CYBER SECURITY 01

Des courriels suspects ? Prenez du recul et vérifiez !

On vous signale une urgence ? On vous demande d'ouvrir une pièce jointe ou encore de vous connecter ? Si vous avez le moindre doute, appelez l'expéditeur ou contactez K-Force.

Connaissez-vous déjà ces astuces ?

Utilisez-les pour travailler en toute sécurité numériquement !

Protégez-vous en verrouillant votre PC

Empêchez quiconque d'utiliser votre appareil et vos programmes, de se connecter avec vos données ou d'effectuer des opérations. Verrouillez toujours votre appareil lorsque vous vous absentez, même quand vous faites simplement une pause.

Apple: ^ control + ⌘ command + Q

Windows: ⊞ + L

Ne donnez jamais votre mot de passe

Soyez méfiant si l'on vous demande votre mot de passe par e-mail, messagerie, SMS, etc. Les banques, institutions gouvernementales, ou même Microsoft, ... ne demandent jamais de mot de passe !

Il vous arrive de devoir partager des mots de passe, par ex. avec des collègues ou des clients ? Utilisez One Time Secret ou un logiciel de gestion de mot de passe professionnel dans ce cas.

www.onetimesecret.com

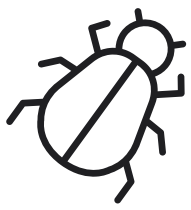
Réseaux WiFi publics ? Non, optez plutôt pour la 4/5G !

Réseau WiFi non sécurisé (sans clé d'accès) ? Prudence, les pirates peuvent peuvent intercepter votre connexion et ainsi voler des données.

www.k-force.be

k-force

connected by ict



Des doutes ? Contactez K Force !

Helpdesk	**helpdesk@k-force.be**
Sales	**sales@k-force.be**
Proximus	**proximus@k-force.be**
Général	**info@k-force.be**
Administration	**administration@k-force.be**
Téléphone	**02 380 23 32**
Lu - ve	8h - 12h & 13h - 17h

LE HAMEÇONNAGE

Première vérification

Les e-mails de phishing vous demanderont toujours quelque chose, parfois pour une raison apparemment tout à fait légitime. Soyez particulièrement vigilent si c'est soi-disant "très urgent". Vérifiez toujours si l'adresse e-mail et le nom de domaine utilisés correspondent bien à ceux de votre contact et si les liens renvoient bien à l'emplacement correct en maintenant votre souris dessus pendant un court instant. Ne cliquez pas sur ces liens!

Hameçonnage ?

Cybercriminalité dans laquelle un attaquant se fait passer pour une source fiable afin d'obtenir des informations sensibles d'une victime.

Typosquattage ? Plutôt rusé !

Le typosquattage consiste à utiliser des noms de domaine mal orthographiés ou des variantes pour faire croire aux utilisateurs que le site qu'ils essaient de visiter est légitime. Si vous avez un doute, surfez vous-même sur le site web en question.

EXAMPLES FOR ANOMALIBANK.COM

- anomalibank.com ✓
- update-anomalibank.com ✗
- anomalibank-alert.x7462e7.com ✗
- wwwanomalibanksecure.com ✗

EXAMPLES FOR DOMAIN.COM:

- domain.com ✓
- domian.com ✗
- domains.com ✗
- doma1n.com ✗
- domain.cm ✗

Imposture et recherche

De plus en plus les attaquants rassemblent un maximum de données personnelles d'une cible spécifique, comme le nom de son employeur (et donc de ses collègues), des achats effectués en ligne récemment, etc... Avec ces données, l'attaquant peut envoyer un message d'apparence authentique semblant provenir d'une source fiable, telle que l'employeur, un collègue ou encore un fournisseur chez qui vous avez récemment commandé. Vous recevez soudain un e-mail étrange d'un collègue ? Attention !

Se connecter ou payer

Soyez toujours particulièrement vigilant lorsque l'on vous demande vos identifiants de connexion. Essayez de vous connecter uniquement si vous êtes certain à 100 % que l'URL du site web est correcte. Même en cas de paiement, la prudence est de mise. Le numéro de compte est-il nouveau, étranger, ou faut-il effectuer le paiement via un portefeuille cryptographique ? Cela est particulièrement suspect !

RECONNAÎTRE

k-force

connected by ict

Des doutes ? Contactez K Force !

Helpdesk	**helpdesk@k-force.be**
Sales	**sales@k-force.be**
Proximus	**proximus@k-force.be**
Général	**info@k-force.be**
Administration	**administration@k-force.be**
Téléphone	**02 380 23 32**
Lu - ve	8h - 12h & 13h - 17h

Vous avez reçu un message suspect ?

suspect@safeonweb.be

Formation et simulations axées sur la sensibilisation à la sécurité

↘ **www.k-force.be/fr/phishing**

SOCIAL ENGINEERING

L'ingénierie sociale ?

L'ingénierie sociale vise à influencer les personnes afin qu'elles divulguent des informations sensibles ou qu'elles posent des actes compromettant les systèmes de sécurité.

Piggybacking

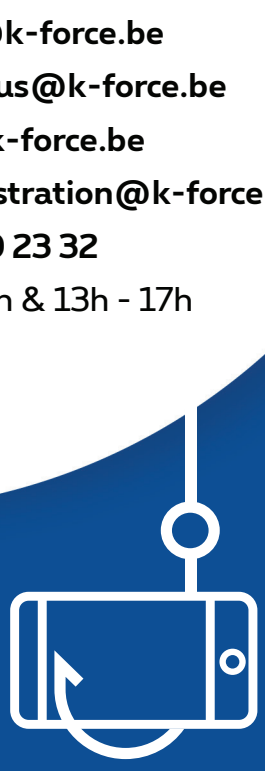
Une personne non autorisée tente d'obtenir physiquement l'accès à des zones sécurisées en accompagnant un employé. Les salles de serveurs sont bien sûr une cible très recherchée. Un bon exemple est cette technique qui consiste à pénétrer dans diverses zones d'une entreprise simplement en portant un gilet jaune.

Pretexting et BEC

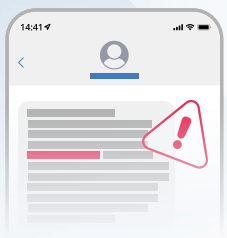
Le pretexting consiste à inventer une histoire crédible pour tromper quelqu'un.
Un exemple classique est celui des prétendus techniciens de Microsoft qui affirment vouloir vous 'aider' avec un problème informatique. Chez BEC (Business Email Compromise) les systèmes de messagerie électronique sont piratés pour envoyer des e-mails contenant de fausses instructions de paiement ou d'autres actions nuisibles, souvent au nom de personnes autorisées (occupant des postes élevés) au sein de l'entreprise.

Whaling ou spear phishing

Ce terme fait référence à une "pêche au gros poisson". Ce sont ainsi les personnes les plus influentes d'une entreprise qui sont spécifiquement ciblées, telles que le PDG, les cadres supérieurs ou encore les employés du département financier. Ces personnes ont généralement accès aux informations les plus critiques de l'entreprise, et elles ont souvent les droits d'accès les plus élevés.



Vishing et smishing



Il arrive aussi fréquemment que l'on tente d'accéder à vos données par téléphone (= vishing) ou par SMS (= smishing). Ne transmettez donc jamais de mot de passe via ces canaux, ne cliquez pas sur des liens suspects et évitez de communiquer des informations sensibles.

En progression: Le quishing

Les victimes sont incitées à scanner des codes QR malveillants. Utilisez des scanners de codes QR sécurisés.

k-force
connected by ict

Des doutes ? Contactez K Force !

Helpdesk	**helpdesk@k-force.be**
Sales	**sales@k-force.be**
Proximus	**proximus@k-force.be**
Général	**info@k-force.be**
Administration	**administration@k-force.be**
Téléphone	**02 380 23 32**
Lu - ve	8h - 12h & 13h - 17h