Quiz de 10 questions - Prévention de l'hameçonnage et à la sécurité en ligne

1. **Qu'est-ce que l'hameçonnage (phishing) ?**
   - ☐ a) Une méthode d'optimisation de site web
   - ☐ b) Une technique visant à voler des informations personnelles en se faisant passer pour un tiers de confiance
   - ☐ c) Un logiciel de protection des données
   - ☐ d) Une façon de sauvegarder ses mots de passe
2. **Quel est le but principal de l'hameçonnage ?**
   - ☐ a) Rediriger les utilisateurs vers des sites de vente
   - ☐ b) Voler des informations personnelles ou professionnelles pour les utiliser de manière frauduleuse
   - ☐ c) Créer un profil en ligne sécurisé
   - ☐ d) Aider à la navigation en ligne
3. **Quel est le premier réflexe à avoir si vous recevez un message douteux demandant des informations personnelles ?**
   - ☐ a) Cliquer sur le lien pour vérifier l'identité de l'expéditeur
   - ☐ b) Partager le message sur les réseaux sociaux
   - ☐ c) Ne jamais communiquer d'informations sensibles et contacter directement l'organisme concerné
   - ☐ d) Ignorer le message
4. **Que faire si vous constatez des débits frauduleux sur votre compte bancaire ?**
   - ☐ a) Attendre un mois avant de vérifier à nouveau
   - ☐ b) Faire opposition immédiatement auprès de votre banque
   - ☐ c) Changer vos mots de passe
   - ☐ d) Contacter un avocat
5. **Quel service peut être contacté pour signaler un message suspect reçu sans y répondre ?**
   - ☐ a) CyberÉco
   - ☐ b) Signal Spam
   - ☐ c) Phishing Report
   - ☐ d) Info Escroqueries

6. **Comment repérer un lien potentiellement frauduleux dans un message ?**

    - ☐ a) En vérifiant l'adresse web en passant le curseur sans cliquer
    - ☐ b) En téléchargeant un logiciel spécial
    - ☐ c) En demandant à un ami de cliquer pour vous
    - ☐ d) En ouvrant le lien directement pour voir ce qu'il contient

7. **Que devez-vous faire si vous avez divulgué un mot de passe à la suite d'un hameçonnage ?**

    - ☐ a) Laisser le mot de passe inchangé
    - ☐ b) Changer ce mot de passe et ceux des autres services où il est utilisé
    - ☐ c) Désactiver tous vos comptes en ligne
    - ☐ d) Réinitialiser votre ordinateur

8. **Quelle pratique est recommandée pour renforcer la sécurité de vos comptes en ligne ?**

    - ☐ a) Utiliser le même mot de passe partout
    - ☐ b) Utiliser des mots de passe complexes et différents pour chaque site
    - ☐ c) Noter tous ses mots de passe sur papier
    - ☐ d) Partager ses mots de passe avec ses proches

9. **Quelle méthode permet de vérifier si un accès illégitime a été effectué sur un compte en ligne ?**

    - ☐ a) Lire tous les e-mails reçus
    - ☐ b) Consulter les notifications sur son téléphone
    - ☐ c) Vérifier la date et l'heure de la dernière connexion à votre compte
    - ☐ d) Changer fréquemment de navigateur

10. **Qu'est-ce que la double authentification ?**

    - ☐ a) Une méthode pour créer des mots de passe plus courts
    - ☐ b) Un moyen de renforcer la sécurité en nécessitant deux étapes de vérification pour se connecter
    - ☐ c) Un type de spam
    - ☐ d) Un système utilisé uniquement par les banques

Voici les réponses au quiz :

1. b) Une technique visant à voler des informations personnelles en se faisant passer pour un tiers de confiance
2. b) Voler des informations personnelles ou professionnelles pour les utiliser de manière frauduleuse
3. c) Ne jamais communiquer d'informations sensibles et contacter directement l'organisme concerné
4. b) Faire opposition immédiatement auprès de votre banque
5. b) Signal Spam
6. a) En vérifiant l'adresse web en passant le curseur sans cliquer
7. b) Changer ce mot de passe et ceux des autres services où il est utilisé
8. b) Utiliser des mots de passe complexes et différents pour chaque site
9. c) Vérifier la date et l'heure de la dernière connexion à votre compte
10. b) Un moyen de renforcer la sécurité en nécessitant deux étapes de vérification pour se connecter