

FAUX E-MAILS ET SMS : NE VOUS LAISSEZ PLUS PIÉGER !



Les premiers indices :

- L'urgence (un délai court pour une action et un lien à cliquer)
- La peur : la perte de données, d'un compte, ...
- Les fautes d'orthographe, un sentiment d'étrangeté (aspect du site, ...)
- Un message non nominatif



Informations recueillies sur les sites www.safeonweb.be et www.cybersimple.be



Ça, c'est la Province !    
WWW.PROVINCE.LUXEMBOURG.BE

QUELQUES CONSEILS EN PLUS :

- Evitez les offres qui semblent trop belles pour être vraies
- Evitez d'ouvrir les messages qui éveillent votre curiosité (ex : regardez ce que j'ai lu sur vous !)
- N'envoyez des informations à un site Web que s'il utilise l'https:// (regardez l'adresse internet du site)
- Installez un logiciel antivirus et un anti-pub pour vous protéger
- Allez toujours directement sur le site Web de votre banque (ne pas cliquer sur un lien dans un mail ou un sms)



Informations recueillies sur les sites www.safeonweb.be et www.cybersimple.be




Ça, c'est la Province !    
WWW.PROVINCE.LUXEMBOURG.BE

VÉRIFIEZ LES CINQ SIGNES D'AUTHENTICITÉ D'UN E-MAIL


De : KBC Banque [kbc@infokbc.pw] **A**
Objet : Votre carte bancaire sera bloquée à partir du 8 février **E**

Cher client, **B**

 **C**

Permettez-nous de vous présenter notre nouvelle carte de banque.
Cette nouvelle carte est mieux protégée contre les pratiques frauduleuses et satisfait parfaitement aux prescriptions européennes en matière de sécurité bancaire. Nous offrons à nos clients un environnement virtuel aussi sécurisé que possible pour leur permettre de procéder à leurs opérations bancaires avec une facilité optimale. L'ancienne carte de banque n'offrait pas toujours la flexibilité et la convivialité que nous visons pour nos clients.
En revanche, notre nouvelle carte de banque recourt aux technologies les plus sophistiquées et vous offrira maintenant et à terme nettement plus de possibilités. **D**

Procédure d'obtention de votre nouvelle carte de banque
Vous pouvez en faire la demande de cette nouvelle carte de banque ci-dessous. La demande est gratuite jusqu'au 8 février 2016. Merci de vérifier vos données via le formulaire ci-dessous. Ensuite, vous pourrez procéder à la demande. Pour clôturer la demande, il faudra recycler votre ancienne carte avec notre programme de recyclage. Vous recevrez ensuite votre nouvelle carte de banque dans les deux jours ouvrables.

 **F**

Attention ! Après le 8 février, votre ancienne carte sera inutilisable. Les frais d'une nouvelle demande obligatoire vous seront alors facturés.

Avec nos meilleures salutations,
KBC Banque

Ce message ne vous est pas destiné ? Toutes nos excuses. Nous mettons tout en œuvre pour que nos données restent actualisées. Faites-le savoir à KBC-Telecenter au 078 153 152. **G**

- A** La partie d'adresse qui suit «@» doit se terminer par le domaine du site Web officiel.
Dans le cas présent : kbc.be
- B** La personnalisation d'un mail est un des indices d'un mail officiel
- C** Le logo de l'institution ne suffit pas pour valider un mail



Informations recueillies sur les sites www.safeonweb.be et www.cybersimple.be



Ça, c'est la Province !    
WWW.PROVINCE.LUXEMBOURG.BE

- D** La crédibilité de l'histoire.
Si c'est bizarre, c'est bizarre ! Pas d'héritage qui vient d'Afrique, aucun paiement direct à la police ou la poste. Réfléchissez et vérifiez !
- E** L'objet du message vous semble-t-il vraisemblable que l'expéditeur vous envoie un message à ce sujet ?
- F** Vers quelle adresse internet (URL) les liens renvoient-ils ? (le site officiel de l'expéditeur ou non ?). Faites passer le curseur au-dessus des liens ou placez le doigt sur eux pour visualiser l'URL.
- G** Les détails pour rendre leurs messages plus réalistes, les escrocs y ajoutent souvent des numéros de téléphone, des adresses e-mails et des numéros de compte. Comparez-les avec ceux que vous trouvez sur le site Web officiel.



Informations recueillies sur les sites www.safeonweb.be et www.cybersimple.be

ET SI VOUS AVEZ MORDU

À L'HAMEÇON, MALGRÉ TOUT ?

- **Avez-vous saisi votre identifiant ou votre mot de passe sur le site falsifié ?** Dans ce cas, changez immédiatement tous vos mots de passe.
- **Avez-vous fourni des données financières ?** Alertez votre banque et demandez à Card Stop (070 344 344) de bloquer immédiatement votre paiement. N'oubliez pas de porter plainte à la police.
- **Si vous avez cliqué sur un lien ou ouvert un fichier suspect,** interrompez immédiatement la connexion Internet. Procédez à un scan antivirus.
- **Si vous n'êtes pas certain d'avoir éliminé le problème,** contactez un expert informatique.
- **Prévenez vos amis** que vous leur avez envoyé un faux message.



Informations recueillies sur les sites www.safeonweb.be et www.cybersimple.be



Ça, c'est la Province !    
WWW.PROVINCE.LUXEMBOURG.BE

ET EN CAS DE DOUTE ?

- **Si ça provient d'un ami** : appelez-le, envoyez un SMS ou un message via les réseaux sociaux. Si le message ne provient pas de votre ami, prévenez-le que son compte a été piraté.
- **S'il s'agit d'une organisation ou d'une entreprise** , allez sur leur site et contrôlez si l'action « urgente » dont il est question existe réellement. Si vous ne trouvez rien, vous pouvez toujours leur téléphoner.



Informations recueillies sur les sites www.safeonweb.be et www.cybersimple.be



Ça, c'est la Province !    
WWW.PROVINCE.LUXEMBOURG.BE

POUR VÉRIFIER QUE
VOS COMPTES N'ONT
PAS ÉTÉ

PIRATÉS :
haveibeenpwned.com

- ...est un site qui permet de vérifier si votre compte a été compromis. Le site vous indique si votre compte se trouve dans l'une des bases de données piratées recensées par le site.
- Que faire si votre compte est piraté ?
La chose la plus importante est de rapidement modifier le mot de passe du compte (avec un mot de passe fort).



Informations recueillies sur les sites www.safeonweb.be et www.cybersimple.be



Ça, c'est la Province!    
WWW.PROVINCE.LUXEMBOURG.BE

UN MOT DE PASSE **FORT** PERMET D'ÉVITER LA GRANDE MAJORITÉ **DES ATTAQUES**

Voici une méthode qui permet de construire un mot de passe très fort, différent pour chaque compte MAIS facile à retenir. D'après les dernières études, c'est la longueur qui est décisive.

- Prendre une petite phrase avec une majuscule ou deux et un mot familier, peu utilisé ou volontairement mal orthographié.
- Insérer des caractères spéciaux dans les espaces vides.
- Ajouter avant, après, ou les deux, quelques lettres du site sur lequel vous êtes.

Phrase de base

J'aime les cahuettes

Caractères spéciaux
(La seule chose à retenir)

«J'aime@les€cahuettes»

1 mot de passe
par compte
(exemples pour
Facebook et Youtube)

**face»J'aime@les€cahuettes»
«J'aime@les€cawettes»yout**

**Pour plus de sécurité encore,
passez à la double identification !!**

