



Cybercriminelen vissen naar gegevens van nabestaanden via rouwberichten

*DELA waarschuwt voor phishing op herdenkingspagina's:
"Oplichters slaan toe op het moment dat families het kwetsbaarst zijn"*

Phishers deinzen nergens voor terug: ze misbruiken zelfs rouw om nabestaanden gegevens en geld af te troggelen. Uitvaartspecialist DELA veroordeelt scherp deze laakbare praktijken en waarschuwt gebruikers voor phishingpogingen via het online condoleanceplatform Ingedachten.be, waar mensen hun medeleven kunnen betuigen via rouwberichten. Het bedrijf neemt ook aanvullende technische maatregelen. De voorbije drie maanden kwamen er, tussen zo'n 45.000 rouwbetuigingen, een honderdtal meldingen binnen van verdachte berichten. Daarbij doen criminelen zich bijvoorbeeld voor als advocaat, verzekeraar of notaris.

"Geachte mevrouw, wij zijn op de hoogte gebracht van het overlijden en willen u informeren over een levensverzekering op naam van de overledene. Stuur ons alstublieft uw e-mailadres zodat wij u de documenten voor de uitkering van de premie kunnen toesturen, of neem per e-mail contact met ons op voor meer informatie."

Deze en gelijkaardige boodschappen duiken op tussen oprechte rouwbetuigingen op de herdenkingspagina [Ingedachten.be](https://www.ingedachten.be) van DELA. Op het eerste gezicht lijkt het een behulpzaam bericht van een verzekeraar, maar in werkelijkheid gaat het om phishing. Fraudeurs proberen zo het vertrouwen van nabestaanden te winnen om hen aan te zetten tot het delen van persoonlijke gegevens en later tot het uitvoeren van betalingen, vaak onder het mom van administratieve kosten of een uitkering.

Caroline Hombroux, verantwoordelijk voor Ingedachten.be: "Oplichters spelen heel doelbewust in op emotie en vertrouwen. Ze weten dat mensen in rouw soms minder alert zijn en sneller geneigd zijn om te reageren, zeker wanneer een bericht dringend of officieel klinkt. Net daarom zijn deze praktijken zo laakbaar: ze maken misbruik van een kwetsbaar moment om mensen financieel en emotioneel te raken."

Steeds slinkser en volhardender

Phishing is geen nieuw fenomeen, maar de aanpak wordt wel geraffineerder. Fraudeurs slaan op grotere schaal toe en gebruiken telkens nieuwe e-mailadressen om berichten te versturen,

vaak met identieke inhoud. Ze proberen een persoonlijk contact op te starten om het gesprek buiten het platform verder te zetten. Een op het eerste gezicht onschuldige vraag, blijkt in de praktijk vaak de eerste stap naar verdere oplichting.

Caroline Hombroukx, verantwoordelijk voor Ingedachten.be: "Fraudeurs doen zich niet alleen voor als officiële instanties, ze stellen ook ogenschijnlijk onschuldige vragen, bijvoorbeeld om een overlijdensbericht door te sturen. Wat onschuldig lijkt, evolueert vaak snel naar een gerichte poging om gegevens te verzamelen of vertrouwen op te bouwen. We zien dat ze bijzonder volhardend zijn: zodra hun pogingen onderschept worden en hun adres geblokkeerd wordt, duiken ze op met nieuwe accounts en blijven ze dezelfde tactieken herhalen. Zo ontvingen we de voorbije drie maanden een honderdtal meldingen van verdachte berichten, of één melding per dag, op een totaal van 45.000 rouwbetuigingen."

Extra maatregelen

Om dit soort fraude tegen te gaan en het risico te beperken, zet DELA verder in op een combinatie van sensibilisering en technische ingrepen. Zo staat er een duidelijke waarschuwing bovenaan op het platform en kunnen bezoekers verdachte berichten onmiddellijk signaleren via een eenvoudige meldpuntknop. Frauduleuze afzenders worden geblokkeerd en vervolgens op een blacklist geplaatst. Ook het aantal privé rouwberichten dat per IP-adres kan worden verzonden, is beperkt om misbruik tegen te gaan.

Bij privécondoleances worden nabestaanden extra gewaarschuwd en kunnen ze verdachte berichten meteen melden. Dit voorjaar volgen nog bijkomende systemen, zoals automatische detectie.

Caroline Hombroukx, verantwoordelijk voor Ingedachten.be: "Phishing is vandaag een breder maatschappelijk probleem. Je ziet het in alle sectoren en jammer genoeg dus ook in de context van rouw. We blijven het platform actief beveiligen en verfijnen onze maatregelen voortdurend. Tegelijk blijft waakzaamheid cruciaal. Daarom zetten we sterk in op sensibilisering, ook tijdens de regelgesprekken bij de uitvaartondernemer, zodat mensen de signalen herkennen en niet ingaan op misleidende berichten. We zien immers hoe belangrijk het digitale rouwregister is voor families: het informeert, brengt mensen samen en biedt steun in een moeilijk moment. Net daarom willen we deze omgeving maximaal beschermen en vrijwaren."

5 tips om niet in de val te lopen van phishers

Wat moet je doen als je als nabestaande op deze manier gecontacteerd wordt of als bezoeker zo'n bericht opmerkt?

1. *Vertrouw geen berichten van zogenaamde verzekeraars, notarissen of advocaten via een condoleanceplatform.*

Juridische en financiële dienstverleners nemen nooit op die manier contact op over dossiers of nalatenschappen.

2. Deel nooit contactgegevens of andere persoonlijke gegevens

Fraudeurs proberen vaak eerst informatie te verzamelen om later verder privé contact op te nemen. Iemand met goede bedoelingen zal geen contactgegevens via een herdenkingspagina vragen.

3. Wees extra waakzaam tijdens kwetsbare momenten en voor emotionele of dringende boodschappen.

Phishers maken misbruik van kwetsbare momenten en spelen in op tijdsdruk om je sneller te laten reageren. Wees je hiervan bewust en laat je goed omringen.

4. Ga niet in op verzoeken om documenten door te sturen.

Vragen zoals “kan je het overlijdensbericht bezorgen?” zijn vaak een eerste stap in oplichting.

5. Meld verdachte berichten meteen via de meldingsknop en zoek advies bij twijfel.

Door verdachte berichten te melden, help je anderen te beschermen. Twijfel je over een bericht? Neem contact op met familie, vrienden, DELA of een officiële instantie.