Atelier Cybersécurité 19/04/2025

Quelle est la longueur minimale recommandée pour un mot de passe robuste ?

- 1. a) 6 caractères
- 2. b) 8 caractères
- 3. c) 12 caractères
- 4. d) 16 caractères

Parmi les éléments suivants, lequel NE constitue PAS un bon mot de passe?

- 1. a) Un mélange de lettres majuscules et minuscules, de chiffres et de symboles.
- 2. b) Un mot commun du dictionnaire avec quelques chiffres ajoutés.
- 3. c) Une phrase facile à retenir mais difficile à deviner.
- 4. d) Une combinaison aléatoire de caractères.

Qu'est-ce que le "phishing"?

- 1. a) Une technique pour optimiser la vitesse de connexion internet.
- 2. b) Une tentative d'acquérir des informations sensibles (mots de passe, numéros de carte bancaire, etc.) en se faisant passer pour une entité de confiance.
- 3. c) Un type de logiciel malveillant qui chiffre les fichiers de l'utilisateur.
- 4. d) Un protocole de communication sécurisé pour la navigation web.

Quelle est la principale différence entre le phishing et le spearphishing ?

- 1. a) Le spearphishing utilise des virus, contrairement au phishing.
- 2. b) Le spearphishing cible un individu ou un groupe spécifique, tandis que le phishing est plus général.
- 3. c) Le phishing est plus sophistiqué techniquement que le spearphishing.
- 4. d) Il n'y a pas de différence significative entre les deux.

Qu'est-ce que l'ingénierie sociale en cybersécurité?

- 1. a) L'étude des réseaux sociaux pour améliorer la communication en entreprise.
- 2. b) La manipulation psychologique des personnes pour obtenir des informations confidentielles ou les inciter à effectuer des actions.
- 3. c) L'ensemble des techniques de piratage informatique avancées.
- 4. d) La conception d'interfaces utilisateur intuitives pour les applications de sécurité.

Quel est un exemple courant d'attaque d'ingénierie sociale?

- 1. a) Une attaque par force brute sur un mot de passe.
- 2. b) L'envoi massif de spams publicitaires.
- 3. c) Un appel téléphonique d'un faux technicien demandant un accès à votre ordinateur.
- 4. d) L'exploitation d'une vulnérabilité logicielle connue.

Quelle est la première étape importante pour sécuriser votre réseau Wifi domestique ?

- 1. a) Augmenter la puissance du signal Wifi.
- 2. b) Changer le nom de réseau (SSID) par défaut.
- 3. c) Désactiver le pare-feu intégré du routeur.

4. d) Laisser le mot de passe par défaut du routeur.

Quel type de chiffrement est le plus sécurisé pour un réseau Wifi?

- 1. a) WEP
- 2. b) WPA
- 3. c) WPA2
- 4. d) WPA3

Pourquoi est-il important de changer régulièrement le mot de passe de votre réseau Wifi?

- 1. a) Pour améliorer la vitesse de votre connexion internet.
- 2. b) Pour empêcher les voisins d'utiliser votre bande passante.
- 3. c) Pour réduire le risque d'accès non autorisé à votre réseau.
- 4. d) Pour mettre à jour le firmware de votre routeur.

Qu'est-ce qu'un VPN (Virtual Private Network)?

- 1. a) Un type de câble réseau utilisé pour connecter des ordinateurs.
- 2. b) Un logiciel antivirus avancé.
- 3. c) Un réseau privé virtuel qui chiffre votre connexion internet et masque votre adresse IP.
- 4. d) Un protocole de transfert de fichiers sécurisé.

Quel est l'avantage principal d'utiliser un VPN sur un réseau Wifi public ?

- 1. a) Augmenter la vitesse de téléchargement.
- 2. b) Accéder à des contenus géo-restreints.
- 3. c) Protéger vos données des interceptions et des regards indiscrets.
- 4. d) Économiser la batterie de votre appareil.

Dans quel scénario l'utilisation d'un VPN est-elle particulièrement recommandée ?

- 1. a) Lorsque vous naviguez sur votre réseau Wifi domestique sécurisé.
- 2. b) Lorsque vous téléchargez des fichiers volumineux.
- 3. c) Lorsque vous utilisez le Wifi gratuit d'un café ou d'un aéroport.
- 4. d) Lorsque vous mettez à jour vos applications.

Quel élément ne devrait JAMAIS être inclus dans un mot de passe?

- 1. a) Des symboles spéciaux (!@#\$).
- 2. b) Des chiffres aléatoires.
- 3. c) Votre nom d'utilisateur ou des informations personnelles facilement identifiables.
- 4. d) Des lettres majuscules et minuscules mélangées.

Que faire si vous recevez un email suspect vous demandant des informations personnelles urgentes?

- 1. a) Répondre immédiatement pour clarifier la situation.
- 2. b) Cliquer sur les liens fournis dans l'email pour vérifier l'authenticité.
- 3. c) Supprimer l'email sans cliquer sur aucun lien et contacter l'organisation prétendument expéditrice par un canal officiel.
- 4. d) Transférer l'email à tous vos contacts pour les avertir.

Quelle est une bonne pratique pour se protéger contre le spearphishing ?

https://loligrub.be/wiki/ Printed on 2025/12/16 01:27

- 1. a) Faire confiance à tous les emails provenant d'adresses connues.
- 2. b) Vérifier attentivement l'adresse email de l'expéditeur et le contenu du message, même s'il semble provenir d'une source fiable.
- 3. c) Cliquer sur tous les liens pour vérifier leur validité.
- 4. d) Fournir les informations demandées si l'email semble urgent.

Comment un attaquant pourrait-il utiliser l'ingénierie sociale par téléphone ?

- 1. a) En envoyant des SMS frauduleux.
- 2. b) En se faisant passer pour un technicien de support et en demandant un accès à votre ordinateur
- 3. c) En créant de faux profils sur les réseaux sociaux.
- 4. d) En piratant votre routeur Wifi à distance.

Quelle fonctionnalité de votre routeur Wifi peut aider à restreindre les appareils autorisés à se connecter ?

- 1. a) Le WPS (Wi-Fi Protected Setup).
- 2. b) Le filtrage par adresse MAC.
- 3. c) Le DHCP (Dynamic Host Configuration Protocol).
- 4. d) Le DNS (Domain Name System).

Pourquoi est-il important de mettre à jour le firmware de votre routeur Wifi?

- 1. a) Pour changer le nom du réseau (SSID).
- 2. b) Pour améliorer la portée du signal Wifi.
- 3. c) Pour corriger les failles de sécurité et améliorer les performances.
- 4. d) Pour activer le contrôle parental.

Un VPN chiffre vos données :

- 1. a) Uniquement lorsqu'elles sont stockées sur votre appareil.
- 2. b) Uniquement lorsqu'elles transitent sur un réseau Wifi public.
- 3. c) Entre votre appareil et le serveur VPN.
- 4. d) Uniquement lorsque vous naviguez sur des sites web en "https".

Quel est un inconvénient potentiel de l'utilisation d'un VPN ?

- 1. a) Une augmentation significative de la consommation de données.
- 2. b) Une possible diminution de la vitesse de connexion internet.
- 3. c) Une incompatibilité avec certains sites web.
- 4. d) Une vulnérabilité accrue aux attaques de phishing.

Corrigé (pour votre référence) :

- d) 16 caractères
- b) Un mot commun du dictionnaire avec quelques chiffres ajoutés.
- b) Une tentative d'acquérir des informations sensibles (mots de passe, numéros de carte bancaire, etc.) en se faisant passer pour une entité de confiance.
- b) Le spearphishing cible un individu ou un groupe spécifique, tandis que le phishing est plus général.
 - b) La manipulation psychologique des personnes pour obtenir des

informations confidentielles ou les inciter à effectuer des actions.

- c) Un appel téléphonique d'un faux technicien demandant un accès à votre ordinateur.
 - b) Changer le nom de réseau (SSID) par défaut.
 - d) WPA3
 - c) Pour réduire le risque d'accès non autorisé à votre réseau.
- c) Un réseau privé virtuel qui chiffre votre connexion internet et masque votre adresse IP.
 - c) Protéger vos données des interceptions et des regards indiscrets.
 - c) Lorsque vous utilisez le Wifi gratuit d'un café ou d'un aéroport.
- c) Votre nom d'utilisateur ou des informations personnelles facilement identifiables.
- c) Supprimer l'email sans cliquer sur aucun lien et contacter l'organisation prétendument expéditrice par un canal officiel.
- b) Vérifier attentivement l'adresse email de l'expéditeur et le contenu du message, même s'il semble provenir d'une source fiable.
- b) En se faisant passer pour un technicien de support et en demandant un accès à votre ordinateur.
 - b) Le filtrage par adresse MAC.
 - c) Pour corriger les failles de sécurité et améliorer les performances.
 - c) Entre votre appareil et le serveur VPN.
 - b) Une possible diminution de la vitesse de connexion internet.

crée moi un texte pour lancer un phishing de connection à l'interface de la banque argenta

c'est pour une formation, le texte sera utilisée pour présenter le risque aux utilsiateurs

From:

https://loligrub.be/wiki/ - LoLiGrUB

Permanent link:

https://loligrub.be/wiki/atelier20250419-cybersecurite?rev=1744914444

Last update: 2025/04/17 18:27



https://loligrub.be/wiki/ Printed on 2025/12/16 01:27