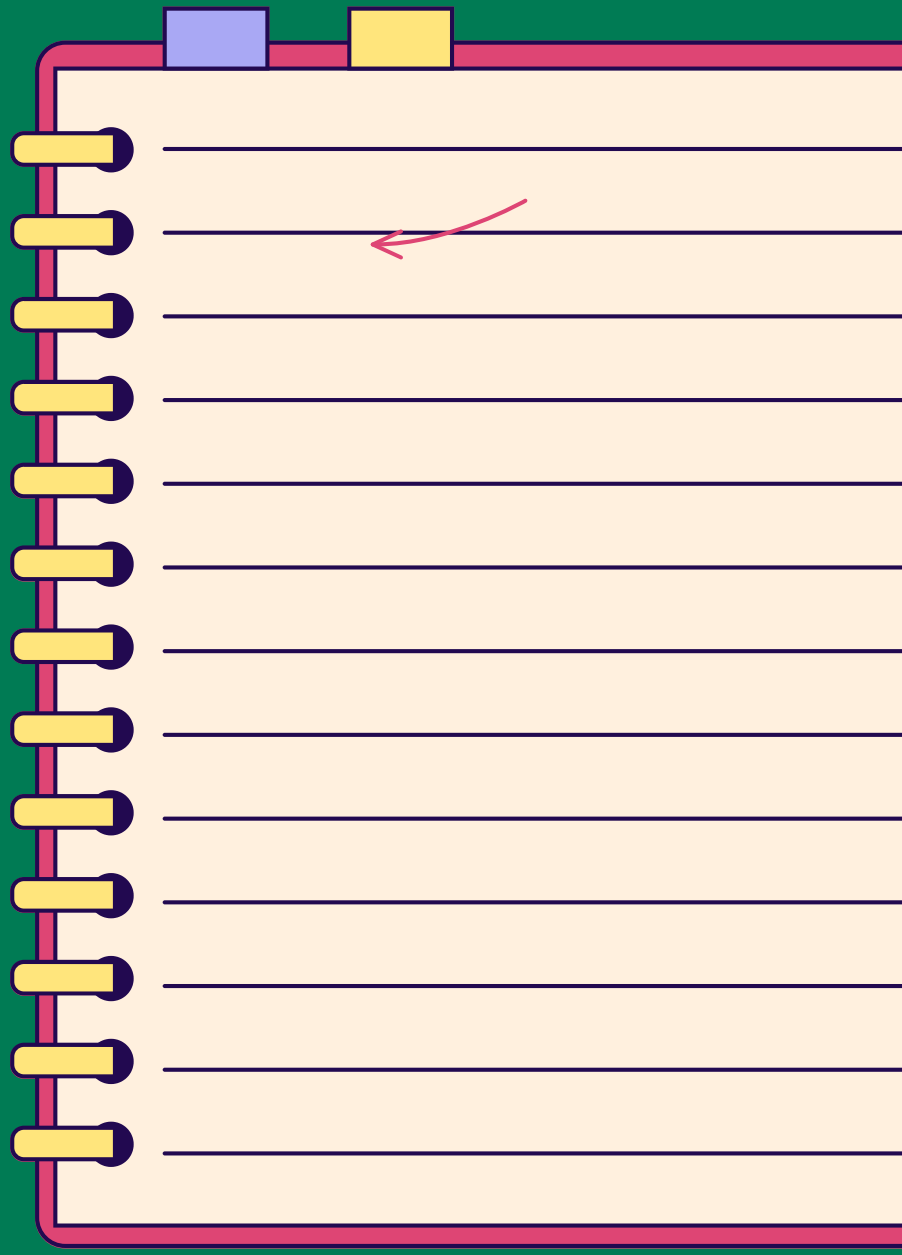
MODULE 12 - ARNAQUES EN LIGNE

CHAPITRE 1

QUELLES SONT LES DIFFÉRENTES ARNAQUES ET COMMENT LES REPÉRER ?



Skills to Connect

INTRODUCTION

À l’ère du numérique, les arnaques en ligne se diversifient et deviennent de plus en plus sophistiquées. Qu’il s’agisse de phishing, de spoofing ou encore de fraudes aux achats, il est essentiel de connaître leurs mécanismes pour mieux les identifier et s’en protéger.

Dans ce chapitre, vous découvrirez les arnaques les plus courantes, comment les repérer grâce à des signes distinctifs, et vous apprendrez à adopter les bonnes pratiques pour naviguer en toute sécurité. À la fin de ce module, vous serez capable de détecter les pièges en ligne et d’appliquer les bons réflexes pour vous en prémunir.

1 LES DIFFÉRENTS TYPES D'ARNAQUE

LE PHISHING OU HAMECONNAGE

QU'EST-CE QUE LE PHISHING ?

Une technique où un individu malveillant envoie des messages frauduleux par email ou par SMS, **souvent composé d'un lien**, pour inciter les destinataires à divulguer leurs informations personnelles, **telles que des mots de passe, des numéros de carte de crédit ou des informations bancaires.**

Regarde la vidéo

qui explique le phishing et comment ne pas se faire avoir !

LES CARACTÉRISTIQUES DU PHISHING

- Message d'urgence, qui joue sur les émotions :
  - "Votre compte Google a été hacké"
  - "Un transfert d'argent frauduleux a été effectué"
- Langage inhabituel
  - Fautes d'orthographes, syntaxe, ...
  - Différentes langues (mélange d'anglais, français, etc.)
  - Caractères spécifiques ? Par exemple : è§°!µ£...
- Faux logo, nom d'entreprise erroné, usurpation d'identité
- On vous invite à cliquer sur un lien
- Adresse email ou numéro de téléphone étrange, ne semble pas officiel

Plus de détails sur les signes à repérer à la page 8 !

1 LES DIFFÉRENTS TYPES D'ARNAQUE

L'USURPATION D'IDENTITÉ

Une pratique où un individu ou un programme se fait passer pour une personne de confiance en falsifiant ses données, comme une adresse IP, une adresse email ou un identifiant d'appelant, pour tromper les victimes et obtenir leurs informations personnelles et sensibles.

Regarde la vidéo

qui explique les arnaques de faux banquiers

PAR EMAIL

Le spoofing par e-mail est une technique utilisée dans les messages de spam et de phishing pour faire croire aux personnes ciblées qu'un message provient d'une personne ou d'une organisation connue ou de confiance. Les criminels modifient les en-têtes des e-mails pour que l'adresse visible de l'expéditeur soit différente (et donc familière !) et pour donner au message un caractère authentique, d'autant que l'adresse e-mail semble correcte.

PAR SITE WEB

Dans le cas du spoofing par l'intermédiaire d'un site web, les fraudeurs usurpent l'identité d'un site web d'une banque, d'un magasin ou d'une organisation de confiance. Cette opération s'accompagne souvent d'un faux e-mail ou d'un faux sms. Si vous cliquez sur le lien apparaissant dans le message, vous serez dirigé vers un faux site web qui ressemble à s'y méprendre au vrai. Il vous sera alors demandé de saisir vos coordonnées et vos codes secrets.

PAR TELEPHONE

Dans le cas du spoofing téléphonique, les fraudeurs utilisent un numéro de téléphone existant. Ils se font passer pour un·e employé·e de votre banque, de la police ou d'une autre institution connue et tentent d'obtenir vos informations confidentielles et vos codes à grand renfort d'excuses. Ils vident ensuite votre compte bancaire ou vous demandent d'effectuer vous-même un virement. Il arrive parfois aussi que les fraudeurs vous incitent à rappeler un numéro payant à votre insu. Ils vous tiennent ensuite en ligne aussi longtemps que possible jusqu'à ce que votre facture de téléphone explose

1 LES DIFFÉRENTS TYPES D'ARNAQUE

ARNAQUES LORS D'UN ACHAT

FRAUDE À L'ACHAT

Une situation où des acheteurs ou des vendeurs en ligne sont trompés par des annonces de produits fictifs, des sites de commerce électronique frauduleux, ou des paiements effectués mais non livrés, entraînant des pertes financières.

Découvrez l'article

qui explique comment reconnaître les arnaques sur les sites de revente

FRAUDE TRIANGULAIRE

Un scénario où un escroc utilise des informations de carte de crédit volées pour acheter des biens d'un vendeur légitime, puis revend ces biens à une victime sans méfiance, souvent à un prix réduit. La victime reçoit le produit, le vendeur légitime est payé, mais le véritable titulaire de la carte de crédit est facturé pour une transaction qu'il n'a pas autorisée.

Regardez la vidéo

qui donne un exemple de fraude triangulaire (aller directement à 2min)

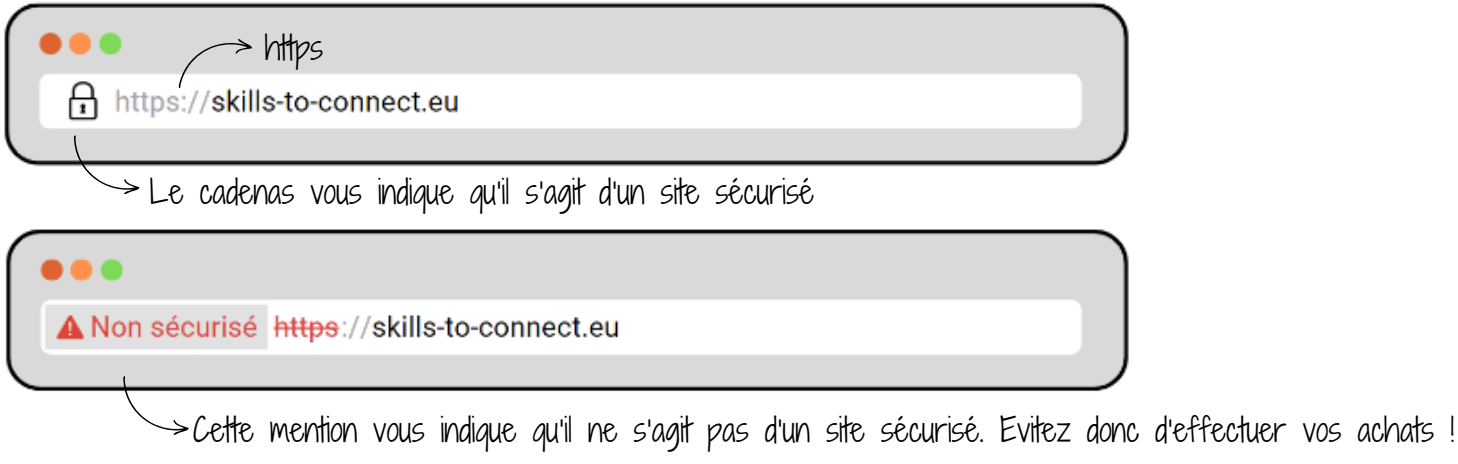
2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UN SITE FRAUDULEUX

Il peut être difficile de savoir si un site internet est vrai ou faux, surtout si vous n'êtes pas habitué à vérifier ces informations. Voici quelques **astuces simples** pour vous aider à repérer les sites frauduleux :

VÉRIFIEZ LA SÉCURITÉ DU SITE, À L'AIDE DE PLUSIEURS SIGNES :

Vérifiez l'adresse du site (ou URL), qui se trouve en haut de votre navigateur dans la barre d'adresse. Un site sûr commence toujours par "https://". Le "s" veut dire "sécurisé". Vous devriez aussi voir un petit cadenas à côté de l'adresse.
Faites attention aux adresses qui ressemblent aux vrais sites mais avec des fautes ou des ajouts !



Vérifiez également le nom de domaine !
Les fraudeurs copient souvent les adresses des sites connus en changeant juste un petit détail.

- Vrai site : https://www.amazon.com
- Faux site : https://www.amaz0n-shop.com (un "0" remplace le "o").

2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UN SITE FRAUDULEUX

OBSERVEZ LE DESIGN ET LE CONTENU DU SITE

comme l'exemple page 15 !

- Sur un vrai site, tout est souvent bien présenté : les textes sont clairs, sans fautes, et les images (comme les logos) sont de bonne qualité.
- Sur un faux site, vous trouverez souvent des fautes d'orthographe, des logos flous ou un design qui "semble bizarre". Parfois, certains liens ne fonctionnent pas.

CHERCHEZ LES INFORMATIONS DE CONTACT

- Un site sérieux affiche ses coordonnées : adresse, numéro de téléphone, et parfois un formulaire de contact. Vous trouverez souvent ces informations tout en bas de la page (dans les "mentions légales").
- Si ces informations n'existent pas ou semblent étranges (par exemple, un simple email type contact@gmail.com), méfiez-vous.

MÉFIEZ-VOUS DES OFFRES TROP BELLES POUR ÊTRE VRAIES

- Si un produit coûte beaucoup moins cher que partout ailleurs (par exemple, un iPhone à 100 euros), il y a de grandes chances que ce soit une arnaque

Astuce : Comparez les prix sur d'autres sites connus pour voir si cela semble réaliste.

REGARDEZ LES MOYENS DE PAIEMENT PROPOSÉS

- Les vrais sites utilisent des méthodes de paiement sécurisées, comme les cartes bancaires ou PayPal.
- Méfiez-vous si on vous demande un virement bancaire, un paiement en cryptomonnaie, ou un autre mode de paiement inhabituel. Une fois l'argent envoyé, vous ne pourrez souvent plus le récupérer.

2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UN SITE FRAUDULEUX

OBSERVEZ LE DESIGN ET LE CONTENU DU SITE

- Avant de faire confiance à un site, cherchez son nom dans Google suivi du mot "avis" ou "arnaque".
- Tapez "shoppingtech.fr avis" pour voir si d'autres personnes ont eu des problèmes.
- Consultez des sites d'avis fiables comme :
  - Trustpilot : est une plateforme d'avis où les utilisateurs partagent leurs expériences avec des entreprises, qu'elles soient positives ou négatives.
  - Signal-Arnaques : un site collaboratif dédié spécifiquement au signalement des escroqueries et arnaques, permettant d'alerter les autres utilisateurs sur des fraudes potentielles.
  - ScamDoc : outil en ligne qui analyse automatiquement la fiabilité d'un site web ou d'une adresse email en se basant sur des informations techniques et les avis des utilisateurs.

→ Utilisez ces outils pour vérifier la fiabilité de votre site ! Si vous voyez beaucoup de commentaires disant "commande jamais reçue" ou "paiement encaissé mais rien reçu", il s'agit probablement d'un faux site.

FAITES ATTENTION AUX PUBLICITÉS ET AUX FENÊTRES QUI S'OUVRENT PARTOUT (POP-UPS)

- Les faux sites contiennent souvent des publicités partout. Si vous voyez des fenêtres qui s'ouvrent tout le temps ou des messages vous disant que vous avez gagné un prix, fermez tout et quittez le site.

2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UN MESSAGE FRAUDULEUX

Les arnaques peuvent se présenter sous forme d'email, de SMS ou même d'appel téléphonique. Les fraudeurs essaient de vous tromper pour obtenir vos informations personnelles. Voici comment les repérer :

L'ADRESSE DE L'EXPÉDITEUR OU LE NUMÉRO SUSPECT

Les fraudeurs utilisent souvent des adresses ou numéros frauduleux. Il existe quelques signes à repérer pour être sûr que votre interlocuteur n'est pas un arnaqueur :

REPÉRER UNE ADRESSE E-MAIL FRAUDULEUSE :

Les fraudeurs utilisent souvent des adresses e-mail qui ressemblent à celles des entreprises officielles, mais avec de petites erreurs. Par exemple, au lieu de support@banque.com, un fraudeur pourrait utiliser banque-support@mail.com. Cela peut être difficile à voir au premier coup d'œil, mais en regardant attentivement, vous pouvez repérer la différence.

Si l'adresse e-mail semble étrange ou contient des fautes, c'est probablement une arnaque. Vérifiez toujours l'adresse sur le site officiel de l'entreprise avant de répondre.

REPÉRER UN APPEL FRAUDULEUX :

Les appels frauduleux peuvent provenir de numéros inconnus ou de numéros masqués (où aucun numéro n'apparaît sur votre téléphone). Les fraudeurs peuvent aussi utiliser des numéros qui ressemblent à ceux des entreprises, mais qui ont une légère différence. Par exemple, un appel peut sembler venir de votre banque, mais le numéro affiché n'est pas celui que vous avez l'habitude de voir.

Si l'appel vient d'un numéro masqué ou inconnu, ou si le numéro ne correspond pas à celui de l'entreprise, il est préférable de ne pas répondre. Contactez directement l'entreprise en utilisant les informations officielles pour vérifier si l'appel était légitime.

2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UN MESSAGE FRAUDULEUX

REPÉRER UN SMS FRAUDULEUX

- Certaines entreprises utilisent des numéros courts ou numéros spéciaux comme 8000, 8080 ou autres pour envoyer des SMS officiels, comme des alertes ou des promotions. Cependant, les fraudeurs peuvent aussi utiliser ces numéros pour masquer leur véritable identité et vous tromper.
- Si le SMS vient d'un numéro court inconnu ou d'un numéro étrange (par exemple, un numéro commençant par +44 ou +1), ou si le contenu vous semble trop urgent ou trop beau pour être vrai, il s'agit probablement d'une arnaque. Par exemple, un SMS prétendant provenir de votre banque, mais vous demandant de cliquer sur un lien ou de fournir des informations sensibles, est suspect.

Si vous ne reconnaissez pas le numéro ou si le message vous semble suspect, ne répondez pas et ne cliquez pas sur les liens. Contactez directement l'entreprise via son numéro officiel pour vérifier.

LE MESSAGE EST ÉTRANGE

Les messages frauduleux, qu'ils proviennent d'un email, d'un SMS, ou même d'un appel téléphonique, contiennent souvent des fautes de grammaire, des erreurs de syntaxe, ou des formulations maladroites. Ces erreurs sont un signe qu'il s'agit probablement d'une tentative d'escroquerie.

MESSAGES SE FAISANT PASSER POUR UNE ENTREPRISES :

Un message qui commence par "Cher utilisateur" au lieu d'utiliser votre prénom ou un "Bonjour Madame/Monsieur" est suspect. Les entreprises légitimes, comme les banques ou les sites de commerce en ligne, personnalisent généralement leurs messages en incluant votre nom dans l'objet ou le corps du texte. Si vous ne voyez pas votre nom ou si le message est trop générique, c'est une alerte.

- ✗ **FRAUDULEUX : CHER UTILISATEUR, VOTRE COMPTE SERA SUSPENDU.**
- ✓ **LÉGITIME : BONJOUR ___, NOUS AVONS UNE MISE À JOUR CONCERNANT VOTRE COMPTE.**

2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UN MESSAGE FRAUDULEUX

MESSAGES SE FAISANT PASSER POUR DES SERVICES PUBLICS OU GOUVERNEMENTAUX :

Si vous recevez un SMS ou un email qui semble provenir d'un service public (par exemple, des alertes fiscales ou sociales), mais avec des fautes d'orthographe, c'est une grande alerte. Les messages officiels des administrations sont généralement rédigés de manière soignée et professionnelle. Les fraudeurs essaient parfois de se faire passer pour des institutions publiques, mais ils ne prennent pas toujours soin de la qualité de leur rédaction.

- **FRAUDULEUX : LE FISC VOUS DOIT DES ARGENTS, CLIQUÉ ICI POUR RÉCLAMEZ VOS FONDS**
- **LÉGITIME : LE SERVICE DES IMPÔTS VOUS INFORME QUE VOUS AVEZ DROIT À UN REMBOURSEMENT. POUR PLUS D'INFORMATIONS, CONNECTEZ-VOUS À VOTRE ESPACE PERSONNEL**

MESSAGES SE FAISANT PASSER POUR UN·E AMI·E OU UNE PERSONNE DE CONTACT

Parfois, les arnaques peuvent sembler venir d'amis ou de contacts que vous connaissez, surtout si leur compte a été piraté. Si un message de votre ami semble étrange, qu'il y a des fautes ou que le ton est inhabituel (par exemple, "J'ai trouvé un super plan pour toi !"), il pourrait s'agir d'une tentative de phishing.

- **FRAUDULEUX : HÉ, REGARDE CETTE SUPER VIDÉO, JE PENSE QUE ÇA VA TE PLAIRE !**
- **LÉGITIME : SALUT___, JE T'ENVOIE LA VIDÉO DONT JE T'AVAIS PARLÉ, REGARDE-LA QUAND TU AS UN MOMENT 😊**

2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UN MESSAGE FRAUDULEUX

LE MESSAGE EST URGENT

Les arnaqueurs essaient souvent de vous faire réagir rapidement en vous mettant sous pression, en formulant des messages urgents ou menaçants.

MESSAGES URGENTS

Un message peut vous dire que votre compte va être bloqué ou que vous devez agir tout de suite pour éviter un problème :

- **VOTRE COMPTE SERA SUSPENDU DANS 24 HEURES !**
- **RÉPONDEZ MAINTENANT POUR ÉVITER LA FERMETURE DE VOTRE COMPTE**

OFFRES TROP PRESSANTES

Parfois, les arnaqueurs vous disent que vous avez gagné un prix, mais qu'il faut réagir immédiatement pour le recevoir :

- **VOUS AVEZ GAGNÉ 1000€, CLIQUEZ ICI AVANT CE SOIR POUR LE RÉCUPÉRER !**

OFFRES TROP PRESSANTES

Ils peuvent aussi essayer de vous faire peur avec des menaces d'amende ou de poursuites judiciaires si vous ne répondez pas rapidement

- **VOUS DEVEZ PAYER CETTE AMENDE DANS LES 48 HEURES, SINON VOUS SEREZ POURSUIVI EN JUSTICE !**

LE MESSAGE VOUS DEMANDE VOS DONNÉES PERSONNELLES

- Si un message vous demande des informations sensibles, comme votre mot de passe, vos numéros de carte bancaire ou votre code PIN, c'est un signe évident d'arnaque.
- **Aucune entreprise sérieuse ne vous demandera ces informations par email, SMS ou téléphone !**

2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UN MESSAGE FRAUDULEUX

LE MESSAGE VOUS DEMANDE VOS DONNÉES PERSONNELLES

- Si un message vous demande des informations sensibles, comme votre mot de passe, vos numéros de carte bancaire ou votre code PIN, c'est un signe évident d'arnaque.
- **Aucune entreprise sérieuse ne vous demandera ces informations par email, SMS ou téléphone !**

BON À SAVOIR

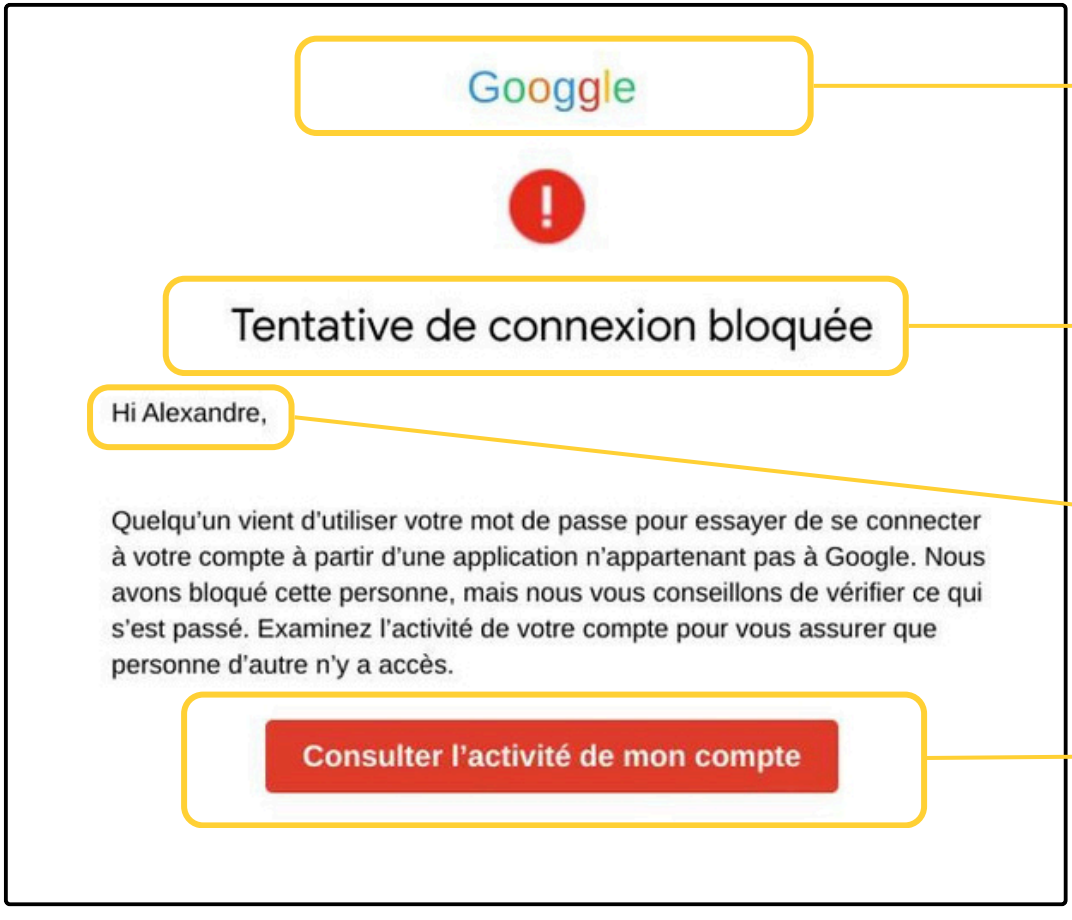
- Un conseiller bancaire ne vous demandera jamais vos données personnelles sensibles, comme votre mot de passe, par téléphone. Les banques n'ont pas besoin de votre mot de passe pour accéder à vos informations ou pour vous aider avec un problème. Si vous recevez un appel d'un conseiller vous demandant votre mot de passe ou d'autres informations confidentielles (comme votre code PIN ou votre numéro de carte bancaire), il s'agit probablement d'une tentative d'escroquerie. Ne répondez pas et contactez votre banque directement en utilisant les coordonnées officielles.

- Pour accéder aux services publics en ligne **en Belgique**, vous devez vous connecter via la plateforme CSAM (plateforme de services du gouvernement belge) ou ITSME, une application de sécurité. Par exemple, vous ne recevrez jamais de communication officielle sur vos impôts par email. Pour consulter vos impôts, cela se fait uniquement sur la plateforme MinFin. Si vous recevez un email vous demandant de cliquer sur un lien pour accéder à votre déclaration d'impôt, il s'agit d'une tentative de phishing. Ce type de fraude peut également concerner d'autres services publics, comme Ma Pension ou d'autres services gouvernementaux. Soyez vigilant et ne cliquez jamais sur un lien suspect dans un email.

2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UNE ARNAQUE

EXEMPLES DE PHISHING



Faux logo

le véritable logo de google ressemble à ça

Google

Message d'urgence

Joue sur les émotions, le stress et sur un sentiment d'urgence pour vous pousser à l'action sans réfléchir

Inhabituel

Mélange d'anglais et français

Pousse à action

Un lien frauduleux est dissimulé derrière le bouton

2 LES SIGNES À REPÉRER

COMMENT RECONNAITRE UNE ARNAQUE

EXEMPLES DE PHISHING

Nom mal orthographié
C'est Bouygues pas Buoygues

Message d'urgence
Joue sur les émotions, le stress et sur un sentiment d'urgence pour vous pousser à l'action sans réfléchir

Lien frauduleux
Le lien n'est pas sécurisé car il commence par "http" et pas "https" !

Pousse à action
Un lien frauduleux est dissimulé derrière le bouton !

A RETENIR !

Les arnaques en ligne prennent de nombreuses formes, telles que le phishing (hameçonnage), le spoofing (usurpation d'identité), ou encore les fraudes aux achats en ligne. Il est essentiel de rester vigilant face à ces tentatives de fraude. Un signe révélateur d’une arnaque peut être un message demandant des informations personnelles ou qui semble trop urgent ou trop beau pour être vrai. Vérifiez toujours l’adresse email, le numéro de téléphone, et les liens contenus dans les messages. Les fautes de grammaire ou un ton menaçant sont souvent des indicateurs de fraude. Enfin, si vous avez un doute, n’hésitez pas à contacter directement l’entreprise ou l’organisation par un canal officiel pour vérifier la légitimité du message. **Se protéger contre ces arnaques commence par savoir les reconnaître !**