Playbook phishing et compromission de compte

Playbook | Français · Modèle à adapter | v3.0 · 2026-10-16

Version du modèle : 3.0. Ce playbook est adapté à une PME pouvant externaliser informatique et surveillance. Le responsable interne décide du risque métier ; le prestataire technique réalise les actions relevant de ses accès. Une même personne peut cumuler des fonctions avec un suppléant identifié. La disponibilité des fournisseurs, du support et des moyens de récupération doit être vérifiée avant adoption.

Mode d'emploi. Les sections 1–6 donnent la séquence courte. Consulter les responsabilités et branches des sections 7–8 au triage, puis les contrôles applicatifs, de session et de levée des sections 10–12 avant les mesures correspondantes. La section 9 s'active dès qu'un paiement est concerné ; la section 13 fournit l'exemple. Les références détaillées précèdent leurs décisions : leur position après le résumé ne reporte pas la préparation après la clôture.

Type : procédure opérationnelle adaptable. Utilisez ce document pour un message suspect, une saisie d'identifiants sur un faux site, une validation MFA inattendue ou une activité de compte contestée. Une réception de message, un clic et une compromission confirmée correspondent à des situations différentes ; documentez ce qui est réellement établi.

Approbation et périmètre

Champ	Valeur à renseigner
Organisation, référence et version	[À RENSEIGNER : organisation, référence, version]
Propriétaire et approbateur	[À RENSEIGNER : sécurité, direction compétente]
Approbation et prochaine révision	[À RENSEIGNER : dates]
Services et populations couverts	[À RENSEIGNER : messagerie, applications, personnels, prestataires]
Incident et coordination	[À RENSEIGNER : référence, responsable, suppléant]
Signalement et contact indépendant	[À RENSEIGNER : canal, numéro vérifié]

Le SOC qualifie et conserve les références. Les équipes messagerie et identité interviennent dans leurs domaines. Le propriétaire applicatif contrôle ses sessions et autorisations. Le responsable métier évalue l'impact des restrictions. Le support accompagne la personne concernée en vérifiant son identité. Le responsable d'incident arbitre les actions ; les fonctions juridique et communication traitent les obligations et messages externes.

1. Recevoir sans aggraver

☐ Demander l'heure, le compte, le poste et les actions effectuées, sans reproche.

☐ Distinguer ouverture, clic, téléchargement, exécution, saisie de secret et validation MFA.

☐ Conserver le message original dans le canal prévu, avec en-têtes et identifiant.

☐ Ne pas faire suivre la pièce jointe à une liste de diffusion ordinaire.

☐ Ne pas demander mot de passe, cookie, token ou code MFA dans le ticket.

☐ Contacter l'utilisateur par un moyen vérifié distinct du compte suspect.

N'ouvrez pas les liens depuis un poste d'administration. L'analyse d'un fichier ou d'une URL doit suivre [À RENSEIGNER : procédure, environnement et autorisations]. Un service public d'analyse peut divulguer le contenu soumis : vérifiez les règles de partage avant tout envoi.

2. Qualifier l'exposition

Situation observée	Vérification proposée	Action à faire autoriser
Message reçu, interaction non établie	Distribution, destinataires, règle de détection	Retrait ciblé si malveillance confirmée
Identifiants saisis ou MFA approuvée	Connexions, méthodes enregistrées, sessions	Restriction du compte et récupération contrôlée
Fichier exécuté	État endpoint, processus, connexions	Confinement du terminal selon risque
Opération applicative contestée	Logs de l'application, cible, résultat	Mesure côté application et préservation

Ces lignes sont des orientations de triage, pas un automatisme. Adaptez l'urgence aux privilèges du compte, à la sensibilité des services et à l'activité en cours. Définissez les critères d'escalade dans [À RENSEIGNER : matrice de gravité]. Une connexion avec MFA satisfaite ne suffit pas à expliquer les actions ultérieures.

3. Conserver une chronologie utile

Rapprochez authentification, renouvellements, changements de sécurité et opérations applicatives. Gardez compte stable, application, résultat, fuseau, identifiants de diagnostic et pièces sources. Inscrivez les catégories de logs absentes ou expirées. N'attribuez pas une opération à une connexion précise si le lien de session n'est pas disponible.

Pour une messagerie, recherchez les règles, transferts, délégations, envois et suppressions inhabituels. Examinez les méthodes MFA, autorisations applicatives et rôles récemment modifiés. Ce sont notamment des vérifications proposées par Microsoft pour un compte de messagerie compromis ; transposez-les seulement aux services présents et aux droits d'investigation autorisés.

Pour une fraude au paiement, activez sans attendre le circuit interne finance et les contacts bancaires vérifiés. Ne reprenez pas les coordonnées indiquées dans le message suspect. Documentez les montants et transactions confirmés dans l'espace restreint prévu, sans diffuser inutilement les données personnelles.

4. Reprendre le contrôle et vérifier

☐ Faire autoriser la restriction du compte selon les conséquences métier.

☐ Réinitialiser les secrets compromis par un canal et un terminal maîtrisés.

☐ Révoquer les accès concernés côté identité et côté applications.

☐ Vérifier puis retirer les méthodes, délégations ou consentements non autorisés.

☐ Rechercher une compromission du terminal avant de lui confier de nouveaux secrets.

☐ Contrôler les actions après leur exécution, avec date et opérateur.

Un changement de mot de passe ne démontre pas la fin de toutes les sessions. Microsoft documente notamment la distinction entre tokens et cookies applicatifs, ainsi que de possibles délais de révocation. Faites vérifier chaque service par son responsable, au lieu de considérer le bouton de révocation comme une preuve universelle de confinement.

5. Réduire l'exposition collective

Recherchez les messages apparentés avec plusieurs critères : identifiants, expéditeur technique, contenu, URL et pièces. Validez les faux positifs avant retrait ou blocage étendu. Évitez de bloquer un service partagé légitime sur un seul indicateur peu spécifique. Consignez la portée et la durée des mesures, leur propriétaire et le retour arrière.

Informez les personnes exposées avec des consignes concrètes : signaler une interaction, ne pas approuver une sollicitation inattendue et utiliser le canal officiel. Les notifications externes dépendent des faits, contrats et obligations applicables ; le référent compétent détermine destinataires et délais.

6. Revenir au fonctionnement normal

☐ Confirmer l'identité de la personne avant réactivation ou nouvel enrôlement MFA.

☐ Vérifier droits attendus, récupération et absence de changements non autorisés connus.

☐ Faire valider le fonctionnement par l'utilisateur et le propriétaire applicatif.

☐ Définir une surveillance ciblée : [À RENSEIGNER : durée, événements, responsable].

☐ Documenter la conclusion, les incertitudes et les actions préventives.

☐ Tester le parcours avec un scénario fictif autorisé, sans collecte de secrets réels.

Limites : ce playbook ne démontre pas à lui seul une compromission, une exfiltration ou leur absence. Il doit être complété pour les comptes privilégiés, les identités non humaines et les terminaux critiques. Les procédures du fournisseur et les habilitations locales restent déterminantes.

Dossier de décision et contrôle de reprise

Une personne est nommée pour suivre chaque mesure, y compris lorsqu'un fournisseur doit intervenir. Le dossier ne doit pas se limiter à « mot de passe changé ». Il décrit les accès visés, les opérations confirmées, les mesures réalisées et les limites de vérification. Si l'application ne fournit pas de preuve exploitable, conserver cette limite et faire accepter le risque par l'autorité compétente.

Élément de reprise proposé	Valeur locale et preuve
Contrôle du compte et des moyens MFA	[À RENSEIGNER : vérification, opérateur, heure]
Contrôle des sessions et autorisations applicatives	[À RENSEIGNER : applications, effet observé, inconnues]
Contrôle du terminal et du canal de récupération	[À RENSEIGNER : périmètre testé, restrictions]
Réactivation et suivi	[À RENSEIGNER : décideur, validation métier, surveillance, fin]

Pour une campagne touchant plusieurs personnes, distinguer les destinataires exposés, les interactions déclarées et les comptes présentant des actions non autorisées confirmées. Cette distinction aide à choisir des mesures proportionnées sans promettre une attribution parfaite. Lors du retour d'expérience, revoir le parcours de signalement, la récupération et les points de contrôle manquants ; ne pas substituer une mise en cause de l'utilisateur à l'examen des protections.

7. Préparer les personnes, périmètres et contacts

La préparation recense messagerie, fournisseur d'identité, applications SaaS, terminaux distants et accès fournisseurs. Pour chaque service, identifier l'administrateur capable de restreindre un compte, exporter les traces et vérifier les sessions. Un MSSP peut détecter sans administrer ; le coordinateur interne doit connaître le prestataire qui peut agir. Les droits manquants, licences ou horaires limités restent visibles dans le plan.

Décision	Autorité interne proposée	Exécution et confirmation
Restreindre un compte ordinaire	Coordinateur selon délégation	Administrateur identité ; compte et services ciblés contrôlés
Bloquer une application ou délégation	Propriétaire métier avec sécurité	Administrateur habilité ; portée et dépendances vérifiées

Décision	Autorité interne proposée	Exécution et confirmation
Suspendre un paiement	Responsable finance autorisé	Finance et interlocuteur bancaire vérifié ; référence de demande
Réactiver et accepter une exception	Propriétaire métier ou direction	Prestataire ; critères satisfaits ou risque accepté

Le dossier initial contient le numéro interne, le compte stable, les services concernés et un contact indépendant. Si le support ou le fournisseur ne répond pas, utiliser le secours puis l'escalade contractuelle. Le coordinateur documente tentatives et conséquences ; il propose une protection ou une suspension métier disponible. Il ne prétend pas qu'une session est révoquée parce qu'un ticket a été ouvert.

Pour un compte privilégié ou partagé, identifier les activités dépendantes avant restriction. Pour une identité de fournisseur, contacter le sponsor interne et le responsable du contrat. Si l'activité concerne un dispositif de sûreté ou un système industriel, obtenir l'arbitrage adapté avant coupure. L'urgence ne donne aucun droit d'intervention sur un équipement personnel non couvert par les autorisations.

8. Choisir une branche de réponse et sa preuve

Entrée observée	Action proposée	Décision et preuve attendue
Message sans interaction établie	Préserver original, qualifier contenu et distribution	Retrait ciblé si justifié ; message et portée conservés
Identifiants saisis ou validation MFA inattendue	Vérifier compte, sessions, méthodes et applications	Restriction proportionnée ; effet contrôlé par service
Téléchargement ou exécution suspecte	Faire examiner le terminal et les connexions pertinentes	Isolement selon risque ; état et limites consignés
Demande de paiement ou modification bancaire	Activer finance par un contact connu	Suspension ou vérification indépendante ; décision tracée

Une branche n'exclut pas les autres. Un message peut conduire à une autorisation applicative sans fichier exécuté ; une fraude peut utiliser une adresse ressemblante sans compromettre votre compte. Documenter le chemin réellement observé. Si la personne ne sait plus ce qu'elle a fait, garder plusieurs hypothèses et rechercher des sources complémentaires, sans exiger qu'elle rejoue le clic ou fournisse un secret.

Le statut « compte compromis » doit reposer sur les éléments du dossier, pas uniquement sur la présence d'un message trompeur. Inversement, une authentification habituelle reconnue n'explique pas nécessairement une modification applicative contestée. Le coordinateur peut autoriser une mesure conservatoire sous incertitude en exposant le risque métier, le besoin de preuve et la condition de réexamen.

9. Examiner BEC, paiement et contexte métier

Le BEC désigne ici une fraude utilisant la messagerie ou l'usurpation d'un contexte professionnel. Le dossier recherche la demande initiale, les échanges, les changements de coordonnées, les validations et l'état réel du paiement. Conserver les références dans un espace restreint. Ne pas qualifier une facture d'illégitime sur son seul montant ni un correspondant de complice à partir d'une adresse affichée.

Finance utilise ses contacts bancaires connus pour demander les mesures disponibles selon l'état de la transaction. Conserver interlocuteur, heure, référence et résultat confirmé. Une demande de rappel n'est pas une garantie de récupération ; seule la réponse appropriée permet d'établir le résultat. Les autorités internes déterminent les démarches externes avec leurs conseils, selon les obligations applicables, sans délai légal universel fixé par ce modèle.

Fiche finance à dupliquer	Valeur à compléter
Transaction et état confirmé	[À RENSEIGNER : référence, montant, devise, état vérifié]
Validation métier	[À RENSEIGNER : valideur, canal indépendant, pièces]
Demande bancaire	[À RENSEIGNER : contact connu, heure, référence, mesure demandée]
Résultat et suivi	[À RENSEIGNER : confirmation, incertitude, propriétaire, prochaine décision]

Préserver les messages nécessaires avant une suppression collective lorsque l'urgence le permet. Un retrait de messagerie peut empêcher un utilisateur d'accéder au message ; la conservation de preuve doit donc être coordonnée avec l'équipe technique. Si la suppression passe d'abord, consigner ce qui a été perdu et quelles sources alternatives restent disponibles. Ne pas retarder une protection urgente uniquement pour produire un dossier parfait.

10. Vérifier applications, consentements et règles

Pour chaque application suspecte, conserver son identifiant, son propriétaire ou éditeur affiché, les autorisations accordées, le bénéficiaire et les événements disponibles. Faire valider par le propriétaire métier si l'application est attendue. Un nom rassurant ou une présentation soignée n'établit pas une autorisation ; une application inconnue de l'analyste n'est pas automatiquement malveillante.

Dans Microsoft Entra, la documentation distingue les permissions consenties par un administrateur et celles consenties par un utilisateur ; leur révocation peut nécessiter des interfaces différentes. L'exécutant doit donc identifier le type d'autorisation et suivre la procédure officielle correspondant à ses droits. Ce modèle ne fournit pas une commande de suppression globale. Pour les autres fournisseurs, vérifier leurs mécanismes propres.

Objet à examiner	Contrôle proposé	Sortie attendue
Consentement ou accès applicatif	Portée, bénéficiaire, historique et besoin métier	Maintien justifié ou retrait autorisé avec effet et limites
Règle de messagerie	Condition, destination, activation et création disponibles	Original préservé ; décision et état final vérifiés
Délégation ou rôle	Identité bénéficiaire, droits et sponsor	Autorisation retrouvée ou restriction proportionnée
Méthode de récupération ou MFA	Ajout, titulaire et validation indépendante	Moyen attendu confirmé ou récupération contrôlée

Ne limitez pas le contrôle aux règles visibles dans le client de messagerie. Le guide Microsoft sur les comptes compromis décrit des vérifications côté administration, notamment les règles et transferts. L'outil effectivement disponible et les permissions du prestataire déterminent la couverture. Faire préciser ce qui a été contrôlé, ce qui reste hors périmètre et qui doit compléter l'examen.

11. Confinement de session : distinguer demande et résultat

Le tableau de confinement sépare mot de passe, authentificateurs, tokens, sessions applicatives, autorisations et état du terminal. Pour chacun, noter l'action autorisée, l'exécutant et la preuve disponible. Microsoft documente que les cookies émis par une application dépendent de celle-ci : ne pas déduire leur fin du seul changement de mot de passe ou d'une action côté identité.

Mesure et cible	Exécutant	Vérification et échec
Restriction identité	[À RENSEIGNER : administrateur ou prestataire]	Contrôle adapté ; si non démontré, conserver restriction et escalader
Session applicative	[À RENSEIGNER : propriétaire du service]	Effet selon mécanisme fournisseur ; inconnue explicitée
Consentement ou délégation	[À RENSEIGNER : administrateur habilité]	État avant/après et dépendances ; retour arrière autorisé si erreur
Terminal suspect	[À RENSEIGNER : exploitant endpoint]	Périmètre examiné ; ne pas y remettre de nouveaux secrets sans décision

La réactivation exige un canal de récupération maîtrisé, des droits attendus vérifiés, le traitement des changements non autorisés identifiés et une surveillance attribuée. Si une application ne permet pas de vérifier une session, le décideur peut différer la reprise ou accepter une mesure compensatoire documentée. L'absence de nouvelle alerte ne remplace pas ce contrôle.

12. Faux positifs, exceptions et retrait des mesures

Un blocage peut affecter une activité autorisée. Pour le lever, retrouver le motif initial, demander une confirmation indépendante du besoin et vérifier que le risque visé est traité ou accepté. Le même propriétaire approuve la levée ou désigne explicitement un remplaçant. Conserver preuves, portée, heure et résultat ; ne pas effacer l'historique pour rendre le dossier plus simple.

Exception ou levée de mesure	Valeur à renseigner
Périmètre et besoin métier	[À RENSEIGNER : compte, service, opération indispensable]
Risque et compensation	[À RENSEIGNER : menace, restriction vérifiée, limite]
Autorité et décision	[À RENSEIGNER : nom, justification, date]
Fin et contrôle	[À RENSEIGNER : expiration, surveillance, déclencheur, propriétaire]

13. Exemple complet, intégralement fictif

Atelier-80 reçoit une fausse demande de changement bancaire dans un échange de commandes. À 10:10 UTC, une comptable signale avoir ouvert une page et accepté une application qu'elle pensait nécessaire. Le coordinateur ouvre EX-P1 et vérifie son identité par le numéro interne connu. Le prestataire administre la messagerie ; le MSSP ne reçoit que certaines alertes. Les horaires et résultats suivants sont fictifs.

Observation fictive	Pièce	Conclusion permise	Action et propriétaire
Demande de changement bancaire	EX-P-E1, message original	Demande reçue ; légitimité non établie	Finance vérifie le fournisseur par contact connu
Autorisation applicative trouvée	EX-P-E2, export administratif	Permission présente ; usage réel à examiner	Prestataire précise portée et retire après autorisation
Règle de transfert contestée	EX-P-E3, export et état	Modification confirmée ; auteur humain non attribué	Propriétaire messagerie contrôle et préserve
Paiement encore en validation	EX-P-E4, confirmation finance	État métier confirmé à cet instant	Finance suspend selon délégation et contacte banque si nécessaire

Le changement de mot de passe fictif est confirmé, mais le dossier ne marque pas les sessions applicatives comme closes. Le prestataire examine les mécanismes du service et conserve une limite sur une application externe. La direction décide une reprise partielle sans cette application, avec propriétaire et réexamen. Une règle métier légitime trouvée dans la recherche est conservée ; l'équipe ne supprime pas tout transfert indistinctement.

L'exercice est accepté si un remplaçant peut distinguer les preuves de réception, d'interaction et d'activité, retrouver les décisions finance et identifier les accès restant à vérifier. Il échoue si « MFA réussie » clôt le dossier, si une demande de révocation vaut preuve universelle ou si le besoin métier n'est jamais entendu. Chaque écart reçoit une correction et un contrôle de résultat.

Références de travail

Pour les permissions applicatives, consulter aussi Microsoft, examiner et révoquer les autorisations des applications. Les interfaces et droits nécessaires doivent être vérifiés au moment d'agir.

Microsoft : réponse à un compte de messagerie compromis ; Microsoft : révocation des accès ; NIST SP 800-61 révision 3. Ces références étayent le cadre ; les séquences et cases proposées sont à adapter, sans garantie de conformité.