Parcours TAI

Module Cybersécurité et RGPD

Activité 2 – La cybersécurité en entreprise

Objectif : Identifier les risques cyber en entreprise et présenter les bonnes pratiques en tant que professionnel de l'assistance informatique.

Consignes :

-Vous êtes chargé(e) de sensibiliser vos collègues aux bonnes pratiques de cybersécurité dans l'entreprise

-Pour chaque thème ci-dessous, effectuer vos propres recherches (sites spécialisés comme cybermalveillance.gouv.fr, ANSSI, CNIL, …)

-Notez vos réponses de manière claire et structurée

-Vous devez illustrer vos réponses par **des exemples concrets** ou **des situations professionnelles**

-Préparer-vous à présenter vos résultats à l'oral ou à rédiger un mini-guide de sensibilisation pour l'examen de fin de module

Thème 1 – Sécurité sur Internet & déplacements professionnels

1. Quels sont les principaux dangers liés à l'utilisation d'internet en entreprise ?

   Risques de malwares et de phishing, exposition des données sensibles (vol d'informations), failles de sécurité sur les réseaux publics.

2. Comment reconnaitre un site web malveillant ? Quels outils ou habitudes peuvent aider à s'en prémunir ?

   URL suspecte (erreurs dans le nom de domaine), absence de HTTPS dans l'adresse, contenu ou design incohérent.

3. Pourquoi est-il important d'installer un antivirus et de maintenir ses logiciels à jour ?

   Protection contre les logiciels malveillants, correction des failles de sécurité exploitées par les hackers.

4. Lors de déplacements professionnels, quelles sont les menaces potentielles sur les données de l'entreprise ?

Connexions sur des réseaux Wi-Fi publics non sécurisés, Vol ou perte d'appareils contenant des **données sensibles.**

5. Quelles précautions prendre lorsqu'on se connecte à internet à l'extérieur de l'entreprise (hôtel, aéroport, coworking, café-restaurant) ?

   Utiliser un VPN pour sécuriser la connexion, éviter les réseaux publics sans protection, activer l'authentification à deux facteurs sur les comptes professionnels.

Thème 2 – Les mots de passe et la double authentification

1. Quelles sont les caractéristiques d'un mot de passe sécurisé ?

   Minimum 12 caractères, mélange de lettres, chiffres et symboles, pas de mot commun ni d'informations personnelles.

2. Pourquoi est-il recommandé d'utiliser un mot de passe différent pour chaque service ?

   Si un mot de passe est compromis, il ne doit pas affecter tous les autres comptes, éviter les attaques par bourrage de mots de passe.

3. Quels sont les risques liés à l'utilisation d'informations personnelles dans un mot de passe ?

   Facilité pour un **pirate** de deviner un mot de passe basé sur une date de naissance ou un prénom.

4. Qu'est-ce que la double authentification et dans quels cas est-elle indispensable ?

   Ajout d'une étape supplémentaire pour accéder à un compte (SMS, application de sécurité), indispensable pour les comptes sensibles (email, banque, accès entreprise).

5. Existe-t-il des outils pour gérer les mots de passes ? Sont-ils fiables ?

   Bitwarden, 1Password, KeePass → Stocker et générer des mots de passe complexes. Fiables, mais doivent être protégés par un mot de passe maître sécurisé

Thème 3 – Sécurité des e-mails

1. Quels types de menaces peuvent se cacher dans un e-mail (pièce jointe, lien, contenu) ?

   Pièces jointes infectées (ransomware, virus), liens piégés conduisant vers des sites de phishing. Usurpation d'identité (messages frauduleux se faisant passer pour des entreprises légitimes).

2. Quels sont les indices qui permettent d'identifier un e-mail potentiellement frauduleux ?

Adresse expéditeur étrange ou contenant des erreurs. Tonalité urgente et demande de clic immédiat. Fautes d'orthographe et mises en page maladroites.

3. Quelle attitude adopter lorsqu'un message suspect est reçu ?

   Ne jamais cliquer sur les liens, ne pas télécharger les pièces jointes douteuses, signaler l'e-mail à l'équipe informatique.

4. A qui signaler un e-mail douteux dans une entreprise ? Pourquoi est-ce important ?

   Équipe IT ou DSI (Directeur des Systèmes d'Information)

5. Quelles pratiques doivent être mises en place pour sécuriser la messagerie professionnelle ?

   Filtrage anti-spam activé, authentification renforcée (2FA), ne jamais partager ses identifiants par e-mail.

Thème 4 – Phishing, ransomware & séparation des usages

1. En quoi consiste une attaque de phishing ? Donner un exemple de scénario

   Technique visant à piéger un utilisateur pour qu'il divulgue ses informations. Exemple : Un faux email de banque demandant de « mettre à jour ses informations » via un lien frauduleux.

2. Que se passe-t-il lors d'une attaque par ransomware ? Quelles sont les conséquences possibles pour l'entreprise ?

   Un logiciel chiffre toutes les données du poste infecté et demande une rançon. Impact : Perte des données, paralysie de l'entreprise, impact financier.

3. Comment détecter qu'un poste est compromis par un logiciel malveillant ?

   Ralentissements soudains et comportement anormal du système. Fenêtre de demande de rançon qui s'affiche. Fichiers devenus illisibles ou renommés étrangement.

4. Quelles sont les premières actions à entreprendre en cas d'infection avérée ?

   Déconnecter immédiatement le poste du réseau, ne pas payer la rançon (aucune garantie de récupération des données), prévenir la cellule de sécurité informatique.

5. Pourquoi faut-il **absolument séparer** les usages professionnels et personnels sur les outils numériques ? Quelles sont les bonnes pratiques à ce sujet ?

   Éviter les contaminations via téléchargements personnels, limiter les risques en cas de vol ou piratage. Bonnes pratiques : Utiliser un PC dédié au travail, éviter les connexions à des comptes personnels sur l'ordinateur professionnel.