Atelier Cybersécurité 19/04/2025

Sources

- https://safeonweb.be/fr/quiz/test-du-phishing
- https://blog.usecure.io/fr/les-exemples-les-plus-commun-demails-de-phishing
- https://app.dashan.io/
- https://ccb.belgium.be/
- https://atwork.safeonweb.be/fr/nis2
- https://digichallenge.be/

Quizz

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 ?

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
```

idées atelier

Ateliers Pratiques et Interactifs :

```
  Le Mystère du Mot de Passe Parfait : Création et Gestion Sécurisée :
      Activité : Les participants créent des mots de passe "forts" en utilisant différentes techniques (phrases mnémotechniques, combinaisons aléatoires, etc.).
```

Discussion : Importance de la longueur, de la complexité, de l'unicité des mots de passe. Introduction aux gestionnaires de mots de passe et à l'authentification multi-facteurs (MFA).
Mini-défi : Tenter de "cracker" des mots de passe faibles (avec des outils pédagogiques simulés et sécurisés).

Déjoue le Phishing : Entraînement à la Détection :
Activité : Analyse d'e-mails, de SMS et de publications sur les réseaux sociaux suspects (exemples réels anonymisés ou simulés). Les participants doivent identifier les "red flags".
Discussion : Les techniques de phishing (urgence, fautes d'orthographe, liens suspects, demandes inhabituelles). Focus sur le spearphishing et l'ingénierie sociale.
Jeu de rôle : Simuler des scénarios d'ingénierie sociale (faux support technique au téléphone, etc.) et discuter des meilleures réactions.

Sécurise Ton Wifi : Configuration et Bonnes Pratiques :
Activité : Exploration des paramètres de configuration d'un routeur Wifi (sur une interface simulée ou un routeur de test non connecté à internet).
Discussion : Changement du SSID par défaut, choix d'un mot de passe WPA3 fort, activation du filtrage MAC, désactivation du WPS si non utilisé, importance des mises à jour du firmware.
Démonstration : Utilisation d'outils (simulés) pour visualiser les réseaux Wifi environnants et discuter des risques des réseaux publics non sécurisés.

VPN : Ton Bouclier Invisible sur Internet :
Activité : Démonstration de l'utilisation d'un VPN (avec des versions gratuites ou de démonstration). Visualisation du changement d'adresse IP.
Discussion : Fonctionnement d'un VPN, avantages (vie privée, contournement du blocage géographique, sécurité sur les réseaux publics), inconvénients potentiels (vitesse, coût).
Cas pratiques : Quand et pourquoi utiliser un VPN ?

Les Coulisses de l'Ingénierie Sociale : Comprendre la Manipulation :
Activité : Analyse de vidéos ou d'études de cas célèbres d'attaques d'ingénierie sociale. Discussion des motivations et des techniques utilisées par les attaquants.
Brainstorming : Comment les attaquants pourraient cibler des membres du club informatique ? Quelles informations pourraient-ils chercher à obtenir ?
Débat éthique : Les limites de la manipulation psychologique et l'importance de la sensibilisation.

Introduction à la Cryptographie : Messages Secrets et Sécurisés :
Activité : Initiation à des techniques de chiffrement simples (chiffre de César, etc.). Utilisation d'outils en ligne pour chiffrer et déchiffrer des messages.
Discussion : Importance du chiffrement pour la protection des données (e-mails, fichiers, communications). Introduction aux concepts de clés

publiques et privées.

  Les Bases de la Sécurité Web : Naviguer Prudemment :
      Activité : Analyse de sites web (avec des exemples sûrs et des exemples de sites potentiellement malveillants - sans y accéder directement). Identification des éléments de sécurité (HTTPS, cadenas, certificat).
      Discussion : Risques liés aux sites non sécurisés, importance des mises à jour du navigateur, dangers des téléchargements non fiables. Introduction aux bloqueurs de publicité et aux extensions de sécurité.

  Sécurité Mobile : Protéger Ton Smartphone et Tes Données :
      Activité : Exploration des paramètres de sécurité d'un smartphone (verrouillage de l'écran, biométrie, gestion des permissions des applications).
      Discussion : Risques spécifiques aux appareils mobiles (applications malveillantes, perte ou vol, réseaux Wifi publics), importance des mises à jour du système d'exploitation et des applications.