Pôle technologies et industrie

cifom CPLN

Le comportement en cas d'attaque

ICT-214 – Instruire les utilisateurs dans leur comportement avec des moyens informatiques

214_07_12_Th_Comportement_en_cas_attaque.pptx

JBL 01.04.2022 d'après MAG-MD

Comportement en cas de suspicion d'attaque

Prévention :

- Il faut rendre les utilisateurs conscients des dangers.
- Leur enseigner à adopter un comportement prudent pour éviter ces dangers est une bonne façon de minimiser les risques pour l'entreprise.
- Vous devez avoir déterminé à l'avance avec le responsable de la sécurité la réaction attendue de la part de l'utilisateur et l'en informer.

Que dois faire l'utilisateur quand l'antivirus détecte un problème ?

Voici quelques suggestions…

Lors d'une alerte de l'antivirus

- Ne pas éteindre l'ordinateur.
- Ne pas continuer votre travail.
- Déconnecter le câble réseau de l'ordinateur
- Signaler **immédiatement** le problème au service informatique ; c'est un cas urgent pour identifier le problème et éviter une propagation.
- Indiquer ce que vous étiez en train de faire (pour aider à l'identification de la source de l'infection).
- Le service informatique se déplacera dans la minute et mettra à votre disposition si nécessaire un autre poste de travail pendant la procédure de dépannage.

Comment reconnaître un email frauduleux ?

- Objectifs de ces courriels: récupérer vos données personnelles et bancaires.
- Anomalies dans le logo de la société (souvent connue).
- Polices de caractères utilisées non conforme à l'identité graphique de la société.
- Fautes d'orthographe.
- Souvent le message n'est pas personnalisé (Cher Client…).
- Le corps du message peut contenir une image à la place du texte.

Comment reconnaître un email frauduleux ?

- Le courriel vous invite dans un délai assez court à :

- répondre directement au mail en fournissant des données personnelles,
- cliquer sur un lien afin de compléter un formulaire,
- ouvrir une pièce jointe.

Comment reconnaître un email frauduleux ?

- Dans l'email frauduleux type, les **prétextes souvent mis en avant** sont les suivants :

- Mise à jour de vos données personnelles
- Désactivation imminente de votre compte
- Récompense ou remise (par exemple, réduction d'impôts)

- En général, le mail peut contenir soit :

- Un **lien** qui renvoie vers un site Internet frauduleux ressemblant fortement au site officiel de la société ou de l'organisme en question (adresse URL du site, page d'accueil et logo quasi-identiques).
- Une **pièce jointe** (formulaire à remplir, programme à exécuter).

Comment reconnaître un email frauduleux ?

- Sachez qu'**un site de phishing est rarement sécurisé** alors que la plupart des sites Internet de banques ou de sociétés de e-commerce le sont.
- Pour **reconnaître un site Internet sécurisé**, regardez si :
- Une icône représentant un **cadenas** est situé dans la barre d'état de votre navigateur.
- L'**adresse URL** du site est précédée de :
- « **https://** » au lieu de « http:// ».
- Si ces conditions sont réunies, vous êtes sur un site Internet sécurisé.

Pôle technologies et industrie

cifom

Quelles sont les précautions à prendre après avoir reçu un mail suspect ?

- Ne répondez pas au mail.
- Signalez le mail frauduleux et l'infraction dont vous avez été victime aux autorités compétentes ou aux organismes concernés.
- Transférez-le aux autorités compétentes.
- Ne cliquez sur aucun lien contenu dans le mail. N'ouvrez pas les pièces jointes.
- Détruisez le mail.
- Mettez à jour le système de protection de votre ordinateur (antivirus, pare-feu, logiciel anti-espion).

Pôle technologies et industrie

cifom

Quelles sont les précautions à prendre après avoir reçu un mail suspect ?

- **Si vous avez un doute :**
- Téléphonez directement à l'organisme ou à la société en question avant de répondre au mail.
- Mais n’utilisez pas le numéro de téléphone indiqué dans l’email suspect !

Si vous avez déjà répondu à un mail frauduleux

- Prévenez l'organisme dont l'identité a été usurpée et modifiez les mots de passe transmis par inadvertance.
- Consultez vos relevés de compte bancaire et assurez-vous qu'aucun montant n'a été prélevé de façon irrégulière.
- Dans le cas contraire, contactez immédiatement votre banque afin de faire opposition.