Que faire contre les virus, les chevaux de Troie et les vers?

Les technologies en constante évolution nous aident à faciliter notre quotidien. Le nombre croissant de nouveaux logiciels malveillants, aussi appelés malware, est l'un des inconvénients de l'évolution des technologies. Les logiciels malveillants sont sans cesse optimisés pour échapper aux antivirus. Dès que l'on trouve des logiciels malveillants, de nouveaux font déjà leur apparition.

Que sont les virus, chevaux de Troie et vers?

On entend par virus, chevaux de Troie et vers des programmes informatiques qui poussent l'utilisateur à exécuter des tâches non souhaitées et le cas échéant dangereuses. Ils appartiennent tous à la catégorie des logiciels malveillants. Si un ordinateur est infecté par un logiciel malveillant, il se peut que les données enregistrées localement ne soient plus protégées contre les accès non autorisés.

Les logiciels malveillants se propagent via les e-mails, les liens sur des sites web ou des clés USB. Comme le nombre d'e-mails et de logiciels malveillants a fortement augmenté ces derniers mois dans le monde entier, il est de plus en plus important de bien se protéger.

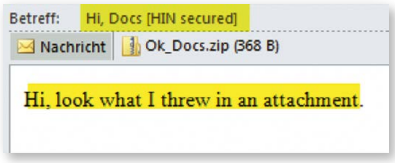
Comment puis-je me protéger contre les logiciels malveillants?

- Faites preuve de vigilance face aux e-mails suspects, même s'ils proviennent d'expéditeurs connus. Malheureusement, il est très facile de falsifier l'adresse des expéditeurs.
- Supprimez immédiatement les messages suspects sans ouvrir les pièces jointes.
- Supprimez également ces messages du dossier Messages supprimés de votre messagerie électronique.
- Notez que les e-mails portant la mention [HIN secured] peuvent aussi contenir des logiciels malveillants.
- Ne cliquez jamais sur les liens contenus dans les e-mails suspects et n'ouvrez aucune pièce jointe.
- N'utilisez jamais votre mot de passe HIN pour des applications tierces.
- Utilisez votre adresse e-mail HIN uniquement à des fins professionnelles et veillez à la transmettre uniquement si c'est nécessaire ou de manière protégée (p. ex. marc.exemple{at}hin.ch).
- Mettez toujours votre système à jour (navigateur, programme de messagerie, antivirus, système d'exploitation, Office etc.). Installez toujours sans attendre les mises à jour, en particulier, lorsqu'il s'agit de mises à jour de sécurité.
- Pour les PC Windows et les Mac, il faut impérativement utiliser des antivirus. Les systèmes Mac sont certes plus rarement concernés par les virus, mais un antivirus augmente la sécurité.
- Réalisez régulièrement des sauvegardes de vos systèmes.

Comment reconnaître des e-mails suspects?

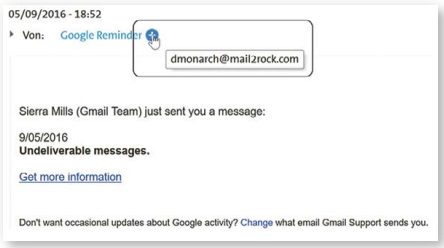
Pièce jointe dangereuse

- Demande directe de cliquer sur la pièce jointe
- Message impersonnel
- En anglais



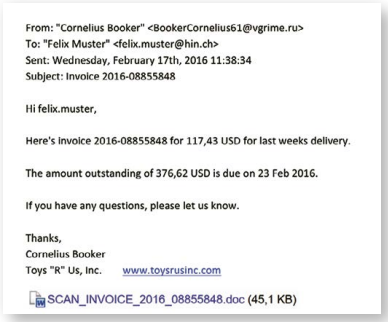
Expéditeur dissimulé

- L'expéditeur de l'e-mail n'a rien à voir avec l'entreprise indiquée.
  Attention: il est simple de falsifier les expéditeurs d'e-mails, c.-à-d. qu'il serait très facile de procéder à une falsification un peu moins évidente que l'exemple montré.



Nom incorrect

- La partie connue de l'adresse e-mail (marc. exemple) est utilisée plusieurs fois, mais n'est pas personnalisée. On peut en déduire que l'expéditeur ne connaît pas ni le destinataire, ni son nom et prénom.
- (La pièce jointe n'est pas affichée dans l'image suivante pour des raisons de place) Liens trompeurs
- Les liens montrent une adresse de destination différente de celle que du lien affiché (attention: déplacer la souris sur le lien, mais ne jamais cliquer dessus).
- La destination du lien s'affiche selon le programme dans le pied de page ou à côté du lien.
- Cette tactique est souvent utilisée dans les e-mails d'hameçonnage en cas de chevaux de Troie bancaires.



Le modèle est toujours le même, il consiste à inciter la personne à ouvrir la pièce jointe ou à cliquer sur un lien (p. ex. facture impayée, chance de gagner, idée commerciale, candidature, tâche oubliée, tâche importante ou urgente etc).

- Les e-mails en français comprennent parfois, mais moins souvent que par le passé, des erreurs de frappe et de langue.
- Les e-mails d'expéditeurs que vous connaissez peuvent aussi comprendre des logiciels malveillants, étant donné qu'ils peuvent se propager de manière inaperçue via le répertoire local des personnes concernées.
- Les logiciels malveillants peuvent se loger discrètement dans les pièces jointes, p. ex sous forme de fichier zip, doc, pdf ou jpg. À l'ouverture du fichier, le logiciel malveillant s'installe sur votre ordinateur.

Que faire après avoir ouvert un e-mail ou fichier malveillant?

- Déconnectez votre ordinateur du réseau local, vous pourrez ainsi peut-être empêcher d'infecter d'autres ordinateurs.
- Vérifiez votre ordinateur avec un antivirus actuel.
- Contactez le service d'assistance HIN. Il pourra clarifier si votre antivirus détecte le logiciel malveillant correspondant.
- Assurez-vous de ne pas ouvrir le message contenant la pièce jointe malveillante sur un autre ordinateur. Informez toutes les personnes travaillant sur des postes de travail. Supprimez également ce message de tous vos comptes de messagerie (y compris dans le dossier Messages supprimés).
- Contactez votre partenaire informatique.

Que fait HIN contre les logiciels malveillants?

HIN s'engage en faveur de la communication et de l'interaction électroniques conformes à la protection des données. Cela signifie que:

- La protection des données chez HIN est garantie – «sûr» signifie «conforme à la protection des données».
- HIN protège contre tout accès de tiers à des e-mails et contre tout accès non autorisé à des applications.
- Les e-mails HIN envoyés à d'autres destinataires HIN sont automatiquement cryptés pour empêcher les tiers de les consulter ou de les modifier.

La protection des données n'est pas un antivirus: le cryptage d'e-mails HIN ne protège pas de la propagation de logiciels malveillants via HIN Mail.

L'équipe HIN travaille en permanence à empêcher la propagation de logiciels malveillants.

- La plateforme HIN est équipée de dispositifs de protection comme les antivirus et les anti-malware.
- L'antivirus HIN contrôle tous les e-mails pour détecter les éventuels logiciels malveillants, peu importe s'ils viennent de l'extérieur ou d'adresses HIN.
- Si un virus est détecté dans un e-mail, HIN ne le transmet pas au destinataire.
- Les virus et les chevaux de Troie, et toutes les cyberattaques en général, présentent un risque très élevé et souvent peu prévisible.

Les logiciels malveillants changent d'une seconde à l'autre, si bien que même les antivirus sont vulnérables et que les logiciels malveillants peuvent se loger sans se faire remarquer dans votre système, par exemple sous forme d'e-mail.

Par conséquent, Health Info Net AG décline toute responsabilité concernant tout dommage éventuel.

Le client est responsable de son système. Il est donc important de suivre les indications mentionnées ici.

Autres informations et questions utiles

- Posez vos questions à notre groupe «Forum sur la sécurité des données» sur HIN Home
- Vous trouverez les questions fréquemment posées dans notre FAQ: www.hin.ch/logicielsmalveillants
- Nous restons à votre entière disposition. Vous pouvez nous joindre en appelant le Call Desk de HIN au numéro 0848 830 740 du lundi au vendredi de 08h00 à 12h00 et de 13h00 à 17h00 ou en envoyant un e-mail à l'adresse support@hin.ch.