

GUIDE

Réussir une simulation de phishing (sans punir)

Le pas-à-pas pour lancer une campagne de phishing éthique en interne : cadre légal, outil GoPhish, scénarios, mesure et débrief pédagogique — pour muscler les réflexes de vos équipes sans les stigmatiser.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~11 min Édition 2026 sedona-ai.com

Une simulation de phishing réussie ne se mesure pas au nombre de collaborateurs « piégés », mais à la progression de leurs réflexes et du taux de signalement. Ce tutoriel vous guide étape par étape : sécuriser le cadre légal (consultation du CSE, RGPD), établir une baseline, configurer l'outil GoPhish, concevoir des scénarios crédibles, mesurer les bonnes métriques et surtout débriefer sans stigmatiser. L'objectif est de sensibiliser, pas de punir : la sanction casse la confiance et fait chuter les signalements.

À retenir

- Le facteur humain reste central : 68 % des violations de données impliquent une erreur ou un piégeage par ingénierie sociale (Verizon DBIR 2024).
- Avant tout lancement, informez et consultez le CSE (art. L2312-38 du Code du travail) : l'oublier est un délit d'entrave passible de 7 500 € et rend les preuves irrecevables.
- Suivez deux métriques, pas une : le taux de clic ET le taux de signalement — c'est le signalement qui prouve la maturité de vos équipes.
- Établissez une baseline avant de lancer votre programme, puis répétez à intervalles réguliers en variant les scénarios.
- Formez au moment du clic (micro-learning contextuel), pas trois semaines plus tard : l'apprentissage est immédiat et déculpabilisant.
- L'approche « sans punir » est la bonne pratique pour un clic isolé, mais ne signifie pas une immunité absolue en cas de comportement gravement et volontairement fautif.

01 Pourquoi simuler le phishing

L'hameçonnage est aujourd'hui la porte d'entrée n°1 des cyberattaques. Une simulation contrôlée transforme une menace abstraite en réflexe concret : vos collaborateurs apprennent à reconnaître les signaux faibles et, surtout, à signaler. C'est l'un des rares dispositifs de cybersécurité qui progresse mois après mois si on le pilote bien.

68 %

des violations de données impliquent un facteur humain non malveillant (erreur ou piégeage par ingénierie sociale)

Verizon, 2024 Data Breach Investigations Report

1er rang

L'hameçonnage est la menace la plus signalée en 2025, avec environ un tiers des demandes d'assistance tous publics confondus

Cybermalveillance.gouv.fr, actualité hameçonnage 2025

02 Étape 0 — Sécuriser le cadre légal avant de lancer

Ne lancez rien avant d'avoir consulté le CSE

Un outil comme GoPhish trace qui ouvre, clique et soumet des données : c'est un dispositif de contrôle de l'activité des salariés. L'article L2312-38 du Code du travail impose d'informer et de consulter le CSE au préalable. À défaut, vous commettez un délit d'entrave et les preuves issues du dispositif deviennent irrecevables devant le juge.

7 500 €

amende encourue pour délit d'entrave en cas de défaut de consultation préalable du CSE

Code du travail, art. L2312-38 et L2317-1

- ☐ Informer et consulter le CSE en amont, et conserver la trace écrite
- ☐ Documenter le traitement de données (finalité = sensibilisation, pas surveillance), conformément au RGPD
- ☐ Appliquer la minimisation : ne collecter que le strict nécessaire, ne pas constituer de fichier disciplinaire
- ☐ Informer globalement les salariés de l'existence d'un programme de sensibilisation (sans annoncer les dates précises)
- ☐ Désigner un référent et prévoir un canal pour les questions

03 Étape 1 — Cadrer objectifs, périmètre et baseline

Une campagne sans point de départ mesurable ne prouve rien. Commencez par établir une baseline : un premier test qui donne votre taux de clic et de signalement initial. C'est votre référence pour mesurer les progrès.

1 Définir l'objectif

Sensibiliser et faire monter le taux de signalement, PAS piéger un maximum de monde ni identifier des « fautifs ».

2 Délimiter le périmètre

Choisir les groupes cibles (service, site, ou échantillon représentatif) et le volume pour ce premier tour.

3 Mesurer la baseline

Lancer une campagne neutre et calme, sans prévenir des dates, pour capturer le taux de clic et de signalement de départ.

4**Fixer une cible réaliste**

Par exemple : faire progresser le taux de signalement et faire baisser le taux de clic sur 2 à 3 campagnes trimestrielles.

04 Étape 2 — Installer et configurer GoPhish

GoPhish est le framework open source de référence pour la simulation : interface web et API REST, templates d'emails et pages d'atterrissage personnalisables, suivi en temps réel des ouvertures, clics, soumissions de données et signalements. Il n'est ni certifié ni endossé par l'ANSSI ou la CNIL — c'est un outil tiers, cité pour ses caractéristiques techniques.

1**Déployer l'instance**

Installer GoPhish sur un serveur maîtrisé (idéalement hébergé en UE), derrière HTTPS, et restreindre l'accès à l'admin.

2**Configurer l'envoi**

Paramétrer un profil d'envoi (SMTP) et un domaine dédié à la simulation, distinct de votre domaine de production.

3**Créer les groupes cibles**

Importer les destinataires par groupe, en cohérence avec le périmètre validé et le principe de minimisation.

4**Préparer template et landing page**

Rédiger l'email piégé et la page d'atterrissage qui déclenche immédiatement le message pédagogique (voir étape 4).

5**Tester en interne**

Envoyer la campagne à une boîte de test avant tout envoi réel, pour vérifier tracking, liens et rendu.

Ne collectez jamais de mots de passe réels

Une landing page de simulation ne doit jamais enregistrer d'identifiants saisis. Détectez la soumission du formulaire pour la mesurer, mais ne stockez pas les valeurs — c'est exigé par le principe de minimisation du RGPD.

05 Étape 3 — Concevoir des scénarios crédibles et proportionnés

Un bon scénario est plausible sans être cruel. Évitez les appâts qui jouent sur des sujets sensibles (prime individuelle, licenciement, santé) : ils piègent beaucoup mais détruisent la confiance. Variez les scénarios d'une campagne à l'autre pour éviter l'accoutumance.

Scénario	Signal à faire repérer	Niveau
Fausse notification RH / note de frais	Domaine expéditeur légèrement altéré, urgence artificielle	Facile
Faux message d'un outil interne (partage de fichier)	Lien qui ne pointe pas vers le domaine officiel	Moyen
Fausse alerte sécurité « réinitialisez votre mot de passe »	Demande d'identifiants, ton pressant	Moyen
Email d'un « fournisseur » avec pièce jointe	Expéditeur inconnu, pièce jointe inattendue	Avancé

06 Étape 4 — Lancer, tracer et mesurer les bonnes métriques

L'erreur classique est de ne regarder que le taux de clic. La métrique qui compte vraiment, c'est le taux de signalement : un collaborateur qui clique puis signale a compris la démarche. Suivez les deux ensemble.

20 %

des collaborateurs identifient et signalent l'email piégé lors d'une simulation ; parmi ceux ayant cliqué, 11 % le signalent quand même ensuite

Verizon, 2024 Data Breach Investigations Report

Métrique	Ce qu'elle mesure	À valoriser
Taux d'ouverture	Portée de l'appât	Contexte
Taux de clic	Exposition au risque	À faire baisser
Taux de soumission	Cas les plus critiques	À faire tendre vers zéro
Taux de signalement	Maturité et bon réflexe	À faire monter — priorité n°1

07 Étape 5 — Débriefing sans stigmatiser

C'est le moment décisif. La sanction ou l'humiliation publique fait chuter les signalements futurs : les gens préfèrent se cacher plutôt que d'alerter. Formez au moment du clic (micro-learning contextuel) et communiquez sur des chiffres agrégés, jamais nominatifs.

1

Formation immédiate

Au clic, la page affiche aussitôt un message pédagogique : « ceci était une simulation », les 3 signaux qui auraient dû alerter, et le bon réflexe.

2

Communication agrégée

Partager les résultats par groupe, jamais par individu. Célébrer la progression du taux de signalement.

3 Renforcement positif

Remercier publiquement (de façon anonyme) ceux qui ont signalé : le signalement est le comportement à ancrer.

4 Boucle d'amélioration

Répéter chaque trimestre en variant les scénarios, et comparer à la baseline.

« Sans punir » ne veut pas dire « immunité absolue »

La CNIL positionne la simulation comme un outil de sensibilisation, pas un dispositif disciplinaire : un clic isolé d'un collaborateur non formé ne justifie généralement pas de sanction. En revanche, un comportement gravement et délibérément fautif, ou répété malgré des formations, relève du régime disciplinaire de droit commun. La règle d'or reste la proportionnalité et la pédagogie d'abord.

08 Étape 6 — Ancrer le programme dans la durée

Une campagne unique ne change rien durablement. L'ANSSI recommande, dans son Guide d'hygiène informatique, de sensibiliser régulièrement et d'organiser des exercices de simulation pour tester les réflexes — la grande majorité des incidents traités par le CERT-FR auraient pu être évités par ces mesures de base.

- Répéter les campagnes à intervalles réguliers (par exemple trimestriels)
- Varier les scénarios et les niveaux de difficulté pour éviter l'accoutumance
- Suivre l'évolution du taux de signalement dans le temps, plus que le taux de clic
- Intégrer la simulation à un dispositif plus large : hygiène des mots de passe, MFA, procédure de signalement claire
- Réévaluer régulièrement votre surface d'exposition externe, car un email piégé exploite souvent une information publiquement accessible

§ Sources

1. Cybermalveillance.gouv.fr — L'hameçonnage (« phishing ») en 2025 : une menace omniprésente — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/hameconnage-phishing-ra26>
2. Cybermalveillance.gouv.fr — Rapport d'activité 2025 — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2025>
3. Verizon — 2024 Data Breach Investigations Report (communiqué officiel) — <https://www.verizon.com/about/news/2024-data-breach-investigations-report-vulnerability-exploitation-boom>
4. Code du travail numérique — Article L2312-38 (consultation du CSE, dispositifs de contrôle) — <https://code.travail.gouv.fr/code-du-travail/l2312-38>
5. CNIL — Sécurité : impliquer et former les utilisateurs — <https://www.cnil.fr/fr/securite-impliquer-et-former-les-utilisateurs>
6. CNIL — Phishing, hameçonnage : détecter un message malveillant — <https://www.cnil.fr/fr/phishing-detecter-un-message-malveillant>
7. ANSSI (cyber.gouv.fr) — Guide d'hygiène informatique (42 mesures) — <https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>
8. GoPhish — dépôt officiel GitHub (Open-Source Phishing Toolkit) — <https://github.com/gophish/gophish>

Vous voulez lancer une simulation sans risque juridique ni faux pas ?

Sedona propose une simulation de phishing : envoi de faux e-mails de test à vos équipes, sur un périmètre défini, après information de votre CSE, suivi d'un débrief collectif — on sensibilise, on ne sanctionne personne. Rapport anonymisé des taux de clic et de signalement. À partir de 1 900 € HT.

Demander une simulation de phishing

sedona-ai.com/contact?service=phishing