

Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

 <p>Denis JACOPINI</p> <p>8 LE JT</p> <p>Denis JACOPINI PAR TÉLÉPHONE</p> <p>EXPERT INFORMATIQUE ASSOCIÉ ENCHÈVE AU TRIBUNAL</p> <p>TV5 MONDÉ PREMIÈRE PAR L'ÉMISSION</p> <p>vous informe</p> <p>20:52</p>	<p>Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?</p>
--	---

En pleine recrudescence, de nombreux sites ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). **Phishing** (hacking) et **ransomware** (ransomware) sont des exemples connus d'actes malveillants portant préjudice aux internautes.

Pour s'en prémunir, des réflexes simples existent. QUELS SONT LES DIFFÉRENTS TYPES D'ATTIQUES ? Attaque par hameçonnage (phishing)

↳ **Hameçonnage**, technique de l'usurpation d'un site légitime.

1. Le cybercriminel se « déguise » en un tiers de confiance (banque, administration, fournisseur d'accès à Internet) et diffuse un mail frauduleux, ou contamine une pièce jointe piégée, à une large liste de contacts. Le mail incite les destinataires à mettre à jour leurs informations personnelles (et souvent bancaires) sur un site internet falsifié vers lequel ils sont redirigés.
2. La liste comprend un nombre et important de contacts et augmente les chances que l'un des destinataires se sente concerné par le message diffusé.
3. De ce clic, il est redirigé vers le site falsifié qui va recueillir l'ensemble des informations qu'il révoque.
4. Ces informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage de identifiants, mots de passe ou données bancaires récupérées.

↳ **Voici le cadre de la Malwareware sur le phishing (OSCE – partenariat ANSSI)**

Pour s'en prémunir :

- N'avez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes, elles pourraient être contaminées. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Ne répondez jamais à une demande d'informations confidentielles par mail.
- Pensez votre accès au-dessus des liens, faites attention aux caractères accentués dans la liste ainsi qu'à la qualité du français ou de la langue pratiquée par votre interlocuteur (ex : orthographe).

↳ **Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.**

Attaque par «ransomiciel» (ransomware)

Les ransomiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

1. Le cybercriminel diffuse un mail qui contient des pièces jointes et / ou des liens piégés. Le corps du message contient un message corrompu, parfois en français, qui demande de payer rapidement une facture payée.
2. De ce clic, le logiciel est téléchargé sur l'ordinateur et commence à chiffrer les données personnelles : les documents bureautiques (doc, xls, pdf, etc.), les photos, la musique, les vidéos, etc.
3. Les fichiers données chiffrées, un message s'affiche pour réclamer le versement d'une rançon, payable en bitcoins ou via une carte prépayée, en échange de la clé de déchiffrement. Attention, rien n'indique que le déchiffreur en question soit efficace !

Pour s'en prémunir :

- N'avez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes et des liens dans les messages dont la provenance est douteuse. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Effectuez des sauvegardes régulières sur des périphériques externes.
- Mettez à jour régulièrement tous vos principaux logiciels en privilégiant leur mise à jour automatique.

↳ **Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.**

↳ **VOUS ÊTES VICTIME D'UN RANSOMWARE OU DE FISHING ?**

↳ **Si vous êtes victime de ces cyberattaques, contactez d'urgence :**

↳ **Malwareware** vous de tous les renseignements suivants :

- **Ransomware** de (ou des) ransomware(s) en français
- **Ransomware** de (ou des) ransomware(s) contactable(s) : adresse de messagerie ou adresse postale, pseudo utilisé, numéro de téléphone, fax, copie des courriels ou courriers échangés.
- **Ransomware** de (ou des) ransomware(s) agissant(s) : adresse de messagerie, référence de votre banque et de votre compte, et copie de votre de compte bancaire ou appareil le identifiant frauduleux.
- **Tous autres renseignements** pouvant aider à l'identification de l'auteur

↳ **Vous pouvez également signaler les faits** dans une autre rubrique de la plateforme de signalement « Paris » ou le numéro dédié : 0112 et 02 17

↳ **Des services spécialisés se chargent ensuite de l'enquête :**

↳ **Police nationale** : l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OC/LCITC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDCL) : 01 47 46 97 33

↳ **Gendarmerie nationale** : le centre de lutte contre les criminalités numériques (CLC) du Service Central de Renseignement Criminel (SCRC) cybergendarmerie.interieur.gouv.fr

↳ **Préfecture de police** : la Préfecture de police de Paris, de la Direction centrale de renseignement intérieur (DCRI) et les Bureaux de la Brigade d'enquête sur les Fraudes aux technologies de l'Information (BEFTI) compétente uniquement pour Paris et petite couronne (75, 92, 93 et 94) : 01 40 70 07 30

↳ **Article original**, de gouvernement.fr



Vous souhaitez en savoir davantage sur les cyberattaques ?
Contactez-nous par téléphone ou par mail.
N'hésitez pas à nous contacter.
Nous sommes à votre disposition pour vous accompagner dans votre démarche.
Nous sommes à votre disposition pour vous accompagner dans votre démarche.



Répondre à cet article

Original de l'article mis en page : Cybercriminalité | Gouvernement.fr