Kalimèra / il y a dix sept années
Conseil de sécurité
Conseils de sécurité pour éviter les fausses cartes électroniques
Publié le : 14/12/2004

Liens connexes
• Cartes électroniques : votre message est-il confidentiel ?
• Choses à faire et à ne pas faire avec les courriers indésirables
• Comment éviter les courriers indésirables
• Cartes de vœux originales : créez des cartes uniques

Grâce à Internet, il est désormais facile et peu coûteux d'envoyer une carte de vœux. Il existe actuellement un grand nombre de sociétés et de services proposant des cartes électroniques, et la plupart sont fiables et faciles à utiliser. Malheureusement, les pirates, les escrocs et les pornographes utilisent eux aussi les cartes électroniques pour leurrer les utilisateurs peu vigilants.

Le nombre de fausses cartes électroniques envoyées est inconnu, mais selon McAfee Security , divers problèmes, simplement ennuyeux ou réellement destructeurs, peuvent découler de ces falsifications. Une carte de vœux factice, une fois ouverte ou téléchargée, peut présenter les risques suivants :

• Un spam qui affiche des images pornographiques ou autres images indésirables sur votre bureau, lance des sites Web pour adultes ou vous infeste de fenêtres publicitaires (même quand vous n'êtes pas sur Internet).

• Un virus informatique qui analyse vos adresses électroniques et envoie une fausse carte électronique à vos contacts personnels et professionnels, généralement sans vous en avertir. Vous pouvez même apparaître comme l'expéditeur de cette fausse carte électronique et de ce virus.

Pas de panique. Avec un minimum de connaissances et de prudence, il est facile d'éviter les fausses cartes électroniques et de discerner les vraies. Il suffit d'appliquer les mêmes principes de précaution que pour chaque courrier électronique que vous recevez.

Comment éviter les fausses cartes électroniques ?
Voici quelques principes élémentaires pour éviter d'ouvrir et d'envoyer de fausses cartes électroniques :

• Ne téléchargez rien et ne cliquez sur rien provenant d'une source inconnue.

• Méfiez-vous des messages électroniques ou des pièces jointes paraissant douteux ou provenant de quelqu'un que vous ne connaissez pas.

• Installez un logiciel antivirus édité par une société connue et mettez-le régulièrement à jour (cependant, ne comptez pas uniquement sur le logiciel antivirus pour assurer votre sécurité).

• Prévisualisez l'adresse Web d'un lien avant de cliquer dessus ; si le lien n'indique aucune adresse, placez votre souris dessus (mais sans cliquer) pour voir l'adresse du lien qui devrait s'afficher dans la barre inférieure de votre navigateur Web.

• N'acceptez pas un contrat utilisateur sans en lire d'abord les termes ; sinon, vous risquez d'accepter par inadvertance l'installation d'un logiciel espion ou d'autre composant non souhaité.

• Utilisez des sites de cartes de vœux bien établis, tels que MSN Greetings , Hallmark , American Greetings , Blue Mountain ou Egreetings lorsque vous envoyez des cartes électroniques.

• Utilisez un logiciel qui vous permet de créer et d'envoyer vos propres cartes électroniques, tel que Microsoft

Photo Story 3 , à télécharger gratuitement, ou Microsoft Digital Image Suite . Vous pouvez également créer vos propres cartes électroniques à l'aide des modèles de cartes de vœux de Microsoft Office .