Les arnaques répandues

Voici certaines des arnaques répandues que vous devez connaître :

Des arnaques qui utilisent le nom de Microsoft ou les noms d’autres entreprises bien connues. Ces arnaques comprennent des courriers électroniques ou des sites Internet fictifs qui utilisent le nom de Microsoft. Le courrier électronique peut indiquer que vous avez gagné un concours Microsoft, que Microsoft a besoin de votre identifiant ou mot de passe ou qu’un représentant de Microsoft vous contacte pour vous aider avec votre ordinateur. (Ces arnaques fictives proposant une aide technique sont souvent réalisées par téléphone). Pour plus d’informations, voir Évitez les arnaques qui utilisent le nom Microsoft de manière frauduleuse.

Arnaques à la loterie. Vous pouvez recevoir des courriers électroniques qui vous indiquent que vous avez gagné à la loterie Microsoft ou à des jeux. Ces courriers électroniques peuvent même ressembler à un message envoyé par un employé Microsoft. Il n’y a pas de Loterie Microsoft. Supprimez le message. Pour plus d’informations, voir Qu’est-ce que l’arnaque à la Loterie Microsoft ?

Arnaques aux logiciels de sécurité non autorisés. Les logiciels de sécurité non autorisés, également appelés « scareware », sont des logiciels qui paraissent bénéfiques d’un point de vue sécuritaire, mais qui n’offrent qu’une sécurité limitée ou aucune sécurité, génèrent des alertes trompeuses ou fausses, ou tentent de vous inciter par la ruse à participer à des transactions frauduleuses. Ces arnaques peuvent apparaître dans les courriers électroniques, les publicités en ligne, votre site de réseau social, les résultats des moteurs de recherche ou même dans des fenêtres publicitaires sur votre ordinateur qui peuvent sembler faire partie de votre système d’exploitation, mais n’en font pas partie. Pour plus d’informations, voir Surveiller les alertes virus fictives.

Comment faire part d’une arnaque

Vous pouvez utilisez les outils Microsoft pour faire part d’une arnaque suspectée.
Internet Explorer. Lorsque vous êtes sur le site suspect, cliquez sur le bouton ou le menu sécurité dans Internet Explorer, pointez la souris sur Filtre SmartScreen. et cliquez Signalez un site Web peu sûr et utiliser la page Internet qui est affichée pour indiquer le site Internet.
Hotmail. Si vous recevez un courrier électronique suspect qui vous demande des informations personnelles, cochez la case à côté du message dans votre boîte de réception Hotmail. Cliquez sur « Marquer comme » et ensuite pointez la souris sur Arnaque par hameçonnage.

Microsoft Office Outlook. Envoyez le message suspect en pièce jointe d’un nouveau message email adressé à reportphishing@antiphishing.org. Pour apprendre comment créer une pièce jointe à un message email, voir Joindre un fichier ou un autre article à un message email.
Vous pouvez aussi téléchargez le complément Junk E-mail Reporting Add-In for Microsoft Office Outlook.
Ce qu’il faut faire si vous pensez avoir été victime d’une escroquerie
Si vous pensez que vous avez répondu à une arnaque par hameçonnage avec des informations personnelles ou financières, prenez ces mesures pour minimiser les dommages.
Changez les mots de passe ou les PIN de tous vos comptes en ligne dont vous pensez qu’ils peuvent être affectés.
Placez une alerte de fraude sur vos rapports de crédit.
Vérifiez auprès de votre banque ou de votre conseiller financier si vous n’êtes pas sûr de la marche à suivre pour faire cela.
Contactez la banque ou le commerçant en ligne directement. Ne suivez pas le lien dans le courrier électronique frauduleux.

Si vous savez qu’un compte quelconque a été visité ou ouvert frauduleusement, fermez ce compte.
Verifiez régulièrement vos relevés mensuels bancaires ou de cartes de crédit pour traquer tout débit inexpliqué ou toute demande que vous n’avez pas formulée.
Outils pour vous aider à éviter les arnaques
Microsoft propose plusieurs outils pour vous aider à éviter des arnaques par hameçonnage lorsque vous naviguez sur Internet ou que vous lisez vos courriers électroniques.
Windows Internet Explorer. Dans Internet Explorer 8, le nom de domaine dans la barre d’adresses est surligné en noir et le reste de l’adresse est en gris pour pouvoir identifier facilement la véritable adresse d’un site Internet.

Le Filtre SmartScreen d’Internet Explorer vous envoie des avertissements sur les sites Internet potentiellement dangereux lorsque vous naviguez. Pour plus d’informations, voir Filtre SmartScreen : Foire aux questions.

Windows Live Hotmail. Le programme de messagerie Internet gratuit de Microsoft utilise également la technologie SmartScreen pour analyser les courriers électroniques. SmartScreen aide à identifier et supprimer les menaces d’hameçonnage et d’autres pourriels des courriers électroniques légitimes. Pour plus d’informations, voir SmartScreen aide à éviter les courriers indésirables.
Microsoft Office Outlook. Le Filtre anti-courrier indésirable dans Outlook 2010, Outlook 2007 et d’autres programmes de messagerie électronique de Microsoft évalue chaque message entrant pour voir s’il ne comporte pas de caractéristiques suspectes communes à des arnaques par hameçonnage. Pour plus d’informations, voir Comment Outlook vous aide à vous protéger des virus, courriers indésirables et hameçonnage.