

À la fin de ce module :



- vous comprendrez les techniques psychologiques utilisées dans les attaques de phishing
- Vous saurez identifier les e-mails, appels ou messages suspects qui cherchent à intercepter vos informations
- Vous connaîtrez les différentes stratégies de réaction, par exemple : comment réagir à un e-mail suspect ou à un clic sur un lien douteux

Qu'est-ce que le phishing ?

✻ **Félicitations!** 💰

**Vous avez gagné le prix de
la loterie nationale de
1.000.000€!
Cliquez ici**

Le phishing est une méthode de fraude par laquelle des criminels tentent d'obtenir des informations personnelles comme des mots de passe, des numéros de carte bancaire ou des données bancaires. Ils se font passer pour des institutions ou des personnes de confiance et envoient des e-mails ou des messages contenant des liens vers des sites web falsifiés. Dès que vous y saisissez vos informations, elles sont volées et utilisées à des fins criminelles.

Quels sont les risques ?



Préjudice financier : Les criminels peuvent utiliser vos données bancaires pour retirer de l'argent de vos comptes ou effectuer des achats en votre nom, entraînant des pertes financières.

Usurpation d'identité : Un fraudeur peut utiliser votre identité pour commettre des délits ou mener des activités illégales, ce qui peut avoir des conséquences juridiques pour vous.

**Teste tes
connaissances**

Phishing Quizz de Google: <https://phishingquiz.withgoogle.com/>

Mes notes & questions :

Comment se protéger contre le phishing ?

Les règles d'or:



- ✓ Think before you click ! Réfléchissez avant de cliquer !
Ne cliquez jamais sur des liens provenant d'expéditeurs inconnus.
- ✓ N'ouvrez pas les pièces jointes de courriels suspects.
- ✓ Vérifiez toujours l'identité de l'expéditeur.
- ✓ Si quelque chose semble trop beau pour être vrai, c'est probablement le cas !

Dois-je signaler le phishing ?



Un outil pratique qui vous permet de gérer facilement les e-mails suspects et de les signaler à des experts qui effectueront un diagnostic complet de chaque message transmis.

Que faire en cas de doute ou de fraude ?

1. Bloquez immédiatement votre carte en contactant Worldline Financial Services (Europe) S.A. au **(+352) 49 10 10** – Service disponible 24h/24 et 7j/7.
2. Changez vos mots de passe sans attendre.
3. Informez votre prestataire de services.
4. Besoin d'aide ? Contactez :
 - CIRCL (Centre de réponse aux incidents informatiques) : **24 78 84 44**
 - Beesecure Helpline : **8002 1234**



Mes notes & questions :