nieuwsgierig naar een filmpje of er wordt dringend om jouw hulp gevraagd.

Wat kan je zelf doen?
• Check de afzender: controleer altijd van wie het bericht komt.
• Neem via het bij jou bekende telefoonnummer of e-mailadres contact op als je de afzender niet herkent.
• Let extra goed op bij vreemde e-mailadressen en links, nooit direct klikken.
• Deel niet te veel informatie op social media.
• Deel je wachtwoord niet met anderen.
• Bij twijfel: klik weg.

laatjenietinterneppen.nl
'Laat je niet interneppen' is een landelijke campagne die mensen helpt om online misleiding te herkennen én te voorkomen. Wil je meer lezen over hoe interneppers te werk gaat en wat jij kunt doen om dit te voorkomen? Bekijk de tips laatjenietinterneppen.nl.

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl