



Les cybercriminels cherchent à soutirer des données aux proches du défunt via des messages de condoléances

*DELA met en garde contre le phishing sur les pages commémoratives :
« Les escrocs frappent au moment où les familles sont les plus vulnérables »*

Des cybercriminels spécialisés dans le hameçonnage sont prêts à tout : ils vont jusqu'à abuser du deuil pour soutirer des données et de l'argent aux proches. Le spécialiste funéraire DELA condamne fermement ces pratiques répréhensibles et met en garde les utilisateurs contre les tentatives de phishing via la plateforme de condoléances en ligne Dansnospensees.be, où les gens peuvent exprimer leur sympathie par le biais de messages de condoléances. L'entreprise prend également des mesures techniques supplémentaires. Au cours des trois derniers mois, une centaine de signalements de messages suspects ont été reçus sur quelque 45 000 messages de condoléances. Les criminels se font, par exemple, passer pour un avocat, un assureur ou un notaire.

« Chère Madame, nous avons été informés du décès et souhaitons vous informer de l'existence d'une assurance-vie au nom du défunt. Veuillez nous envoyer votre adresse e-mail afin que nous puissions vous faire parvenir les documents nécessaires au versement de la prime, ou contactez-nous par e-mail pour plus d'informations. »

Ce message et d'autres messages similaires apparaissent parmi les sincères condoléances sur la page commémorative [Dansnospensees.be](https://dansnospensees.be) de DELA. À première vue, ils ressemblent à un message utile d'un assureur, mais il s'agit en réalité d'une tentative de phishing. Les fraudeurs tentent ainsi de gagner la confiance des proches afin de les inciter à partager des données personnelles et, par la suite, à effectuer des paiements, souvent sous couvert de frais administratifs ou d'un versement.

Caroline Hombroux, responsable de Dansnospensees.be : *« Les escrocs jouent délibérément la carte de l'émotion et de la confiance. Ils savent que les personnes en deuil sont parfois moins attentives et sont plus enclines à réagir, surtout lorsqu'un message semble urgent ou officiel. C'est précisément la raison pour laquelle ces pratiques sont si condamnables : elles exploitent un moment de vulnérabilité pour porter atteinte aux personnes sur les plans financier et émotionnel. »*

De plus en plus sournois et tenaces

Le phishing n'est pas un phénomène nouveau, mais ses mécanismes sont de plus en plus sophistiqués. Les fraudeurs agissent à plus grande échelle et utilisent sans cesse de nouvelles adresses e-mail pour envoyer des messages, souvent au contenu identique. Ils tentent d'établir un contact personnel afin de poursuivre la conversation en dehors de la plateforme. Une question innocente à première vue s'avère souvent, en pratique, être la première étape vers une escroquerie plus élaborée.

Caroline Hombroux, responsable de Dansnospensees.be : « Les fraudeurs ne se font pas seulement passer pour des instances officielles, ils posent également des questions apparemment innocentes, par exemple, pour transmettre un avis de ils posent également des questions qui paraissent, à première vue, innocentes, par exemple pour transmettre un avis de décès. Ce qui semble innocent évolue souvent rapidement vers une tentative ciblée de collecter des données ou d'établir une relation de confiance. Nous constatons qu'ils sont particulièrement tenaces : dès que leurs tentatives sont déjouées et que leur adresse est bloquée, ils réapparaissent avec de nouveaux comptes et continuent à répéter les mêmes tactiques. Ainsi, au cours des trois derniers mois, nous avons reçu une centaine de signalements de messages suspects, soit un signalement par jour, sur un total de 45 000 messages de condoléances. »

Mesures supplémentaires

Pour lutter contre ce type de fraude et limiter le risque, DELA continue de miser sur une combinaison de sensibilisation et d'interventions techniques. Ainsi, un avertissement clair figure en haut de la plateforme et les visiteurs peuvent immédiatement signaler les messages suspects via un simple bouton de signalement. Les expéditeurs frauduleux sont bloqués puis blacklistés. Le nombre de messages de condoléances privés pouvant être envoyés par adresse IP est également limité afin de lutter contre les abus.

Dans le cas des condoléances privées, les proches sont davantage mis en garde et peuvent signaler immédiatement les messages suspects. D'autres systèmes tels que la détection automatique seront mis en place ce printemps.

Caroline Hombroux, responsable de Dansnospensees.be : « Le phishing est aujourd'hui un problème sociétal plus large. On le constate dans tous les secteurs et, malheureusement, également dans le contexte du deuil. Nous continuons à sécuriser activement la plateforme et affinons constamment nos mesures. En même temps, la vigilance reste cruciale. C'est pourquoi nous misons fortement sur la sensibilisation, notamment lors des entretiens avec l'entrepreneur de pompes funèbres, afin que les gens reconnaissent les signaux et ne donnent pas suite à des messages trompeurs. Nous constatons en effet à quel point le registre de deuil numérique est important pour les familles : il informe, rassemble les gens et offre un soutien dans un moment difficile. C'est précisément la raison pour laquelle nous voulons protéger et préserver au maximum cet environnement. »

Cinq conseils pour ne pas tomber dans les filets des hameçonneurs

Que faire si, en tant que proche, vous êtes contacté de cette manière ou si, en tant que visiteur, vous remarquez un tel message ?

1. Ne faites pas confiance aux messages provenant de prétendus assureurs, notaires ou avocats via une plateforme de condoléances.

Les prestataires de services juridiques et financiers ne prennent jamais contact de cette manière au sujet de dossiers ou de successions.

2. Ne partagez jamais vos coordonnées ou d'autres données à caractère personnel

Les fraudeurs tentent souvent de collecter d'abord des informations pour vous contacter ensuite en privé. Une personne bien intentionnée ne demandera pas vos coordonnées via une page de commémoration.

3. Soyez particulièrement vigilant(e) dans les moments de vulnérabilité et face à des messages émotionnels ou urgents.

Les hameçonneurs profitent de moments de vulnérabilité et jouent sur la pression du temps pour vous pousser à réagir plus vite. Soyez conscient(e) de ce piège et entourez-vous de personnes de confiance.

4. Ne répondez pas aux demandes de transmission de documents.

Des questions telles que « pouvez-vous nous envoyer l'avis de décès ? » constituent souvent la première étape d'une escroquerie.

5. Signalez immédiatement les messages suspects via le bouton de signalement et demandez conseil en cas de doute.

En signalant les messages suspects, vous contribuez à protéger les autres. Vous avez des doutes concernant un message ? Contactez votre famille, vos amis, DELA ou une autorité officielle.