knowbe4

2026 Mois de sensibilisation à la cybersécurité

Dossier stratégique de ressources

SEMAINE 1
SEMAINE 2
SEMAINE 3
SEMAINE 4

BRIEFING DE MISSION :

Mois de sensibilisation à la cybersécurité 2026

Votre mission, si vous l'acceptez : armer votre équipe avec les renseignements tactiques nécessaires pour garder une longueur d'avance sur les menaces mondiales.

Intégrez la « Workforce Risk Division » (WRD), la division des risques liés au personnel, une unité d'élite, et exploitez pleinement la panoplie d'outils, d'équipements et de spécialistes de la cybersécurité mise à votre disposition cette année. Au sein de la WRD, vous aiderez vos utilisateurs à se lancer dans quatre missions d'une semaine, chacune ciblant une cybermenace spécifique.

Transformer vos collaborateurs en une force de défense de première ligne devient un véritable jeu d'enfant. Nous avons fait le plus dur pour vous grâce à une collection gratuite de ressources.

Cette campagne clé en main pour le mois de sensibilisation à la cybersécurité propulse vos employés dans la peau d'« agents secrets » en guerre contre le cybercrime. En plus des modules de formation gratuits, des affiches et des documents d'accompagnement, nous avons inclus quatre cartes de personnages « Spécialistes » qui incarnent les compétences indispensables pour évoluer dans le paysage des menaces actuel. Vous trouverez également quatre scénarios de jeux de rôle pré-configurés, conçus pour être menés en présentiel ou en distanciel, afin d'aider votre équipe à forger sa résilience face aux menaces à venir.

Votre équipement

Notre page web dédiée vous donne accès aux éléments suivants :

FOR YOUR EYES ONLY

Confidentiel

- **Webinaire :** Comment sécuriser l'adoption de l'IA dans votre organisation
- **Livre blanc :** Sécuriser la main-d'œuvre hybride : protéger les humains et les agents d'IA dans une nouvelle ère
- **Quatre documents de scénarios de jeux de rôle thématiques**
- **Planificateur web hebdomadaire de sensibilisation à la sécurité**, qui organise l'ensemble des ressources destinées aux utilisateurs en thématiques hebdomadaires pour tout le mois d'octobre :

PLANIFICATEUR HEBDOMADAIRE

Pour vos agents

Accès à l'intégralité des formations et contenus via les liens fournis jusqu'au **31 octobre 2026.**

- **Six modules de formation interactive ou vidéo gratuits**
  - La folie du hameçonnage par SMS (disponible dans 35 langues)
  - Ingénierie sociale : l'offensive des deepfakes (disponible dans 35 langues)
  - Protection de la propriété intellectuelle (disponible dans 12 langues)
  - Mots de passe robustes, comptes sécurisés (disponible dans 35 langues)
  - Audiocast : adoptez des réflexes anti-piratage (disponible dans 12 langues)
  - Jeu : en quête de confidentialité (disponible dans 13 langues)
- **Quatre cartes/affiches de personnages « Spécialistes » de la Workforce Risk Division**
- **Quatre affiches et des visuels dynamiques, idéaux pour rappeler les concepts clés**

Workforce Risk Division 101

Pour les agents du WRD, la lutte incessante contre les personnes malintentionnées est déjà un défi de taille. Nous avons donc tout fait pour que le recrutement de nouveaux collaborateurs soit aussi simple que possible. Pour commencer, chaque contenu est articulé autour d'un thème central sur lequel se concentrer durant chacune des quatre semaines complètes d'octobre. Chaque semaine, pensez à partager un ou plusieurs de ces types de contenu :

- **Module de formation vidéo ou interactif**
- **Affiche/Document d'information**
- **Carte de personnage Spécialiste WRD**
- **Document de scénarios de jeu de rôle**

Nous détaillerons chaque thématique hebdomadaire plus loin dans ce dossier.
Voici toutefois un récapitulatif :

- **Semaine 1 :** Hameçonnage et ingénierie sociale
- **Semaine 2 :** Sécurité de l'IA et deepfakes
- **Semaine 3 :** Sécurité des données et mots de passe
- **Semaine 4 :** Signalement des incidents

Pour visualiser la structure globale de l'opération, consultez notre planificateur de sensibilisation à la sécurité, disponible ici :

PLANIFICATEUR HEBDOMADAIRE

Utilisez ce planificateur comme point d'accès unique à l'ensemble des ressources de la WRD mises à votre disposition.

Profils des spécialistes de la WRD

Les missions sont fixées. Il est maintenant temps de rencontrer les spécialistes. Servez-vous de ces quatre profils de spécialistes pour présenter à vos utilisateurs les quatre ensembles de compétences dont ils auront besoin pour les cyber-opérations tout au long du mois de sensibilisation à la cybersécurité. Chacun d'eux apporte sa contribution aux exigences nécessaires pour mener à bien les missions du mois. Le reste dépend de vos utilisateurs.

HAMEÇONNAGE/INGÉNIERIE SOCIALE

MIRAGE

DEVISE :

LA CONFIANCE EST
UN LUXE
LA VÉRIFICATION
UNE NÉCESSITÉ

RÔLE : SPÉCIALISTE EN CONTRE-ESPIONNAGE

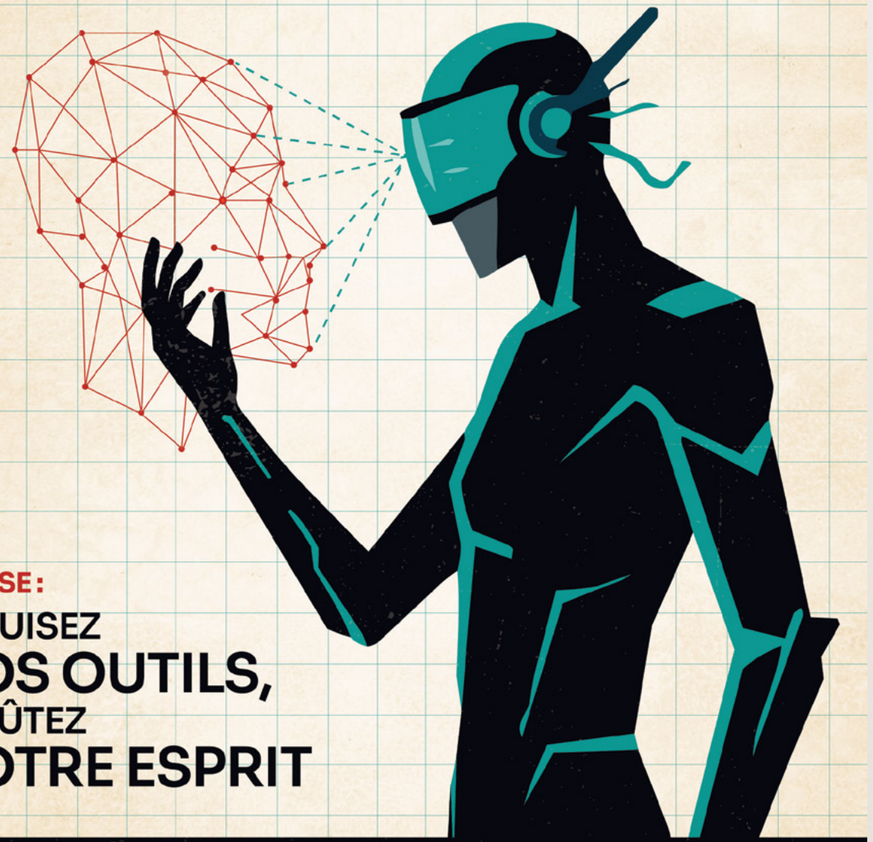
SPÉCIALITÉ : DÉTECTION DU PRÉTEXTE ET DE L'INGÉNIERIE SOCIALE SOPHISTIQUÉE

CONSEIL : SI UN E-MAIL JOUE SUR UN FAUX SENTIMENT D'URGENCE, C'EST PROBABLEMENT UN PIÈGE

PAGE

SÉCURITÉ/MENACES LIÉES À L'IA

SENTINELLE



DEVISE :

AIGUISEZ
VOS OUTILS,
AFFÛTEZ
VOTRE ESPRIT

RÔLE : EXPERT TECHNIQUE

SPÉCIALITÉ : SÉCURITÉ DE L'IA ET DÉTECTION DE DEEPFAKES

CONSEIL : CONVENEZ D'UN MOT DE PASSE AVEC VOTRE FAMILLE OU VOS COLLÈGUES POUR VÉRIFIER LEUR IDENTITÉ LORS D'APPELS SUSPECTS SE PRÉTENDANT « URGENTS »

PAGE

SÉCURITÉ DES DONNÉES ET MOTS DE PASSE

SÉSAME

DEVISE :

[CLASSIFIÉ]

RÔLE : CRYPTOGRAPHE

SPÉCIALITÉ : CLÉS D'ACCÈS, MFA ET CHIFFREMENT

CONSEIL : VOTRE MOT DE PASSE NE DEVRAIT PAS ÊTRE UN MOT, MAIS UNE HISTOIRE QUE VOUS SEUL CONNAISSEZ

SIGNALEMENT DES INCIDENTS

SIGNAL

DEVISE :

FUITE DE DONNÉES REPÉRÉE : FUITE DE DONNÉES SIGNALÉE.

RÔLE : AGENT DE TERRAIN

SPÉCIALITÉ : SIGNALEMENT DES INCIDENTS ET SÉCURITÉ PHYSIQUE

CONSEIL : VOUS REMARQUEZ QUELQUE CHOSE D'ANORMAL ? SIGNALEZ-LE

Rassembler tous vos collaborateurs

Nous avons élaboré quatre plans de formation complets pour guider votre équipe lors de jeux de rôle simulant des crises de sécurité.

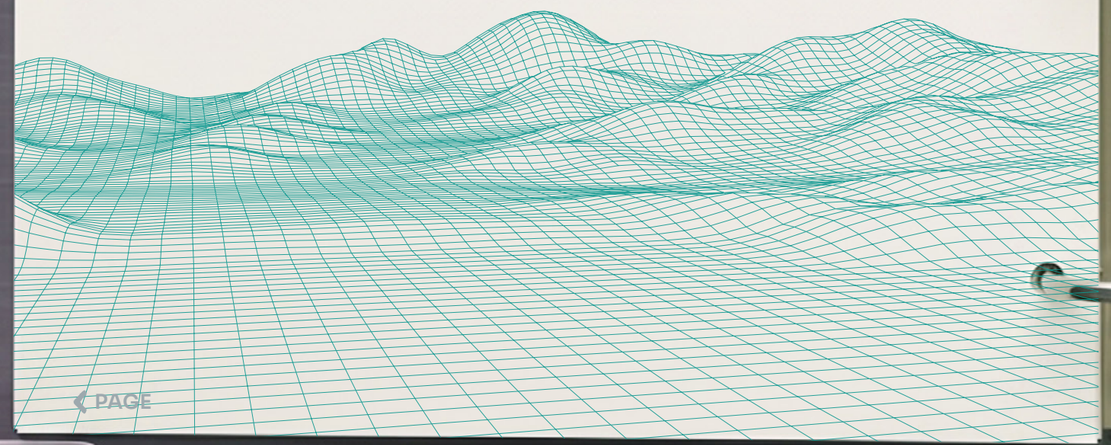
L'objectif est d'intégrer tous les utilisateurs quel que soit leur niveau technique, en mettant l'accent sur l'identification des rôles, la prise de décision et la coordination d'équipe. Les activités incluent la priorisation de listes de contrôle d'intervention et la réalisation de simulations de scénarios réalistes avec des imprévus. Grâce à des exercices pratiques et des séances de débriefing structurées, vos collaborateurs découvriront les procédures de réaction aux incidents établies, la communication interservices et l'adaptabilité face aux incidents de sécurité.

Voici quelques suggestions prêtes à l'emploi pour tirer le meilleur parti de ces ressources :

1. Mission clé en main pour les responsables :
Partagez ces ressources avec les chefs de service accompagnées du *briefing de la Direction*. Suggérez-leur de choisir le sujet le plus pertinent pour leur département et de mener une session de *réponse rapide*.

2. Opération Télétravail sous pression :
Avec une majorité des collaborateurs en distanciel, utilisez les sections *Fiche scénario* des ressources de jeu de rôle pour soumettre des sondages lors des visioconférences mensuelles d'octobre sous forme de tests. Débriefez les résultats de la semaine précédente lors de la réunion suivante pour voir comment vos collaborateurs s'en sont sortis.

3. L'*aventure dont vous êtes le héros* via la messagerie instantanée :
Choisissez un jour de la semaine pour partager une *fiche scénario* dans votre canal dédié à l'infosec et à la sensibilisation à la sécurité sur l'application de messagerie interne de votre choix. Le premier agent à « signaler l'incident » correctement, en expliquant en quoi il s'agit d'un problème et quelles mesures pourraient être prises, pourra remporter un prix thématique ou toute autre récompense autorisée par votre organisation.



Conseil des experts de la WRD : Stratégies de campagne

L'équipe de scientifiques et de chercheurs travaillant dans l'ombre au service du WRD ne sort peut-être pas beaucoup, mais elle maîtrise son sujet. Les cerveaux derrière ces ressources ont constaté que les stratégies de campagne suivantes fonctionnent pour les organisations de toutes tailles :

Pensez comme un officier traitant, déployez comme un agent de terrain
Votre objectif est de modifier les comportements à risque, et non de vous contenter de transmettre des informations. Inspirez-vous de la manière dont les meilleurs services de renseignement élaborent des récits de couverture élaborée : ils multiplient les angles d'approche pour renforcer une vérité unique. C'est pourquoi nous avons autorisé suffisamment de ressources pour adopter une approche en immersion totale. En déployant différents médias (vidéos, jeux et briefings) tout au long de la semaine, vous conditionnez leurs réflexes de sécurité par une interaction régulière. C'est ainsi que vous transformerez des employés passifs en dernière ligne de défense aguerrie.

Recrutez vos alliés sur tous les fronts
Aucune opération de renseignement ne se gagne de manière isolée. Pour bâtir une culture de la sécurité vraiment robuste, vous devez aller chercher vos alliés bien au-delà du secteur informatique. Profitez du mois d'octobre pour activer vos « agents dormants » chez les RH et dans les services juridique et marketing. Faites-leur comprendre qu'ils ont un rôle crucial à jouer dans la WRD. Quand le message de sécurité ne vient plus du « technicien informatique », mais d'un collègue de confiance au sein de leur propre équipe, il est bien plus probable qu'il soit réellement entendu et appliqué.

Priorisez les renseignements essentiels
Ne grillez pas vos agents en les submergeant d'informations critiques à la mission. Si vous les inondez de données, ils finiront par expédier les briefings par simple automatisme, juste pour vider leur boîte de réception. Identifiez plutôt les deux ou trois failles les plus dangereuses au sein de votre organisation et concentrez vos actions dessus. Nos thématiques hebdomadaires, à savoir le hameçonnage, la sécurité liée à l'IA, les mots de passe et les signalements, sont calibrées pour forger des agents aguerris. Restez concentré sur la mission en cours, sécurisez l'objectif et gardez les renseignements détaillés pour les opérations futures.

Bien que les ressources de ce kit ne remplacent en rien un programme complet de formation sur la sensibilisation à la sécurité, elles sont conçues pour être diffusées facilement et déployées là où elles auront le plus d'impact auprès de vos équipes.

Feuille de route mission par mission

Vous trouverez ci-dessous le contenu détaillé semaine par semaine, avec des suggestions de sujets à mettre en avant ainsi que les modèles d'e-mails associés.

À ce stade, vous avez probablement déjà des idées ou des stratégies en tête pour aborder ce mois. Quelle que soit la manière dont vous structurez votre campagne, nous vous suggérons d'envoyer un e-mail de présentation le 1er octobre, ou même durant la dernière semaine de septembre.

Voici un exemple de communication :

Objet suggéré :
[DÉBUT DE MISSION] **Votre intégration au sein de la Workforce Risk Division**

MOIS DE SENSIBILISATION À LA CYBERSÉCURITÉ 2026 | **LANCEMENT DE LA MISSION**

knowbe4

Workforce Risk Division : briefing d'initiation

Chers agents,

Dans la guerre de l'ombre qui se joue sur le terrain du cyber-espionnage mondial, vous êtes à la fois la cible principale et notre rempart le plus solide.

Seuls les agents les plus vigilants et les mieux formés peuvent résister à la vague de deepfakes générés par IA, à l'ingénierie sociale sophistiquée et à la cyberguerre de l'ombre qui guette chaque recoin de notre réseau.

Le terrain est dangereux, et vous ne devez pas opérer de manière isolée. Heureusement, nous avons autorisé une série de sessions de renseignement permettant de nous assurer que vous serez prêts pour la mission à venir.

LA MISSION :

En octobre prochain, nous marquons le mois de sensibilisation à la cybersécurité en intégrant chaque membre de notre équipe au sein de la Workforce Risk Division (WRD). Tout au long du mois, vous serez briefés par quatre spécialistes, chacun représentant un pilier essentiel de notre culture de la sécurité.

Préparez-vous à un déploiement de quatre semaines où chaque mission représente un nouveau niveau de renseignement à maîtriser.

Gardez l'esprit vif ce mois-ci pour **[Insérez ici les activités ou thèmes prévus. Utilisez les idées de ce guide de l'utilisateur pour vous inspirer.]**

Si vous avez des questions, contactez **[insérez le nom de la personne à contacter]**.

Votre premier briefing tombe lundi. Tenez-vous prêts, agents, et bonne chance.

SEMAINE 1

Hameçonnage et ingénierie sociale

Les espions les plus aguerris ne s'introduisent jamais par effraction. On les laisse entrer par la grande porte. Cette semaine se concentre sur les signaux d'alarme subtils de l'ingénierie sociale que les filtres techniques pourraient manquer, et sur la manière de les repérer.

Voici un résumé des ressources pour cette semaine :

Module de formation - La folie du hameçonnage par SMS

Ce module de sept minutes présente les dangers du hameçonnage par SMS et montre comment vos utilisateurs peuvent éviter de devenir une nouvelle victime de ce type de cyberattaque.

Vos employés découvriront :

- **Comment les cybercriminels peuvent utiliser l'ingénierie sociale via les SMS**
- **À quoi ressemble l'hameçonnage par SMS**

ACCÉDER À LA RESSOURCE

Ressource pour scénario de jeu de rôle - Démasquer les attaques d'hameçonnage et de whaling

Ce scénario de jeu de rôle prépare vos collaborateurs à repérer et à déjouer les tentatives d'hameçonnage et de whaling sophistiquées. Les participants passeront au crible un e-mail simulant une fraude au président, apprenant ainsi à repérer les faux indicateurs de confiance générés par l'IA et les véritables signaux d'alerte comportementaux. Conçu pour tous les niveaux, cet exercice est une mise en situation idéale pour aiguiser l'esprit critique de vos collaborateurs et ancrer les procédures officielles de l'organisation.

Deux ressources téléchargeables

- **Ne mordez pas à l'hameçon : signalez toute tentative d'hameçonnage -** Une affiche mémo des signes courants d'un e-mail d'hameçonnage et la marche à suivre si vous suspectez une tentative d'hameçonnage
- **Votre rôle dans la sécurité sur Internet :** ressource de type infographie rappelant aux utilisateurs les tactiques de cybercriminalité les plus courantes et comment les éviter

RESSOURCES DE LA SEMAINE 1

Partage du contenu

Voici un exemple d'e-mail du spécialiste Mirage à utiliser pour diffuser le module de formation de la semaine :

Objet suggéré :
[MISSION DE LA SEMAINE 1] **Neutraliser la menace du « hameçonnage par SMS »**

knowbe4

Neutraliser la menace du « hameçonnage par SMS »

MOIS DE SENSIBILISATION À LA CYBERSÉCURITÉ 2026 | **MISSION SEMAINE 1**

Chers agents,

Ici votre spécialiste, nom de code **Mirage**.

Nos appareils mobiles sont désormais les cibles prioritaires des ingérences extérieures. L'ennemi a étendu son champ d'action : de votre boîte de réception, il est passé à votre poche.

LA MISSION :

Terminez le briefing « Frénésie du hameçonnage par SMS ». Ce module de formation présente les dangers du hameçonnage par SMS et montre comment éviter de devenir une nouvelle victime de ce type de cyberattaque.

Vous allez découvrir :

- **Comment les cybercriminels peuvent utiliser l'ingénierie sociale via les SMS**
- **À quoi ressemble le hameçonnage par SMS**

Votre accès (https://training.knowbe4.com/modstore/view/af44ce18-ea58-47c9-a352-fb1f277ec903)

Si vous avez des questions, envoyez une transmission à **[insérez le nom de la personne à contacter]**.

Soyez prudents. Surveillez les prochains briefings ce mois-ci.

Mirage, fin de transmission.

PAGE

SEMAINE 2

IA et deepfakes

Explorez la face sombre de l'IA pour apprendre aux utilisateurs comment les personnes malintentionnées exploitent les outils génératifs afin de créer des clones et des scripts parfaits. Vos agents doivent s'appuyer sur leur atout le plus précieux, leur esprit critique, pour vérifier ce qui est réel.

Voici un résumé des ressources pour cette semaine :

Module vidéo - Une attaque d'ingénierie sociale par deepfake

Ce module vidéo de six minutes met en scène des acteurs de la célèbre série de sensibilisation à la sécurité « The Inside Man » pour démontrer comment les cybercriminels utilisent le clonage vocal par IA et la technologie du deepfake vidéo afin d'usurper l'identité de personnes que vous pourriez connaître.

Vos employés découvriront :

- **Comment les cybercriminels peuvent utiliser les deepfakes et l'ingénierie sociale pour compromettre les défenses d'une organisation par le biais de demandes simples**
- **Les signaux d'alarme à surveiller pour vous protéger, vous et votre organisation, contre les attaques sophistiquées par deepfake**

ACCÉDER À LA RESSOURCE

Module de formation - Protection de la propriété intellectuelle

Ce module de formation de 10 minutes, disponible dans la bibliothèque KnowBe4 Compliance Plus, explique l'importance de la propriété intellectuelle.

Vos employés découvriront :

- **Ce qu'est la propriété intellectuelle et pourquoi elle est si précieuse**
- **Comment protéger la propriété intellectuelle contre le vol, l'utilisation abusive et l'exposition accidentelle, y compris dans le cadre d'une utilisation par l'intelligence artificielle**

ACCÉDER À LA RESSOURCE

Ressource pour scénario de jeu de rôle - Le défi des prompts IA

Ce scénario de jeu de rôle permet aux employés d'identifier les risques liés à l'utilisation de prompts non sécurisés au travail. Les participants analyseront des prompts IA pour déterminer lesquels sont sûrs et lesquels exposent des données privées. Conçu pour tous les niveaux, cet exercice permet d'aiguiser l'esprit critique et de respecter les politiques de l'organisation.

PAGE

Deux ressources/visuels dynamiques téléchargeables

- **Vrai ou faux ? Repérer les deepfakes –** Affiche mémo sur l'utilisation des indices contextuels et de l'esprit critique pour identifier les deepfakes auxquels vous pourriez être confrontés
- **L'hameçonnage devient plus intelligent : comment l'IA transforme les escroqueries en ligne –** Ressource de type infographie expliquant comment l'IA rend les tentatives d'hameçonnage plus difficiles à détecter

RESSOURCES DE LA SEMAINE 2

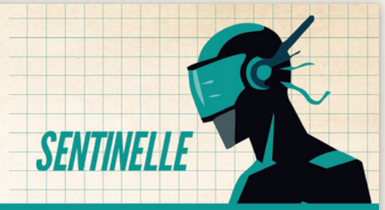
Partage du contenu

Voici un exemple d'e-mail du spécialiste Sentinelle à utiliser pour diffuser notre ressource phare de la semaine : le module « Une attaque d'ingénierie sociale par deepfake ».

Objet suggéré :
[MISSION DE LA SEMAINE 2] **Démasquer les deepfakes**

knowbe4

Démasquer
les deepfakes



MOIS DE SENSIBILISATION À LA CYBERSÉCURITÉ 2026 | **MISSION SEMAINE 2**

Chers agents,

Ici le spécialiste **Sentinelle** .

Ça m'agace de voir les avancées de l'IA détournées à des fins malveillantes. Les personnes malintentionnées utilisent les dernières innovations en matière de clonage vocal par IA et de deepfakes vidéo pour usurper l'identité de membres de la direction et de vos collègues. Toute personne qu'ils parviennent à dupliquer pour obtenir l'accès et les données nécessaires à la réalisation de leurs propres missions malveillantes est une cible légitime.

LA MISSION :

Terminez le briefing vidéo *Une attaque d'ingénierie sociale à l'ère du deepfake*. Ce module présente des renseignements essentiels fournis par les experts de la série « The Inside Man », démontrant comment les cybercriminels utilisent le clonage vocal par IA et la technologie du deepfake vidéo pour usurper l'identité de personnes que vous pourriez connaître.

Vous allez découvrir :

- **Comment les cybercriminels peuvent utiliser les deepfakes et l'ingénierie sociale pour compromettre les défenses d'une organisation par le biais de demandes simples**
- **Les signaux d'alarme à surveiller pour vous protéger, vous et votre organisation, contre les attaques sophistiquées par deepfake**

Votre accès (https://training.knowbe4.com/modstore/view/0451be1f-0531-4724-a664-21f109be6308)

Si vous avez des questions, contactez **[insérez le nom de la personne à contacter]**.

Aiguisez vos outils, affûtez votre esprit. Surveillez les prochains briefings ce mois-ci.

Sentinelle, fin de transmission.

SEMAINE 3

Sécurité des données et mots de passe

Les données sensibles sont la monnaie du monde moderne, et les personnes malintentionnées sont prêtes à tout pour les obtenir. Assurez-vous que vos agents connaissent la valeur de ce qu'ils protègent et les enjeux en cas de fuite. Cette semaine, l'accent est mis sur l'utilisation des gestionnaires de mots de passe et de la MFA pour garantir que, même si un agent est compromis, les données de l'agence restent chiffrées.

Voici un résumé des ressources pour cette semaine :

Module de formation destiné aux utilisateurs d'appareils mobiles - Mots de passe robustes, comptes sécurisés

Ce module de cinq minutes, conçu pour une utilisation sur appareils mobiles, détaille l'importance des mots de passe et des phrases secrètes sécurisés dans la vie professionnelle et personnelle de vos utilisateurs.

Vos employés découvriront :

- **Des conseils pour créer des mots de passe robustes et sécurisés, et utiliser efficacement les phrases secrètes**
- **Comment éviter les erreurs de sécurité courantes qui rendent les comptes vulnérables**
- **Les bonnes pratiques pour sécuriser les mots de passe et les phrases secrètes**

ACCÉDER À LA RESSOURCE

Ressource pour scénario de jeu de rôle - Deviner le mot de passe

Ce scénario de jeu de rôle propose aux employés de se mettre dans la peau d'un pirate pour faire l'expérience du craquage de mots de passe faibles. Les participants examineront des publications sur les réseaux sociaux et tenteront de deviner les mots de passe de leurs propriétaires en se basant uniquement sur les informations partagées en ligne. Cet exercice démontre comment la combinaison d'un partage excessif d'informations en ligne et de mauvaises pratiques en matière de mots de passe permet aux personnes malintentionnées d'accéder plus facilement aux comptes par force brute.

Deux ressources/visuels dynamiques téléchargeables

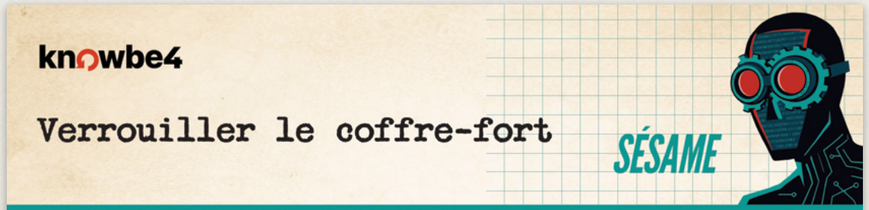
- **Des mots de passe robustes pour assurer votre tranquillité en ligne –** Ressource de type affiche mettant l'accent sur l'importance des mots de passe robustes
- **Données sensibles : sous scellés et hors de portée –** Document de type infographie expliquant les bases de la sécurisation des informations sensibles et les raisons de le faire

RESSOURCES DE LA SEMAINE 3

Partage du contenu

Voici un exemple d'e-mail *du* spécialiste Sésame à utiliser pour diffuser le module de formation de la semaine :

Objet suggéré :
[MISSION DE LA SEMAINE 3] **Verrouiller le coffre-fort**



Chers agents,

Ici le spécialiste **Sésame** en liaison depuis… un lieu tenu secret défense.

Un secret ne vaut que par la solidité de sa serrure. Nous revenons aux fondamentaux concernant les protocoles de mots de passe. Ce qui peut sembler être des informations basiques n'en diminue pas pour autant leur importance. Nos coffres les plus sophistiqués sont inutiles s'ils sont laissés ouverts.

LA MISSION :

Terminez le module de formation destiné aux utilisateurs d'appareils mobiles « Des mots de passe robustes, comptes sécurisés ». Découvrez pourquoi les phrases secrètes sont supérieures aux mots de passe et comment éliminer les erreurs courantes qui exposent notre périmètre.

Vous allez découvrir :

- **Des conseils pour créer des mots de passe robustes et sécurisés, et utiliser efficacement les phrases secrètes**
- **Comment éviter les erreurs de sécurité courantes qui rendent les comptes vulnérables**
- **Les bonnes pratiques pour sécuriser les mots de passe et les phrases secrètes**

Votre accès (https://training.knowbe4.com/modstore/view/c0ee0966-ff3a-4fc2-93bb-2a632811140b)

Si vous avez des questions, envoyez une communication chiffrée à **[insérez le nom de la personne à contacter]**.

Je conclurai en évoquant une phrase de mon magicien préféré : gardez-les secrets. gardez-le en sécurité.

S

SEMAINE 4

Signalement des incidents

Au sein de la Workforce Risk Division, rester à l'affût est un élément vital de toute opération. Aucun agent ne peut mener une mission à bien tout seul. Il est donc crucial que vos agents comprennent l'importance d'informer l'équipe lorsque quelque chose semble anormal. Cette semaine, nous nous assurons que chaque agent sache exactement comment demander des renforts lorsqu'il détecte un comportement suspect.

Voici un résumé des ressources pour cette semaine :

Audiocast – Adoptez des réflexes anti-piratage : signalements

Cet audiocast de 15 minutes, divisé en modules de cinq et dix minutes, aborde l'importance du signalement des menaces de sécurité.

Vos employés découvriront :

- **Les obstacles potentiels au signalement qui peuvent survenir face à une menace de sécurité**
- **Pourquoi le signalement est une étape si cruciale dans la lutte contre la cybercriminalité**
- **Un processus décisionnel qu'ils peuvent utiliser pour analyser les situations et prendre les mesures de sécurité adaptées**

ACCÉDER À LA PARTIE 1

ACCÉDER À LA PARTIE 2

Jeu : en quête de confidentialité

Ce jeu interactif de 15 minutes permettra à vos utilisateurs de mieux comprendre les lois internationales sur la confidentialité des données grâce à une aventure captivante autour du monde qui affinera leurs connaissances en matière de conformité.

Vos employés découvriront :

- **L'importance des réglementations sur la confidentialité des données**
- **Les différentes approches régionales et internationales en matière de confidentialité des données**

ACCÉDER À LA RESSOURCE

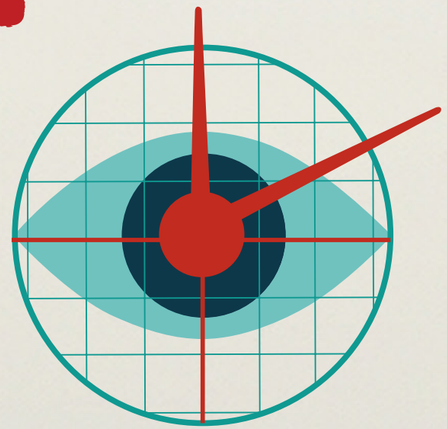
Ressource pour scénario de jeu de rôle - Réaction aux incidents

Ce plan de formation complet sur la réaction aux incidents guide les employés de l'entreprise à travers des jeux de rôle simulant des incidents de sécurité. Cet exercice est accessible à tous, quel que soit le niveau technique des participants, et met l'accent sur l'identification des rôles, la prise de décision et la coordination d'équipe. Les activités incluent la priorisation de listes de contrôle d'intervention et la réalisation de simulations de scénarios réalistes avec des imprévus. Les participants apprendront les procédures établies de réaction aux incidents, la communication interservices et l'adaptabilité face aux incidents de sécurité grâce à des exercices pratiques et des séances de débriefing structurées.

Deux ressources/visuels dynamiques téléchargeables

- **Un rapport, une protection partagée -** Ressource de type affiche qui souligne l'importance de signaler rapidement les e-mails suspects afin de protéger les informations personnelles, les collègues et les données des clients
- **Hameçonnage, sécurité physique et violations de données : la totale ! -** Ressource de type infographie rappelant aux utilisateurs pourquoi le signalement immédiat des préoccupations de sécurité permet d'éviter que des problèmes mineurs ne se transforment en incidents majeurs

RESSOURCES DE LA SEMAINE 4



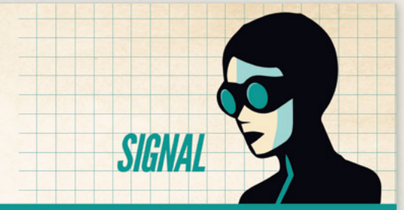
Partage du contenu

Voici un exemple d'e-mail du spécialiste Signal à utiliser pour diffuser l'audiocast et le module de jeu :

Objet suggéré :
[MISSION DE LA SEMAINE 4] **Maintenir l'équipe en alerte**

knowbe4

Maintenir l'équipe en alerte



MOIS DE SENSIBILISATION À LA CYBERSÉCURITÉ 2026 | MISSION SEMAINE 4

Chers agents,

Ici **Signal**, pour un dernier rapport de situation et un briefing.

La réussite de nos missions dépend de la vigilance de la WRD sur le terrain.

Signaler des incidents n'est pas de la délation. C'est transmettre des renseignements vitaux afin que nos équipes puissent sécuriser le périmètre et tenir les personnes malintentionnées à distance.

Voici les deux objectifs de votre quatrième et ultime briefing :

LA MISSION :

Écoutez : adoptez des réflexes anti-piratage : signalements. Maîtrisez un processus décisionnel fondamental en cybersécurité pour analyser les menaces en temps réel

Accéder à la partie 1 (https://training.knowbe4.com/modstore/view/ad7bb017-916b-442f-b1e7-4f96bf6b202f)

Jouez : en quête de confidentialité. Voyagez autour du monde (virtuellement) et testez vos connaissances sur les pratiques mondiales de confidentialité des données pour mieux comprendre les enjeux liés aux incidents de violation potentiels

Accéder à la partie 2 (https://training.knowbe4.com/modstore/view/a5ec90a8-956b-4675-8c63-c336812752e7)

Si vous avez des questions, contactez **[insérez le nom de la personne à contacter].**

Signal, fin de transmission au nom de toute l'équipe de la WRD.

DÉBRIEFING DE MISSION :

Garder toujours à l'esprit les risques liés au personnel

L'équipe de direction de la WRD espère que ce dossier de mission et les ressources fournies vous ont aidé à doter vos collaborateurs des compétences et des outils nécessaires pour repousser les cybermenaces de toutes natures.

Établir et maintenir une culture de la sécurité solide est une mission permanente. Un véritable changement de comportement positif repose sur une stratégie qui transforme votre plus grande surface d'attaque, votre personnel, en votre atout le plus précieux, réduisant ainsi les risques liés à la main-d'œuvre.

Considérez ces ressources comme un complément à une approche globale de la sensibilisation et de la formation à la sécurité. Si vous souhaitez savoir comment KnowBe4 peut vous aider à passer à l'étape suivante, contactez-nous.

Pour obtenir davantage de ressources et d'informations pour vous et vos utilisateurs tout au long du mois de sensibilisation à la cybersécurité, assurez-vous de suivre et de mentionner @KnowBe4 sur les réseaux sociaux. Utilisez les hashtags #CyberEngagés et #CyberSecMonth pour rester informé tout au long du mois de sensibilisation à la cybersécurité.

knowbe4