F2. Utiliser en toute sécurité les réseaux sociaux

Aussi banalisé qu'il soit, l'usage des réseaux sociaux par les salariés n'est pas toujours anodin. En effet, un salarié peut, volontairement ou non, porter préjudice à son établissement par ses publications. C'est pourquoi chaque établissement doit adopter une politiqur en la matière et chaque salarié un comportement adéquat.

ORGANISATIONNEL

➤ Mettre en place une charte sur le bon usage des réseaux sociaux à l'attention des salariés.

➤ Instaurer des séances de sensibilisation régulière du personnel et rappeler les enjeux liés à l'usage des réseaux sociaux pour l'entreprise et le caractère juridique de la charte.

➤ Expliquer les principales vulnérabilités associées à l'usage des réseaux sociaux telles que :

- la publication de contenus révélant son activité professionnelle ou la politique de l'entreprise ;
- les interactions sociales entre les utilisateurs connus ou inconnus ;
- la possibilité d'être utilisés comme vecteurs de transmission de logiciels malveillants, d'attaque par **hameçonnage** ou par **ingénierie sociale**.

COMPORTEMENTAL

➤ Appliquer les bonnes pratiques indiquées dans la charte de l'entreprise.

➤ Avant toute diffusion, s'assurer que l'information publiée n'est pas susceptible de compromettre les intérêts de l'entreprise.

➤ Ne jamais utiliser le même mot de passe pour accéder à un réseau social et aux ressources informatiques de l'entreprise.

➤ Éviter de communiquer des informations professionnelles et personnelles trop détaillées (organigramme, positionnement hiérarchique, responsabilités professionnelles, missions à l'étranger, projets en cours, situation matrimoniale, date et lieu de naissance, numéro de téléphone, etc.) sur les réseaux sociaux.

➤ Utiliser prudemment les données de géolocalisation ouvertes sur les réseaux sociaux. Elles peuvent apporter des renseignements sur l'emploi du temps professionnel : absence, vacances, missions, etc. Vérifier régulièrement les paramètres de confidentialité et de sécurité des comptes. Privilégier une authentification forte pour protéger les mots de passe.

➤ Être vigilant quant aux multiples sollicitations *via* les réseaux sociaux (contacts par messagerie, commentaires – *posts* –, liens hypertexte, photos de célébrités, etc.). Ces approches peuvent mener vers des pages malveillantes et permettre de pirater des comptes, dérober des informations personnelles ou professionnelles ou infecter les systèmes d'informations d'un établissement.

Mots clés

Hameçonnage (*phishing*) : méthode d'attaque qui consiste à imiter les couleurs d'une entreprise ou d'une institution pour inciter le destinataire à fournir des informations personnelles.

Ingénierie sociale : recueil d'informations basée sur l'étude de l'environnement personnel et/ou professionnel, à partir notamment des informations publiées sur les réseaux sociaux par la personne ciblée.

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)
- Guide d'hygiène informatique
- Recommandations de sécurité relatives aux mots de passe