

FICHE DE SENSIBILISATION

INGÉNIERIE SOCIALE & SÉCURITÉ PHYSIQUE

Objectif : Cette fiche a pour objectif de sensibiliser l'ensemble du personnel aux risques d'ingénierie sociale et de renforcer les bonnes pratiques de sécurité physique et numérique au sein de l'organisation.

1. LES 3 ATTAQUES D'INGÉNIERIE SOCIALE LES PLUS COURANTES

1.1 TAILGATING / PIGGYBACKING

Description : Une personne non autorisée suit un employé légitime pour entrer dans une zone sécurisée sans présenter de badge ou d'identification. **Méthode** : L'attaquant profite de la politesse, de la distraction ou de moments d'affluence (pause-café, déjeuner) pour suivre un employé autorisé. **Conséquences** : Accès non autorisé aux locaux, vol d'informations, installation de matériel d'écoute, accès aux systèmes informatiques.

1.2 BAITING / APPÂT NUMÉRIQUE

Description : Utilisation d'un appât physique ou numérique pour inciter une victime à exécuter une action compromettante. **Méthode** : Clé USB « perdue », CD-ROM « promotionnel », lien trompeur par email, offre trop alléchante en ligne. **Conséquences** : Installation de malware, vol de données, prise de contrôle du poste de travail, accès au réseau interne.

1.3 IMPERSONNATION / USURPATION D'IDENTITÉ

Description : L'attaquant se fait passer pour une personne de confiance ou une autorité légitime pour obtenir des informations ou un accès. **Méthode** : Appel téléphonique en se faisant passer pour le support IT, technicien de maintenance, cadre supérieur, ou fournisseur. **Conséquences** : Divulcation d'informations confidentielles, modification de paramètres de sécurité, autorisation d'accès frauduleuse.

2. BONNES PRATIQUES DE SÉCURITÉ

RÈGLE N°1 : NE JAMAIS LAISSER SUIVRE SANS BADGE • Chaque personne doit présenter son badge d'accès individuel • Ne jamais tenir la porte pour un inconnu, même s'il semble pressé • Vérifier systématiquement que la porte se referme bien derrière vous • Signaler immédiatement toute personne sans badge dans les zones sécurisées

Scénario type : Un individu se présente à l'entrée en prétendant avoir oublié son badge. Il vous demande de le laisser passer car il a un rendez-vous urgent avec la direction. **Réponse appropriée :** 1. Lui demander de contacter son interlocuteur pour qu'il vienne le chercher 2. L'accompagner à la réception pour vérifier son identité 3. Ne jamais lui donner accès sans vérification formelle

RÈGLE N°2 : NE JAMAIS BRANCHER DE CLÉ USB INCONNUE • Toute clé USB trouvée doit être remise au service sécurité/système • N'utiliser que des périphériques fournis et approuvés par l'entreprise • Désactiver l'exécution automatique sur tous les postes de travail • Scanner tout périphérique externe avant utilisation

Scénario type : Vous trouvez une clé USB dans le parking avec une étiquette "Salaires Décembre 2023 - CONFIDENTIEL". **Réponse appropriée :** 1. Ne pas brancher la clé USB sur votre ordinateur 2. La remettre immédiatement au service sécurité 3. Signaler la découverte à votre responsable

RÈGLE N°3 : TOUJOURS VÉRIFIER L'IDENTITÉ D'UN INTERVENANT • Demander systématiquement une pièce d'identité officielle • Vérifier l'autorisation de visite auprès du service concerné • Accompagner les visiteurs dans les zones non publiques • Ne jamais divulguer d'informations sans autorisation préalable

RÉCAPITULATIF DES BONNES PRATIQUES

Situation	Action à éviter	Action à privilégier
Personne sans badge	Laisser passer par politesse	Demander vérification identité
Clé USB trouvée	La brancher pour voir le contenu	Remettre à la sécurité
Technicien inconnu	Lui donner accès immédiat	Vérifier auprès du service IT
Appel "urgent" du support	Donner ses identifiants	Rappeler sur numéro officiel
Email suspect	Cliquer sur les liens	Signaler à l'équipe sécurité

3. CADRE LÉGAL ET RÉFÉRENCES

LOI N° 19-05 DU 10 RAMADHAN 1440 CORRESPONDANT AU 15 MAI 2019 relative à la protection des personnes physiques dans le traitement des données à caractère personnel **Article 14 : Violation de la vie privée** "Constitue une violation de la vie privée le fait, par tout moyen, de collecter, de traiter, de conserver, d'utiliser ou de divulguer des données à caractère personnel concernant une personne physique sans son consentement exprès, ou en violation des dispositions de la présente loi." **Sanctions prévues** : • Amende de 100.000 à 1.000.000 DZD • Emprisonnement de 6 mois à 2 ans • Les deux peines peuvent être cumulées **Responsabilité de l'entreprise** : En cas de violation de données due à une négligence dans les mesures de sécurité, l'entreprise peut être tenue responsable civilement et pénalement.

OBLIGATIONS DES EMPLOYÉS Conformément à la politique de sécurité de l'entreprise et aux dispositions légales, chaque employé est tenu de : 1. Respecter les procédures de sécurité établies 2. Signaler immédiatement tout incident ou tentative d'intrusion 3. Protéger les informations confidentielles dont il a connaissance 4. Participer aux formations de sécurité organisées 5. Ne pas contourner les mesures de sécurité mises en place

CONTACTS EN CAS D'INCIDENT • **Service Sécurité** : extension 1111 | securite@entreprise.dz • **Support Informatique** : extension 2222 | support.it@entreprise.dz • **Ressources Humaines** : extension 3333 | rh@entreprise.dz • **Urgences 24/7** : 021-XX-XX-XX

ATTESTATION DE PRISE DE CONNAISSANCE Je soussigné(e), _____, certifie avoir pris connaissance du contenu de cette fiche de sensibilisation et m'engage à respecter les bonnes pratiques de sécurité décrites. Fait à _____, le ____/____/____
Signature :