Qu'est ce qu'un « N-Tech »

Le N-Tech est un militaire de la Gendarmerie Nationale formé aux nouvelles technologies au sein de son institution et de l'université technologique de Troyes.

C'est un enquêteur spécialisé en investigations et criminalistique liées aux nouvelles technologies. Il est officier de police judiciaire et titulaire d'un diplôme universitaire ou d'un master 2 en sécurité des systèmes d'information. (SSI)

Il est affecté dans des unités de police judiciaire.

Il dispose de moyens informatiques et de logiciels évolués permettant de traquer les arnaques se développant sur Internet.

Son action est suivi au niveau national par la division de lutte contre la cybercriminalités au sein de l'institut de recherches criminelles de la gendarmerie.

Un réseau de 220 N-Tech tisse sa toile sur la France mais également dans les TOM et les DOM.

Une coopération policière avec l'Europe permet de lutter contre la cybercriminalité même en dehors de nos frontières (Europol—Interpol).

Comment contacter le « cybergendarme »

Adjudant Chef RENAULT Frédéric

Groupement de gendarmerie

Caserne MDL/Chef Bongeot

23000 Guéret

05.55.51.50.00

Vous naviguez sur Internet,

vous effectuez des achats sur le web,

Prévenir les arnaques sur Internet

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'INTERIEUR

Gendarmerie nationale

Sur votre ordinateur

* Installer un logiciel antivirus dès l'installation de votre ordinateur (Avast ou Antivir par exemple),
* Installer un anti-malware contre les logiciel malveillant, (Malware Bytes par exemple,
* Faire régulièrement des recherches avec l' antivirus sur votre disque dur mais également sur les clefs USB,
* Installer un logiciel reconnu (revo Uninstaller par exemple) pour désinstaller vos logiciels inutilisés,
* Ajouter à votre navigateur Internet (Mozilla) des add-ons (petits plus) bloquant les publicités intempestives,
* Ne pas installer un logiciel sans en connaître l'origine, ni les conditions d'utilisation,
* Ne pas installer un logiciel sans passer par un site connu (01net, Comment ça marche, Clubic,…),
* Pendant l'installation d'un logiciel ne pas cliquer « I agreed » sans regarder ce que vous installez,
* Ne pas installer un logiciel issue d'une publicité sur Internet ou d'alerte vous indiquant des failles de sécurité,
* Ne jamais enregistrer ses mots de passe, ses coordonnées bancaires dans un fichier de l'ordinateur,

Sur *Internet*

* Ne pas « surfer » sans antivirus,
* Sécuriser votre « box » dès sa mise en route en changeant le login et le mot de passe qui par défaut sont identiques à tous les utilisateurs,
* Ne pas prendre de risques en surfant sur des sites pirates,
* Ne pas communiquer pas vos identifiants et mots de passe sur le net,
* Ne communiquez jamais vos coordonnées bancaires suite à un courriel sur Internet,
* Créer une adresse passe-partout sur Internet pour la laisser sur des sites où vous n'avez pas confiance,
* Interdiction de télécharger sur des sites « peer to peer », c'est illégal,
* Le téléchargement gratuit sur Internet existe avec les sites « replay » de nombreuses chaines de télévision,
* Ne pas répondre aux courriels dont vous ne connaissez pas l'expéditeur,
* Ne pas ouvrir une carte de vœux si ce n'est pas votre anniversaire ou si vous ne connaissez pas l'expéditeur, risque de virus,
* Ne pas ouvrir la pièce jointe d'un courrier dont l'expéditeur ne vous est pas connu,
* Les sites pédopornographique sont illégaux.
* Télécharger « une » image à caractère pédophile entraine des poursuites judiciaires,
* Désactiver le Wi-Fi de votre « box » si vous ne vous en servez pas.

Sur les sites en ligne

* Faire des achats en ligne uniquement sur des sites connus.
* Ne pas faire d'achats en ligne sur les spots Wi-Fi gratuits dans les bars ou enseignes de restauration rapide,
* Ne payer vos achats qu'en carte bleue, avec un site de paiement comme « paypal » ou avec une @carte.
* Ne pas payer vos achats sur internet en Western Union ou mandat cash, fort risque d'arnaque,
* Au moment du paiement, vérifier que votre URL est passée en HTTPS (mode sécurisé)
* Ne pas communiquez vos coordonnées de carte bancaire par téléphone,
* Un prix trop alléchant sur Internet cache très souvent une arnaque,
* Les propositions de ventes venant d'Afrique sont très souvent des arnaques,
* Les produits venant de la RPC (République Populaire de Chine) sont très souvent des contrefaçons. Vous pouvez vous exposer à des poursuites judiciaires,
* Avant de faire un achat vérifier le prix sur deux ou trois sites différents,
* Vérifier les mentions légales des sites et les conditions générales de ventes, en bas de la page web.