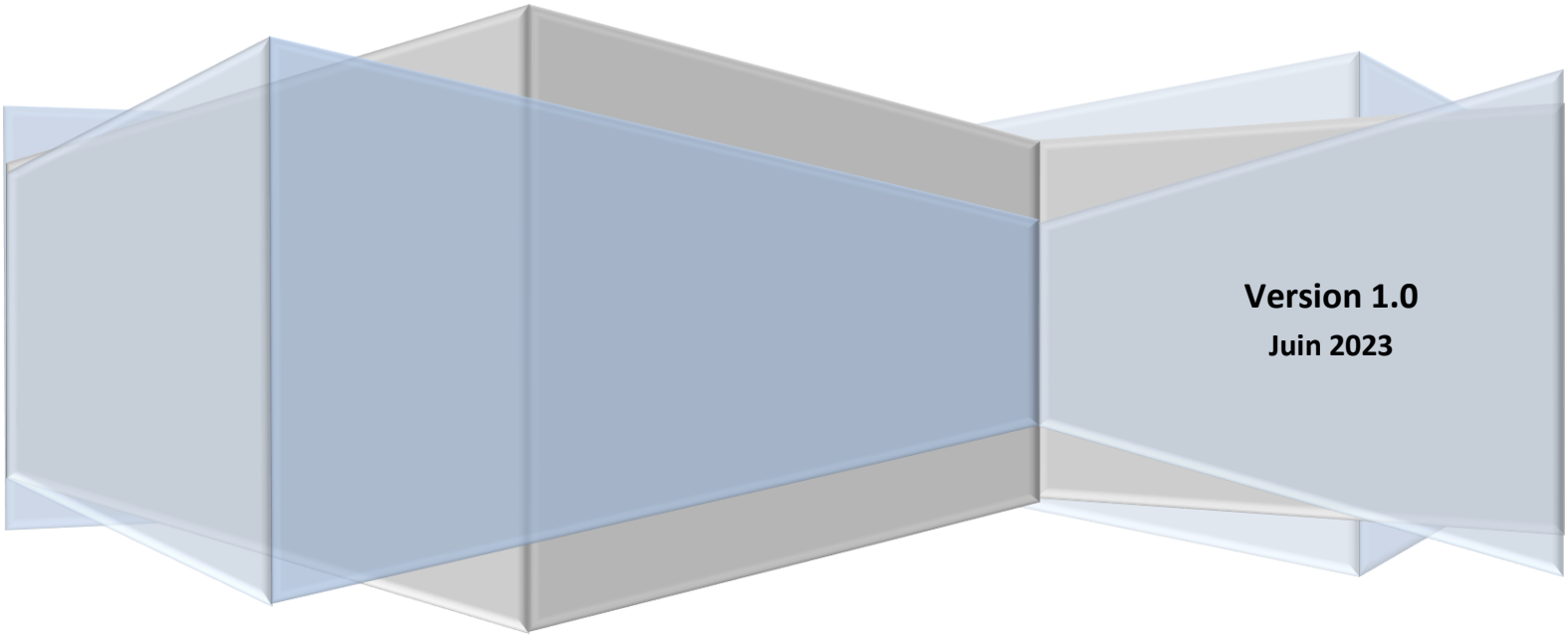
الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

GUIDE DE BONNES PRATIQUES POUR UNE ADMINISTRATION SÉCURISÉE DES PAGES FACEBOOK OFFICIELLES



Version 1.0

Juin 2023

GUIDE DE BONNES PRATIQUES POUR UNE ADMINISTRATION SÉCURISÉE DES PAGES FACEBOOK OFFICIELLES

Introduction

La sécurité des **réseaux sociaux** des organismes est essentielle pour préserver leurs réputations, éviter les atteintes à la confidentialité, prévenir les usurpations d'identité, se protéger contre les tentatives de Phishing et des escroqueries et maintenir la confiance de leurs abonnés. Pour cette occasion, l'**Agence Nationale de la Sécurité Informatique** - **ANSI** met à la disposition des organismes publics ce guide qui **groupe les différentes mesures** à appliquer pour **réduire le risque de piratage** via **leurs réseaux sociaux professionnels**, entre autres, leurs **pages Facebook officielles**.

A- Sécurité des postes de travail pour les administrateurs de la page Facebook officielle

- Utiliser un ***poste de travail protégé*** par des solutions de sécurité telles que l'***antivirus***, les ***firewalls*** et les ***IDS/IPS***. De plus, l'efficience de ces solutions dépend énormément de leur ***bonne configuration ou paramétrage validé par le RSSI*** de votre établissement ;
- Il ne faut ***jamais utiliser un appareil tierce*** ou d'***une autre personne*** pour la gestion du contenu relatif à la page Facebook ;
- Utiliser une infrastructure de ***logiciels fiables*** en optant pour des ***logiciels authentiques*** notamment les ***systèmes d'exploitation***, les **outils dédiés aux processus métiers** et les **extensions des navigateurs web**. En effet, cela va ***réduire***, drastiquement, le ***risque de l'exploitation des failles de sécurité relatives aux logiciels et le vol de vos données enregistrées dans les caches des navigateurs web***;
- Il est recommandé d'adopter une ***politique de sécurité*** qui inclus l'aspect organisationnel de la ***gestion des comptes utilisateurs*** et ce, à travers la création d'une procédure qui permet de spécifier la ***responsabilité et les tâches des différents intervenants*** dans le processus de ***gestion du contenu digital de l'entreprise***.

- Il faut adopter une ***politique rigoureuse de gestion des mots de passe*** ainsi que la ***gestion des privilèges***. Il est aussi, crucial de ***renforcer la sécurité des accès relatifs aux comptes des administrateurs*** ;

- Utiliser des ***comptes utilisateurs de privilèges limités*** pour l'administration et l'édition de la page Facebook ;

- S'assurer que le poste de travail, lors de l'administration ou l'édition de la page Facebook officielle, est ***connecté à un réseau sécurisé.***

- ***Eviter les connexions aux réseaux Wi-Fi public***.

B- Gestion des rôles pour l'administration de la page Facebook officielle

Facebook offre la possibilité d'attribuer un rôle pour chaque compte associé à la page et permet ainsi, de limiter les actions que l'on peut réaliser sur la page. De ce fait, pour une page Facebook donnée, il est fortement recommandé de **définir un seul « Administrateur »** et d'**attribuer des rôles limités** et adaptés **pour les autres intervenants** sur la page :

- **Éditeur** : Le rôle d'éditeur permet de tout faire, sauf gérer les rôles et les paramètres de la Page.
- **Modérateur : Les modérateurs peuvent envoyer des messages et** répondre aux commentaires sur la Page.
- **Gestionnaire d'offres d'emplois** : Le gestionnaire d'offres d'emploi peut publier des offres d'emploi et gérer les candidatures.
- **Annonceur** : Le rôle d'annonceur permet uniquement de créer des publicités et de consulter les statistiques.
- **Analyste** : Les analyses peuvent uniquement consulter les statistiques et connaître l'identité des personnes qui ont publié sur la Page.

D'autre part, l'**ANSI** vous recommande de :

- **Choisir** avec précaution les **administrateurs** et les **éditeurs** de la page ;
- **Créer** pour chaque intervenants **des comptes dédiés** et d'**éviter** immédiatement l'utilisation **des comptes email et Facebook personnels** ;
- De **réserver des numéros de téléphone mobile** pour **chaque intervenant** qui seront **utiles pour l'authentification à double facteurs** (Voir « **C** »).

C- Sécurité des accès aux comptes de messageries électroniques et aux comptes Facebook liés à l'administration de la page Facebook officielle

Pour assurer l'utilisation sécurisée de la **page Facebook officielle**, il faut protéger les accès aux « **comptes de messageries électroniques »** liés aux « **comptes Facebook » des différents intervenants.** La gestion de ces accès doit être **contrôlée** et **approuvée par le RSSI** de l'organisme.

De ce fait, l'**ANSI** vous recommande de :

- Utiliser la ***navigation privée*** pour l'administration et l'édition de la page Facebook ;
- Se connecter au Facebook via une ***connexion sécurisée*** (***HTTPS***) et vérifier que l'URL commence par **https**://www.facebook.com/;
- Déployer des **mots de passes robustes** avec des combinaisons de lettres, de chiffres, de caractères spéciaux et d'éviter l'utilisation des informations personnelles évidentes ;
- **Ne pas utiliser les mêmes mots de passe** pour le compte **email** et le compte **Facebook** ;
- **Ne pas enregistrer les mots de passe** de votre compte email et de votre compte Facebook **dans le navigateur web** ;
- Activer **l'authentification à deux facteurs (A2F)** qui permet la **réception d'un code de vérification** par **SMS**, via une **application d'authentification** ou une **clé de sécurité physique** afin d'approuver **les demandes de connexion** pour chaque **comptes email** et chaque **comptes Facebook impliqués**;
- **Activer les alertes** qui se déclenchent lors d'une connexion via un appareil ou un navigateur **qui ne sont pas habituellement utilisés** ;
- **Activer le chiffrement des emails de notifications** ;
- **Surveiller** régulièrement **votre page** afin d'éviter les **activités suspectes**, les **messages indésirables** ou les **publications inappropriées** ;
- **Vérifier** régulièrement les « **Accès à la page »** l' **« Historique de gestion de votre page »** afin de signaler les **utilisateurs suspects.**
- **Ne pas cliquer sur les liens suspects** pour éviter les attaques de **Phishing** ;

- **Eviter de partager des informations confidentielles et privés** sur la page Facebook ;
- **Déconnecter les comptes après avoir finis les modifications** souhaitées sur la page.

D- Activation du Badge Bleu

Le **badge bleu sur Facebook** est un symbole de **vérification d'authenticité** et de **légitimité** d'un compte. Il indique que la page ou le profil vérifié est celui d'une entreprise ou d'une organisation. La **vérification est effectuée par Facebook** pour confirmer l'identité de la personne ou de l'entité derrière le compte. Pour qu'un organisme public puisse **obtenir ce badge** pour sa **page Facebook officielle**, il doit coordonner avec l'ANSI conformément au **circulaire 23 du 05 novembre 2020** et déposer sa demande en arabe ou en français dont le sujet est « **Demande d'obtention du badge bleu / حول الحصول على الشارة الزرقاء**» à l'**ANSI** par **email** aux adresses **ansi@ansi.tn / boc@ansi.tn,** par **Fax** au numéro 71 846 363 **ou par voie postale** à l' « Agence Nationale de la Sécurité Informatique » –Adresse : 49, avenue Jean Jaurès, 1000 Tunis. En effet, cette demande doit mentionner les informations suivantes :

- Le **lien de la page facebook officielle**.
- Les **noms et prénoms**, les **emails professionnels dédiés**, les **numéros de téléphone mobile dédiés** de l'administrateur et les éditeurs qui interviennent pour l'administration de la page Facebook officielle.

Références

- Pages d'aide de Facebook

  https://www.facebook.com/help

- Centre de sécurité de Business Manager

  https://www.facebook.com/business/help/216940652189296?id=199156230960298&wtsid=rdr_0P63sSXsAZJD1L6vO

- Guide pour la sécurité de la messagerie électronique

  https://www.ansi.tn/sites/default/files/guide%20de%20La%20s%C3%A9curit%C3%A9%20de%20la%20messagerie%20electronique.pdf