INCLUSION DIGITALE

febelfin

Febelfin informe et sensibilise

Le document que voici présente le matériel que Febelfin, l'organisation faîtière du secteur financier, met à disposition dans un souci d'inclusion numérique et de sécurité en ligne. Il s'agit d'un aperçu pratique de tout ce qu'il faut savoir pour être en mesure d'effectuer ses paiements numériques et de gérer ses finances en ligne aisément et en toute sécurité. L'amélioration des compétences numériques pour toutes et tous aidera notre société. Nous souhaitons contribuer à cette avancée.
Vous pouvez utiliser ce matériel pour aider les autres à progresser dans l'univers du numérique ou pour faire évoluer vos propres connaissances et compétences.

Une grande partie de notre vie se déroule en ligne et nous réalisons bon nombre de nos opérations de manière numérique. Faire ses courses, lire le journal, postuler un emploi ou demander une nouvelle carte d'identité : tout cela peut se faire en quelques clics. Les paiements et les services bancaires font également partie de cette liste. Acheter en ligne, vérifier son solde et effectuer des virements via son PC ou son smartphone, mais aussi payer avec sa carte dans un magasin... De plus en plus de personnes en passent par-là. Et pour une raison simple : c'est rapide et facile.

Beaucoup d'entre nous trouvent aisément leur chemin dans ce nouvel univers numérique, mais ce n'est malheureusement pas le cas de tout le monde. Ainsi nous est-il régulièrement donné d'entendre la question suivante : tout cela est-il sûr ? Et aussi : Comment éviter de tomber dans le piège des fraudeurs ?
Au travers de ce document, nous souhaitons offrir une aide et des conseils afin de répondre à ces questions. **Il s'agit d'un aperçu pratique de tout ce qu'il faut savoir pour être en mesure d'effectuer ses paiements numériques et de gérer ses finances en ligne aisément et en toute sécurité**. Toute une série de sujets sont abordés : du phishing, et des mules financières à de nombreuses autres formes de fraude, en passant par les tendances et les principes des paiements et des services bancaires numériques.

Le document que voici présente le matériel que Febelfin, l'organisation faîtière du secteur financier, met à disposition dans un souci d'**inclusion numérique** et de **sécurité en ligne**. Vous pouvez utiliser ce **matériel** pour **aider les autres à progresser** ou pour **mieux vous prémunir contre les risques éventuels**.

L'amélioration des compétences numériques pour toutes et tous aidera notre société. Nous souhaitons contribuer à cette avancée qui s'inscrit pleinement dans le cadre de notre engagement social : créer un environnement numérique sûr et faire en sorte que chacun y trouve sa place.

Avez-vous encore des questions ou des suggestions après avoir lu ce document ? N'hésitez pas à nous le faire savoir.

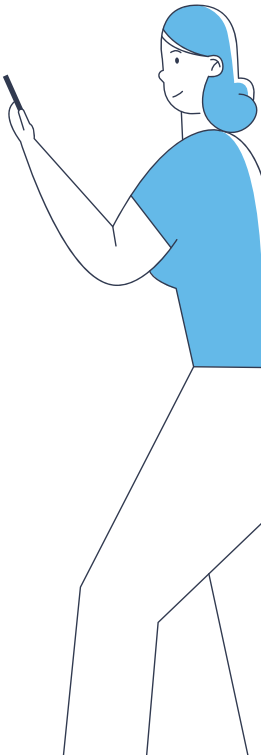


TABLE DES MATIERES

1 Banque numérique

2 Sécurité des opérations bancaires numériques : phishing, mules et autres formes de fraude

3 Paiement numérique

1. Services bancaires numériques

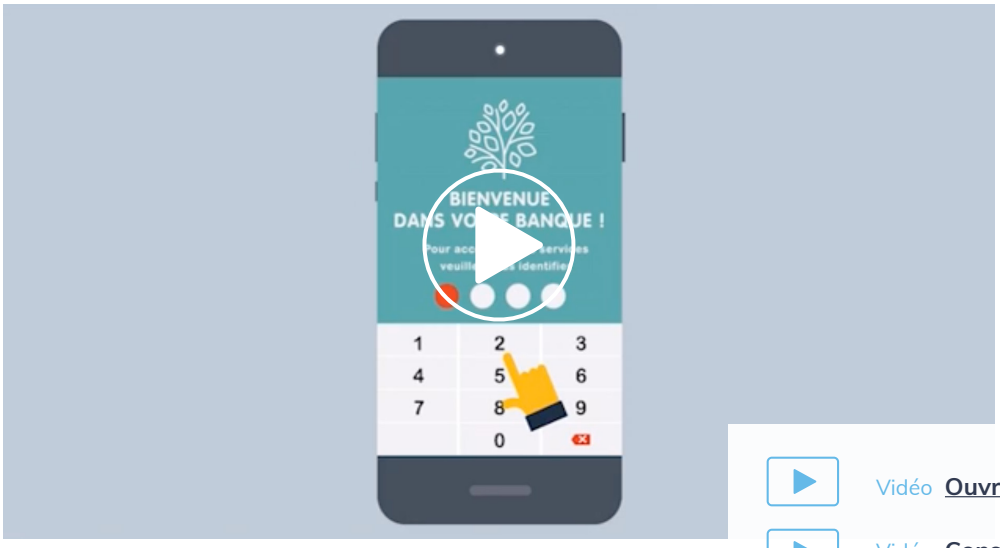
La banque numérique, ce sont les opérations bancaires que vous effectuez via votre ordinateur, votre tablette ou votre smartphone. Mais comment se lancer et est-ce sans risque ? Comment installer l'application de votre banque ? Comment effectuer un virement ? Febelfin vous aide à vous y retrouver. Que vous soyez un ou une consommateur-trice ou un ou une accompagnant-e, vous pouvez commencer dès maintenant avec le matériel ci-dessous.

Vous souhaitez une séance d'information sur la sécurité des services bancaires numériques dans votre ville ou commune ? C'est possible ! Vous trouverez ci-dessous de plus amples informations sur les sessions d'information gratuites organisées par Febelfin.

Pour le ou la consommateur-trice

Ces informations offrent aux consommateurs-trices un guide pratique de la banque en ligne. Les articles sont accompagnés de petites vidéos simples à comprendre qui expliquent un peu plus en détail les principes de base.

Article **Comment se mettre à la banque digitale ?**



Vidéo **Ouvrir l'application bancaire**

Vidéo **Consulter vos comptes**

Vidéo **Faire un virement**

Article **Comment télécharger l'application de votre banque**

Article **Comment joindre votre banque**

Article **La banque digitale est-elle sûre ?**

Pour l'accompagnant-e

En 2020, Febelfin a lancé le module **« Réaliser des opérations bancaires avec un smartphone »** sur la plate-forme « 123 Digit ». Ce module est destiné aux accompagnant-e-s de personnes qui ne connaissent pas ou guère la banque numérique.
Le module cible principalement les accompagnant-e-s qui proposent des séances de formation ou d'information sur les services bancaires mobiles, mais toute personne souhaitant aider un tiers dans ce domaine peut l'utiliser.
Grâce à des exercices interactifs, l'apprenant-e se familiarise avec les services bancaires mobiles et se retrouve, au terme du module, capable de gérer en toute autonomie ses affaires bancaires par ce biais. Le module peut être utilisé par tout le monde et est entièrement gratuit.

Module **Réaliser des opérations bancaires avec un smartphone**

Séances d'information sur la banque, les paiements et la sécurité numériques

Febelfin propose aux groupes des séances d'information gratuites sur les services bancaires et les paiements numériques, éventuellement complétées par un commentaire des différentes formes de fraude, comme le phishing ou la fraude à l'amitié. Si vous souhaitez organiser une telle séance d'information dans votre ville ou commune, prenez contact avec **info@febelfin.be**

2. La sécurité de la banque numérique

Phishing, mules financières et autres formes de fraude

Phishing

Site web de Febelfin

Le site web **www.febelfin.be/fr** fournit des informations sur les dernières techniques de fraude, les mesures prises par les banques pour repérer à temps les transactions suspectes et mettre les criminels hors-jeu. Vous y trouverez toutes sortes d'articles, d'astuces et de conseils **sur le thème Securité et fraude**.

Campagne : « Déjouez le phishing »

Le 16 novembre 2021, le Centre pour la Cybersécurité Belgique (CCB), Febelfin et la Cyber Security Coalition ont lancé une campagne de sensibilisation percutante sur les dangers du phishing : Soyez malin. Déjouez le phishing. Cette forme de fraude en ligne est en pleine croissance et continue de faire de nombreuses victimes, tant parmi les particuliers que parmi les entreprises et les organisations. Il est donc toujours très important de sensibiliser le public à ce problème. Cette campagne sera menée jusqu'en avril 2022.

MATÉRIEL DE CAMPAGNE :

Le matériel de campagne est gratuit et disponible en français, néerlandais, anglais et allemand.

Site web de la campagne donnant des informations sur le phishing et des conseils pour éviter de tomber dans le piège et sur quoi faire si l'on a malgré tout été victime de phishing.

Matériel de campagne
Vous pouvez retrouver des posters, bannières, dépliants, signatures d'e-mail, vidéo...

Application Safeonweb : Cette application vous prévient des cybermenaces et des escroqueries en ligne. L'application Safeonweb envoie deux types d'alertes. Les "menaces" seront signalées si une contamination a été notifiée à Safeonweb concernant le réseau domestique que vous avez enregistré sur l'application. Vous recevrez aussi des « News » vous mettant en garde contre des cybermenaces en général dans notre pays.

Brochure “There is plenty of phish in the sea”

Vous voulez un aperçu complet de tout ce que nous savons sur le phishing ? Alors ce dépliant est pour vous. Il s’agit d’un long document contenant de nombreuses informations générales, des chiffres et un aperçu des formations qui existent pour différents groupes cibles.

Brochure Phishing

Webinaire Cybersécurité

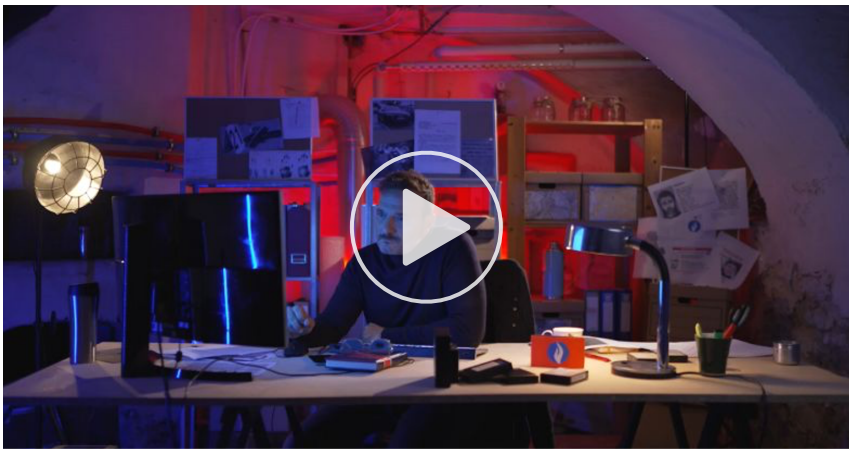
Comment reconnaître un message frauduleux ? Qu’est-ce qu’une mule financière ? Comment traitez-vous les personnes qui ont été abusées et ont perdu de l’argent ? Comment pouvez-vous les avertir ou les aider ? Les réponses à ces questions et à bien d’autres ont été données au cours d’un webinaire organisé par **Febelfin** en collaboration avec l’Observatoire du Crédit et de l’Endettement. Vous pouvez revoir le webinaire :

Webinaire

Un webinaire de votre organisation, en collaboration avec Febelfin ? Nous serons heureux-ses de participer ! Contactez-nous via **info@febelfin.be**.

Vidéos d’explication

Patrick Ridremont reprend le rôle de l’inspecteur Sam Leroy de la série policière Unité 42 et répond aux questions des téléspectateurs. En cinq vidéos, il donne des explications et des conseils sur les sujets suivants : le phishing, le smishing, la fraude à la carte bancaire, les mules financières et la fraude sur les sites de vente.

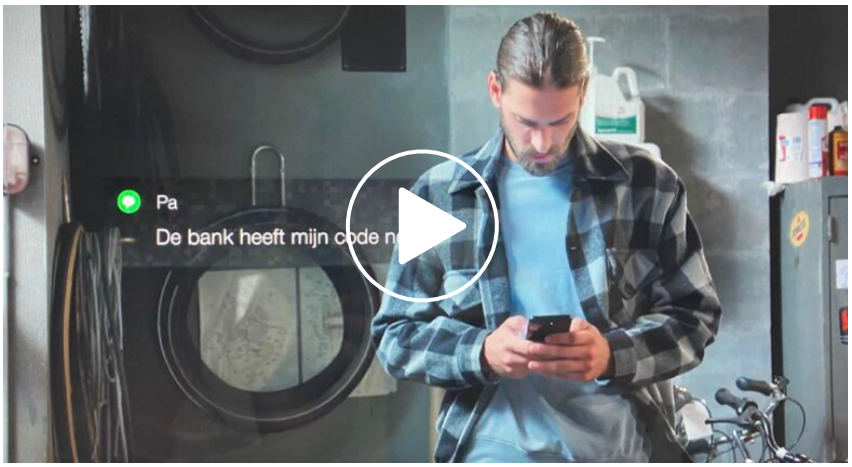


Vidéo d’explication avec l’inspecteur Sam Leroy de la série Unité 42

- Phishing
- Smishing
- Phishing à la carte bancaire
- Mules financières
- Fraude sur les sites de vente

Pour ce qui est du côté néerlandophone, Febelfin a participé à la rédaction du scénario de la série télévisée « Familie » afin de mettre en lumière ce problème. Le personnage de Jan Van den Bossche reçoit un appel suspect d'un prétendu employé de sa banque. Son compte va-t-il être pillé ? Et comment peut-il mieux se prémunir ? Vous le découvrirez dans les épisodes gratuits via VTM GO.

- Familie S31 Episode 83



Episode Familie sur le phishing

Mules financières

Les mules prêtent leur compte bancaire et/ou leur carte bancaire et leur code PIN à des criminels en échange d'une certaine rémunération et participent ainsi - peut-être sans en être conscient - au blanchiment d'argent. Et c'est punissable.
Pas moins de 14% des jeunes seraient disposé-e-s à prêter leur carte bancaire en échange d'argent. Cette situation préoccupante doit changer. Afin de faire connaître le phénomène et de sensibiliser le public, Febelfin a réalisé des affiches et deux brochures d'information, l'une pour les accompagnant-e-s et l'autre pour les jeunes. Ces brochures contiennent toutes les informations nécessaires, expliquées de manière claire, et peuvent être utilisées lors de leçons, d'activités, d'ateliers, de moments d'information ou de discussion. Des vidéos d'influenceurs sont par ailleurs aussi disponibles.

Brochures

Ces brochures sont faciles à imprimer.
Elles existent en français, néerlandais et anglais.

Brochure pour les accompagnant-e-s

Brochure pour les jeunes

Affiches

L'affiche est gratuite et facile à imprimer en format A3.
Elle existe en français, néerlandais et anglais.

Affiche

Matériel pédagogique

Par ailleurs, Febelfin a collaboré avec ED TV, une plate-forme pour les jeunes et les enseignant-e-s qui utilise des vidéos pour aborder plus facilement les sujets difficiles. ED TV a mis en ligne des épisodes accompagnés de fiches scolaires qui commentent le phénomène de la mule financière et permettent d'engager la discussion. Ce matériel est conforme aux objectifs finaux de l'enseignement et répond à la nécessité d'aborder l'éducation financière en classe. Ce matériel et cette offre ne sont disponibles qu'en néerlandais.

Episodes C(r)ash

Fiche scolaire 1 – Introduction générale

Teaserfiche

Afin de diffuser le matériel didactique sur les mules financières et le phishing du côté francophone (brochures...), Febelfin a également collaboré avec la plate-forme de contenu **Enseignons.be**, la principale plate-forme belge de matériel pédagogique et de cours en ligne.

Vidéo

Vidéo en néerlandais sous-titrée en français avec le duo d'influenceurs Kurkdroog :

Articles

Dossier contenant différents articles donnant des informations sur le phénomène des « mules financières » : **Jouer à la mule ? Pas si innocent que vous le croyez.**

Autres formes de fraude

Il est devenu impossible d'imaginer la vie sans internet. Vous y lisez les dernières nouvelles, consultez votre boîte mail, découvrez les frasques de vos ami-e-s... Mais en ligne, on fait malheureusement aussi des rencontres bien moins agréables. Parfois, vous tombez sur des fraudeurs qui abusent de votre confiance et pillent votre compte bancaire. Dans cette section, vous pouvez lire tout ce qui concerne les techniques de fraude les plus courantes.

Phishing à la carte bancaire

Dans le cas du phishing à la carte bancaire, les fraudeurs tentent d'entrer directement en possession de votre carte bancaire et des codes allant de pair. Afin d'arriver à leurs fins, ils vous font croire que votre carte de débit doit être remplacée. Par e-mail, téléphone ou SMS, ils vous demandent de retourner votre carte bancaire par la poste à une adresse donnée. Dans le même temps, ils vous fournissent un lien qui vous amène sur un site web non sécurisé. Ces fraudeurs vous invitent alors à saisir vos codes personnels sur ce site; par ce biais, ils s'efforcent de mettre la main sur l'ensemble de vos données bancaires et codes personnels.

Article **Phishing à la carte bancaire**

Fraude au compte à sécurité renforcée

Les cybercriminels vous contactent par téléphone en se faisant passer pour un membre du personnel de votre banque. Ils vous signalent des mouvements suspects sur votre compte bancaire. Puis, ils vous conseillent de transférer votre argent vers un nouveau compte réputé hautement sécurisé.

Article **Comment fonctionne la fraude au compte à sécurité renforcée ?**

Vidéo **Comment fonctionne la fraude au compte à sécurité renforcée ?**

Fraude à la demande d'aide

Un cybercriminel se fait passer pour l'un ou l'une de vos proches en vous contactant par e-mail, sms ou par des messages dans des applications. Ou inversement : il écrit à vos proches en votre nom. Dans les deux cas, il demande un soutien financier urgent et vous demande de l'aider.
Il fournit ensuite un numéro de compte frauduleux et vous vous retrouvez à transférer votre argent sur le compte d'un fraudeur.

Article **Qu'est-ce que la fraude à la demande d'aide ?**

Vidéo **Qu'est-ce que la fraude à la demande d'aide ?**

Fraude à l'amitié

Dans le cadre de la fraude à l'amitié, les cybercriminels tentent d'entrer en contact avec leurs futures victimes via un faux profil sur internet. Ils vous font croire qu'ils veulent être votre ami-e et établissent une relation de confiance avec vous. Mais il ne faut pas attendre longtemps avant qu'ils ne vous demandent de les aider financièrement.

Article **Comment fonctionne la fraude à l'amitié ?**

L'arnaque au faux support technique

Dans le cadre de ce type de fraude, les cybercriminels se font passer pour du personnel du support technique d'une société informatique et vous contactent par téléphone. Ils vous informent qu'il y a un problème avec votre ordinateur, et vous demandent de brancher celui-ci et de suivre leurs instructions. En réalité, ils vous piratent, prennent le contrôle de votre ordinateur, et vident vos comptes.

Article **Comment fonctionne l'arnaque au faux support technique ?**

La fraude au moteur de recherche

Si vous utilisez un moteur de recherche (Google, Bing, Ecosia, etc.) pour trouver le numéro de téléphone d'un service clientèle, par exemple, il y a des chances que vous tombiez sur un faux site web. Si vous appelez le numéro que vous avez trouvé, vous aurez au bout du fil un cybercriminel qui se fera passer pour un employé fiable.

Article **Comment fonctionne la fraude au moteur de recherche ?**

La fraude au CEO

Dans le cadre de la fraude au CEO, le fraudeur se fait passer pour le CEO (ou une autre personne de confiance interne ou externe) d'une société et donne pour instruction à un ou une collaborateur-trice de cette société d'effectuer des paiements de montants importants. L'ordre est explicitement présenté comme hautement confidentiel afin que le collaborateur ne vérifie pas auprès de ses supérieurs.

Article **Comment éviter la fraude au CEO.**

Vidéo **Comment éviter la fraude au CEO ?**

Logiciels malveillants

Le malware est un terme générique pour désigner toute une série de logiciels malveillants et nuisibles. Ces logiciels s'installent sans que vous les ayez demandés et à votre insu sur votre ordinateur.

Article **Comment fonctionne un logiciel malveillant ?**

Fraude à la facture

Dans le cadre de la fraude à la facture, les fraudeurs interceptent une vraie facture, en modifient le numéro de compte et envoient la facture falsifiée. Tant les particuliers que les entreprises peuvent en être victimes.

Article **Comment se protéger ou protéger son entreprise contre la fraude à la facture ?**

Vidéo **Comment éviter la fraude à la facture?**

La fraude de type Boilerroom

Il s'agit d'une forme d'escroquerie dans le cadre de laquelle les fraudeurs vous proposent d'acheter des actions ou d'autres produits financiers fictifs ou sans valeur.

Article **La fraude de type "boiler room"**

La fraude à la Recoveryroom

Cette pratique consiste pour les fraudeurs à contacter des investisseurs qui ont été dupés précédemment (par exemple via **La fraude de type "boilerroom"**) et à leur proposer de les aider à récupérer leur argent.

Article **La Fraude à la Recoveryroom, c'est quoi ?**

Card- et cash trapping

Les fraudeurs bloquent votre carte de paiement dans le distributeur automatique de billets. Puis, quand vous partez chercher de l'aide, ils dérobent votre carte dans l'appareil. Entre-temps, ils vous ont épié-e et connaissent votre code secret.

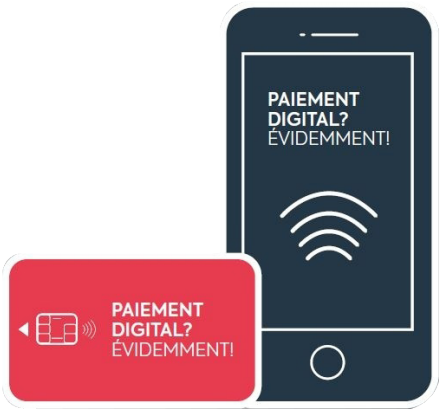
Article **Attention au card et - cash trapping !**

Shoulder surfing

Dans le cas du « shoulder surfing », un fraudeur regarde par-dessus votre épaule pendant que vous effectuez une transaction à un guichet automatique ou à une caisse. Puis ils essaient de s'emparer de votre carte bancaire. Lorsqu'ils ont volé vos données personnelles, vos codes et votre carte, ils vident votre compte.

Article **Qu'est-ce que le shouldersurfing ?**

3. Paiements numériques



Nous payons de plus en plus souvent par voie numérique. Des commissions au magasin ? Nous payons par carte, sans contact ou avec notre smartphone. Pour certaines personnes, tout cela est déjà très évident, mais pour d'autres, ça l'est beaucoup moins. Nous en sommes bien conscient-e-s. C'est pourquoi le secteur financier souhaite aider chacun-e à développer les compétences nécessaires aux paiements numériques. Les vidéos ci-dessous expliquent clairement comment payer par voie numérique.

Payer par carte

Vidéo **Paiements par carte**

Paiements sans contact

Article **Payer sans contact avec la carte**

Vidéo **Comment payer sans contact**

Payer par code QR

Article [Le paiement digital avec le smartphone]

Vidéo [Payer par code qr]

Virements, domiciliations, paiements instantanés

Payer par **domiciliation** :

Article [Payer par domiciliation]

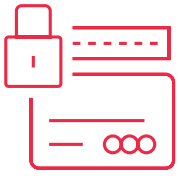
Payer par **virement** :

Article [Payer par virement]

Paiements instantanés : virements en quelques secondes :

Article [Comment virer de l'argent en quelques secondes ?]

Vidéo [Les paiements instantanés]



Sécurité des paiements numériques

A quel point les paiements numériques sont-ils sûrs :

Article **Les paiements sans contact sont-ils sûrs?**

Article **Les paiements digitaux : sont-ils sécurisés ?**

Notre série d'initiatives pour une plus grande inclusion numérique est toujours en mouvement. Au sein de Febelfin, une équipe travaille en permanence sur des projets visant à améliorer les compétences numériques de chacun-e. Il existe des collaborations dans le cadre de divers projets de subvention, mais aussi avec des organisations individuelles engagées dans l'inclusion numérique. Parce que nous croyons fermement en une approche large et structurelle visant à inclure tout le monde dans notre société numérique. Vos idées et suggestions sont dès lors toujours les bienvenues. Vous pouvez aussi toujours nous contacter pour obtenir de plus amples informations sur nos projets.

Contactez-nous : info@febelfin.be

Editeur responsable : Belgian Financial Sector Federation asbl

Boulevard du Roi Albert II 19, 1210 Brussels

www.febelfin.be