G DATA academy

SECURITY AWARENESS TRAININGS

COMMENT LES COURS EN LIGNE ET LES APPROCHES LUDIQUES FAVORISENT LA RÉUSSITE DE L'APPRENTISSAGE

G DATA academy

CONTENU

L'ignorance ne protège pas des cyberattaques 3

Menaces actuelles : des attaques chaque seconde 3

Vulnérabilité : l'Homme 4

Le rôle de l'Homme dans la sécurité informatique 6

Security Awareness Trainings - Au-delà de l'hameçonnage .. 7

Vigilance renforcée grâce aux formations en ligne 8

Formation en ligne : Le même savoir pour tous 9

Pourquoi le storytelling améliore la réussite de l'apprentissage 10

L'IGNORANCE NE PROTÈGE PAS DES CYBERATTAQUES

Améliorer la prise de conscience des cyber-risques et protéger les entreprises contre les attaques grâce aux Security Awareness Trainings

La conduite automobile et la sécurité informatique ont plus en commun qu'il n'y paraît à première vue. Dans les deux cas, les mesures technologiques protègent contre les accidents graves ou leurs conséquences. Pour les voitures, il s'agit des airbags, des ceintures ou des assistants de freinage, pour les ordinateurs et les réseaux, de la protection des terminaux, des pare-feux et des sauvegardes. Mais la réalité nous rappelle tous les jours que nous, les êtres humains, jouons également un rôle central dans la prévention des accidents. Oublier de regarder par-dessus son épaule, mal évaluer une distance et c'est l'accident. Nous apprenons généralement à nous comporter correctement sur la route à l'auto-école, mais où apprenons-nous à nous comporter correctement dans l'espace numérique ?

Ce livre blanc se penche sur le rôle des employés en matière de sécurité informatique (spoiler : ils jouent un rôle très important !) et sur la manière dont les formations en ligne peuvent aider à les sensibiliser à une utilisation sûre de l'informatique.

MENACES ACTUELLES : DES ATTAQUES CHAQUE SECONDE

Les années passées nous ont montré de manière impressionnante à quel point la situation en matière de sécurité informatique est fragile. Dans le monde entier, les cybercriminels ont profité de la vulnérabilité des gens suite à la pandémie de coronavirus. Selon une analyse des menaces de G DATA CyberDefense, le nombre de tentatives d'attaques bloquées a augmenté de 85 % au cours du deuxième semestre 2020 par rapport aux six premiers mois de la même année. Constat : Les cybercriminels se sont rapidement rendu compte que le télétravail entraînait de nouvelles vulnérabilités. Et ils en profitent. De même, les failles de sécurité critiques, l'absence de mises à jour ou l'imprudence des employés sont généralement à l'origine d'une attaque réussie.

Il est frappant de constater que les cybercriminels ont recours à des logiciels malveillants bien connus, dont certains sont utilisés depuis plusieurs années déjà, mais qui sont constamment améliorés. Les chiffres suivants prouvent l'ampleur du danger :

- En 2020, plus de 16,1 millions d'échantillons de logiciels malveillants différents ont été découverts par les experts en cyberdéfense de G DATA.
- Par rapport à l'année précédente, cela représente une augmentation de 228,6 %.
- Chaque minute, les cybercriminels ont publié 76 nouvelles versions d'un logiciel malveillant.

Une enquête récente menée par G DATA auprès des moyennes entreprises le prouve : Les petites et moyennes entreprises - et leurs collaborateurs - ne sont pas suffisamment conscients des cybermenaces. Ils ne se considèrent pas comme des cibles intéressantes pour les cybercriminels, malgré l'immense augmentation des menaces. Les conséquences de ces erreurs de jugement sont fatales et font que les entreprises ne se protègent pas suffisamment contre les attaques et que les incidents de sécurité informatique les frappent d'autant plus durement.

Le manque de sensibilisation et le manque de ressources nécessaires sont des obstacles majeurs pour les entreprises interrogées... Environ un quart des PME interrogées se justifient en disant que leur entreprise n'est pas une cible intéressante pour les cybercriminels.

© Copyright 2023 G DATA CyberDefense AG.

VULNÉRABILITÉ : L'HOMME

Une enquête de l'institut de recherche criminologique de Basse-Saxe conclut que 74 % des attaques de logiciels malveillants commencent par un courriel d'hameçonnage. Il suffit qu'un employé clique sur un lien corrompu pour que tout commence. Ces courriels contiennent souvent une pièce jointe malveillante ou un lien vers un site web permettant de distribuer des codes malveillants ou de « récupérer » des données confidentielles. Les conséquences peuvent menacer l'existence de toute entreprise. Au préjudice financier causé par l'arrêt de la production pendant des jours ou des semaines s'ajoute également le préjudice à la réputation lorsque des données confidentielles de clients, telles que des informations de connexion ou des données de paiement, tombent entre les mains de tiers.

L'exemple suivant illustre les conséquences que peut avoir la négligence d'un seul collaborateur : En février 2020, une cyberattaque a paralysé les activités du grossiste en matériel électrique Möhle à Münster pendant trois semaines. Un employé avait ouvert une pièce jointe infectée par un logiciel malveillant, ce qui a permis aux pirates d'accéder au réseau et de le crypter. Tous les écrans de l'entreprise sont devenus blancs et n'affichaient plus qu'un message d'avertissement. Pour compliquer les choses, l'entreprise n'a pas pu restaurer facilement ses données en raison d'une erreur dans le système de sauvegarde. L'entreprise s'est vue contrainte - contrairement aux conseils de la police judiciaire - de négocier avec les malfaiteurs. Au final, Möhle a dû payer une rançon de 120 000 euros. Sans ce paiement, ils n'auraient pas pu accéder aux données, ce qui aurait mis en péril l'existence de l'entreprise.

Le fait que l'hameçonnage soit un moyen d'attaque simple et populaire auprès des cybercriminels provoque également l'inquiétude de nombreux employés. C'est ce que démontre une étude de l'initiative « Deutschland sicher im Netz e.V. ». Plus de 56 % des personnes interrogées ont indiqué qu'elles étaient inquiètes à l'ouverture d'un e-mail.

© Copyright 2023 G DATA CyberDefense AG.

Fraude au PDG : Attaque par e-mail

PB

peter.b.kohlemacher@kohlemacher.ru
To: brigitte@kohlemacher.de

Bonjour Brigitte,
peux-tu effectuer le virement suivant pour notre client Hilf & Reich :
Total : 17 500 euros
IBAN : DE12 3456 6543 0000 1234 56
Communication : Remboursement pour erreur comptable

Chez Hilf & Reich, une nouvelle comptable a commencé il y a six semaines et elle a fait une erreur de comptabilité. Mais on peut rapidement rectifier cette erreur.

Merci beaucoup pour ton aide
Peter

Directeur

Brigitte Ziffrich, chef comptable depuis de nombreuses années au sein du cabinet de conseil fiscal « Kohlemacher & CO. », se méfie dès la première lecture. Depuis quand son patron la tutoie-t-il ? Bien que tous deux travaillent en confiance depuis de nombreuses années, ils se vouvoient - comme les 17 collaborateurs. En y regardant de plus près, elle remarque que la signature de son patron n'est pas la même que d'habitude : L'écriture est différente et le logo de l'entreprise est également déformé. Elle imprime le mail et s'adresse directement à Peter Kohlemacher. Sa réponse : « Non, ce mail ne vient pas de moi ! »

Ensemble, ils examinent d'autres détails du message. En comparant les IBAN, ils remarquent qu'il ne s'agit pas du compte habituel de l'entreprise Hilf & Reich. Et l'adresse e-mail de l'expéditeur est également fausse :peter.b.kohlemacher@kohlemacher.ru.

Dans cet exemple, l'entreprise a eu de la chance dans son malheur et n'a pas été victime de ce que l'on appelle une fraude au PDG. Avec cette arnaque, les criminels se font passer pour la direction ou les cadres d'une entreprise. À travers des courriels falsifiés, ils demandent aux collaborateurs du service de comptabilité de virer des sommes importantes depuis les comptes de l'entreprise. Au préalable, les malfaiteurs collectent de nombreuses informations sur l'entreprise qu'ils veulent attaquer et obtiennent ainsi les connaissances d'initiés nécessaires à leur escroquerie. Ils utilisent ces connaissances lors de l'attaque et causent ainsi d'importants dommages financiers.

© Copyright 2023 G DATA CyberDefense AG.

LE RÔLE DE L'HOMME DANS LA SÉCURITÉ INFORMATIQUE

Le coronavirus nous a contraints, en tant que société, à nous confronter à de nouveaux rythmes interpersonnels : Comment travailler en dehors de mon bureau ? Comment communiquer avec mes collègues si je ne les vois que virtuellement ? Comment structurer ma journée de travail que je passe entre mes quatre murs ? Dans un lieu qui est davantage associé à des mots comme « fin de journée » ou « détente », mais pas nécessairement au travail ? Nous nous posons ces questions parce qu'elles nous concernent directement en tant qu'êtres humains, en tant qu'individus.

Et pour chaque impact direct, il existe systématiquement un impact indirect. Cette catégorie comprend par exemple les questions relatives à notre sécurité numérique. Pourquoi ? La réponse est simple : À l'époque de la vie de bureau normale, notre employeur ou son service informatique veillait à ce que nous et notre lieu de travail soyons protégés numériquement. Dans ce contexte, outre les solutions évidentes de protection des terminaux, les pare-feux et les authentifications à deux facteurs, il existe d'autres mesures de sécurité telles que les restrictions d'accès et les mécanismes d'identification. Celles-ci doivent définir clairement les autorisations de chacun. Les mesures visent à empêcher que des informations critiques pour l'entreprise ne tombent entre les mains de personnes non autorisées. Cette liste n'est évidemment pas exhaustive.

Globalement, on peut affirmer ce qui suit : Dans le contexte professionnel normal, nous n'avons eu que peu à faire face aux questions relatives à la sécurité numérique et à la sécurité de nos informations. Une grande partie des employés travaillent en étant convaincus que leur employeur gère déjà très bien la situation au bureau.

Mais : Qu'en est-il de la sécurité informatique dans le contexte du télétravail ? Comment les collaborateurs se comportent-ils dans une situation où notre équilibre entre vie professionnelle et vie privée a fortement changé, car nous séparons moins strictement le travail et la vie privée ? Dans laquelle certaines personnes sont confrontées à des questions sur lesquelles se penchent d'habitude les experts ? Comment protéger les données critiques de l'entreprise lorsque je ne me trouve pas dans mon cocon habituel protégé, c'est-à-dire dans mon bureau ?

Depuis longtemps, les plus cyniques affirment que le plus grand risque se trouve juste devant l'écran. Cette phrase un peu vieillotte a (re)pris beaucoup d'importance en raison du coronavirus. Mais elle illustre une évidence : Le rôle de l'homme dans la sécurité informatique n'a jamais été aussi important !

Pourquoi donc ?

Une raison : Nous devons faire face à une situation inconnue. Nous travaillons à la maison, entourés de notre famille, qui ne fait toutefois pas partie du cercle de collègues. Nous ne disposons pas toujours d'un bureau personnel, alors nous travaillons sur la table de la cuisine ou dans le salon. Les membres de la famille sont susceptibles de tomber sur les informations affichées sur notre écran et d'entendre nos appels téléphoniques, alors que ces éléments sont confidentiels. On ne peut pas non plus se débarrasser des documents du bureau en les jetant à la poubelle. Au bureau, des boîtes ou des déchiqueteuses séparées et fermées à clé sont généralement prévues. Ces trois exemples doivent illustrer une chose : Pour que nous puissions continuer à travailler en toute sécurité avec des données critiques pour l'entreprise, un grand changement de mentalité s'impose. Un changement de mentalité qu'aucune solution de protection des terminaux ne peut remplacer. Depuis le début de la pandémie, le monde du travail s'est transformé et le télétravail fait partie du nouveau quotidien de nombreuses entreprises.

Pour que la présence numérique et que toutes les données restent sûres dans cette nouvelle situation de travail, il ne faut pas seulement une solution de sécurité. Il faut une nouvelle prise de conscience du rôle central de l'être humain pour protéger ses propres données, mais aussi les données critiques de l'entreprise.

Cette constatation soulève une autre question centrale : Comment réussir ce changement de mentalité ? En d'autres mots : Que doivent faire les entreprises pour que leurs collaborateurs, mais aussi les prestataires de services, adoptent de nouveaux comportements ? Pour qu'ils protègent également les données et informations importantes en dehors du bureau ?

Nous pouvons y parvenir en « mettant à jour » le comportement humain, grâce aux Security Awareness Trainings. Ces formations mettent l'accent sur les personnes et non sur la technique. Elles illustrent la manière dont nous protégeons numériquement non seulement notre employeur et ses fichiers, mais aussi nous-mêmes contre les dangers et les attaques. Ces formations permettent de faire évoluer les mentalités de manière ciblée et de faire comprendre aux collaborateurs la contribution qu'ils peuvent et doivent apporter à la sécurité informatique.

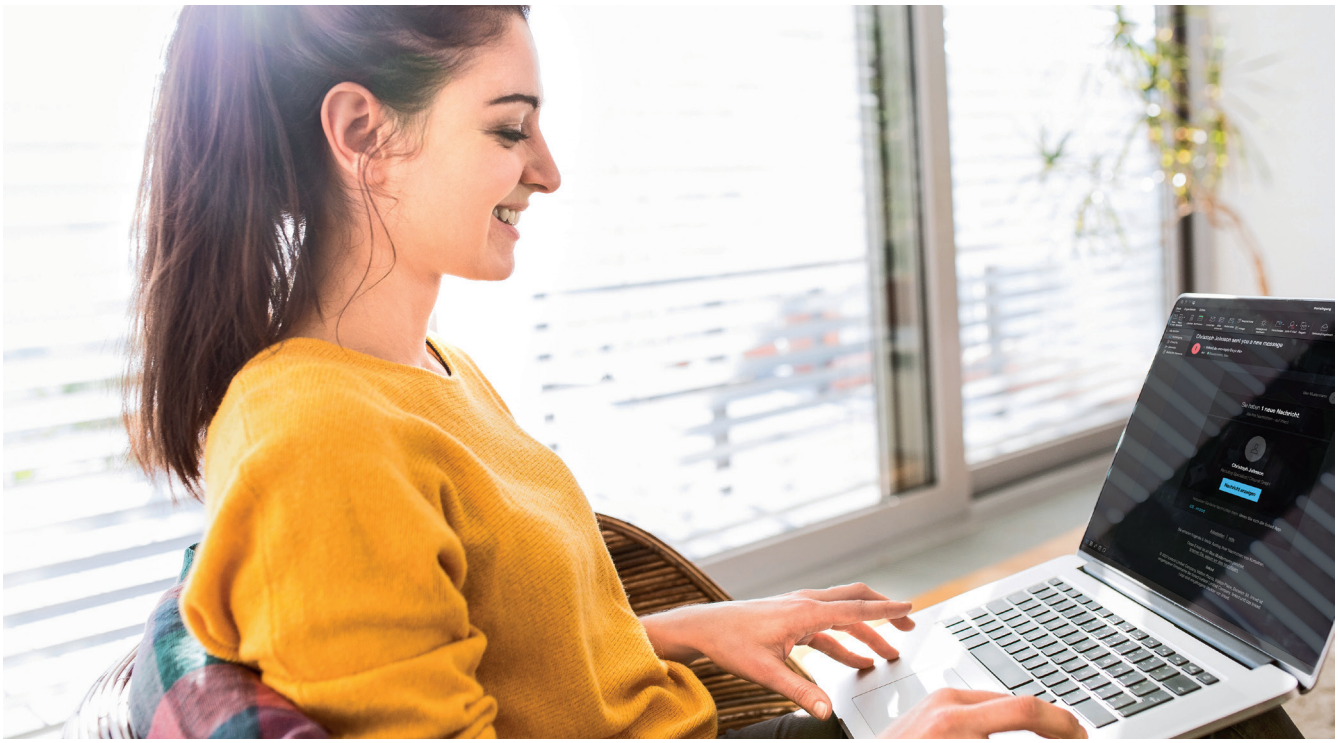
© Copyright 2023 G DATA CyberDefense AG.

SECURITY AWARENESS TRAININGS - AU-DELÀ DE L'HAMEÇONNAGE

Plus clairement : Les Awareness Trainings ne sont pas un sprint, mais une course de fond, car le comportement des collaborateurs vis-à-vis de la sécurité doit changer à long terme. En outre, le nombre de thèmes abordés étant large, cela nécessite un programme d'études complet et à long terme. Les employés ne doivent pas seulement connaître, mais aussi appliquer le cadre juridique de la protection et de la sécurité des données, qui découle du RGPD de l'UE ou des directives spécifiques au secteur. Autre sujet : La simple existence d'un plan d'urgence informatique n'empêche pas les cyberattaques. Les collaborateurs doivent les reconnaître et réagir en conséquence, c'est-à-dire s'adresser au Chief Information Security Officer ou à un collaborateur responsable dès le moindre soupçon

Les thèmes suivants devraient être abordés par les Security Awareness Trainings :

- La nouvelle façon de travailler - travailler en dehors du bureau et dans des lieux publics
- Gestion des risques et mots de passe - Créer et utiliser correctement des mots de passe sécurisés
- Hameçonnage et logiciels malveillants - Comment vos employés détectent les logiciels malveillants et les tentatives d'hameçonnage
- Classification des informations à traiter et à stocker - De quelles données s'agit-il ? Comment les informations sont-elles classifiées et pourquoi ?
- Travailler dans le cloud - Médias sociaux et travailler dans le cloud en toute sécurité
- Incidents de sécurité et rapports - Incidents de cybersécurité et contrôles d'accès
- Ingénierie sociale : comment les pirates manipulent les employés pour lancer leurs attaques
- Appareils mobiles - Utiliser de manière sécurisée les smartphones, tablettes, etc. au travail
- Gestion des informations - RGPD de l'UE, protection des données et vie privée
- Ransomware, chevaux de Troie d'accès à distance, enregistreurs de frappe et rootkits - Quels sont les logiciels malveillants qui menacent les entreprises ?



© Copyright 2023 G DATA CyberDefense AG.

VIGILANCE RENFORCÉE GRÂCE AUX FORMATIONS EN LIGNE

Les cybercriminels sont de plus en plus ciblés dans leurs attaques et s'adressent directement à leurs victimes. Dans cette situation, les chances de succès sont nettement plus élevées que lors d'une attaque de masse.

La raison ? Le comportement humain peut être attribué à différents déclencheurs externes. Ce sont des influences externes qui déclenchent un comportement concret chez les personnes. Parmi ces déclencheurs, on trouve la curiosité, comme le montre l'exemple suivant :

Peu avant les vacances de Noël, un mail arrive dans la boîte de réception de Tina, employée administrative dans un groupe d'assurances. Le contenu est effroyable : L'expéditeur fait savoir qu'il a pris des photos compromettantes de Tina lors de la dernière fête d'entreprise. Il lui demande de les regarder et de lui répondre pour éviter qu'elles ne soient diffusées. Tina réfléchit fébrilement à ce qui s'est passé lors de la fête de Noël deux semaines plus tôt et envisage de cliquer sur le lien contenu dans le mail. Il s'agit ici d'un e-mail d'hameçonnage. Les photos n'existent pas et pourtant, on peut comprendre le désir de clarifier la situation en cliquant sur le lien. Pourquoi ? Pourquoi de nombreuses personnes cliquent-elles sur ces messages ou sur des messages similaires ? Cela est dû au déclencheur « Curiosité » dont nous avons parlé. Même si la probabilité est faible, il se peut que ce soit vrai. D'autres déclencheurs sont la serviabilité ou la cupidité. Qui n'a pas reçu dans sa boîte de réception un e-mail lui faisant miroiter un gain d'un million ou un héritage ?

L'exemple ci-dessus illustre les astuces utilisées par les cybercriminels pour inciter les gens à agir de manière irréfléchie. Ceux qui pensent que les attaques sont sournoises et qu'une protection efficace semble à peine possible, se sont déjà résignés à leur sort.

Mais la vérité est tout autre. La voici : Les formations en ligne et les Security Awareness Trainings font des utilisateurs non seulement la dernière ligne de défense contre les cyberattaques, mais aussi la plus efficace.

Aucune mesure de protection technique, telle qu'une solution de sécurité, ne peut protéger totalement les utilisateurs contre les attaques d'hameçonnage. C'est aux personnes et surtout grace à leur sensibilisation à la sécurité de reconnaître à temps ces attaques et de les repousser.

Les formations en ligne modernes permettent aux élèves d'acquérir de nombreuses connaissances sur les différentes attaques et formes d'attaques. Les unités de formation expliquent comment les attaques se déroulent au quotidien, quels sont leurs dangers et comment les employés peuvent s'en protéger. Les formations en ligne modernes dans le domaine de la Security Awareness sont dynamiques et surtout structurées en petites séries d'apprentissage (séries de formations de qualification). Les élèves peuvent ainsi accéder à la formation à tout moment et se perfectionner rapidement et facilement.

Conclusion: Il n'existe pas de protection technique suffisante pour protéger les utilisateurs de tous les cyber-risques. Les campagnes d'hameçonnage, en particulier, contournent les mécanismes de protection techniques en ciblant directement les personnes en tant qu'utilisateurs.

Mais: Avec les connaissances étendues acquises grâce aux Security Awareness Trainings consacrés aux méthodes et aux objectifs des pirates, les collaborateurs sont armés pour ne pas tomber dans le piège des escrocs.

Les formations en ligne et les Security Awareness Trainings font des utilisateurs non seulement la dernière ligne de défense contre les cyberattaques, mais aussi la plus efficace.

© Copyright 2023 G DATA CyberDefense AG.

FORMATION EN LIGNE : LE MÊME SAVOIR POUR TOUS

Les Security Awareness Trainings visent à permettre aux élèves d'identifier les dangers qui les ciblent directement et contre lesquels il n'existe aucune protection technique suffisante. Les formations numériques sont en pleine mutation et en constante évolution. Les progrès technologiques et la numérisation croissante ont fait évoluer la nature des apprentissages en ligne. L'époque où les collaborateurs devaient suivre des formations en ligne d'une durée parfois de 60 minutes, avec peu d'animations, non sonores et austères, est révolue. Cette méthode d'apprentissage était particulièrement inefficace.

La raison : En moyenne, toutes les onze minutes, les e-mails, les appels téléphoniques, les collègues, les tâches secondaires ou d'autres bruits ne cessent de nous distraire. Il est donc de plus en plus difficile de se concentrer et de travailler sans être dérangé pendant une période prolongée. L'attention devient de plus en plus une ressource rare et précieuse. Le microapprentissage tient compte de cette situation et veille à ce que les petites unités d'apprentissage s'intègrent facilement au rythme de travail d'aujourd'hui. Les formats d'apprentissage en ligne d'une durée de 45 minutes ou plus sont de moins en moins populaires. Les entreprises et les particuliers ont de plus en plus recours à des offres d'apprentissage mobiles, intelligentes et courtes.

Les formations en ligne modernes s'adaptent aux besoins et aux conditions individuelles des élèves. Les aspects centraux d'un apprentissage en ligne moderne sont les suivants :

- Unités courtes
- Storytelling efficace
- Enregistrement de la progression
- S'adresser directement à l'élève
- Interactions nombreuses entre la formation et les élèves
- Approfondissement direct des connaissances

Sachant que les formations en ligne modernes peuvent être suivies sur des appareils mobiles, elles permettent aux élèves d'apprendre à tout moment et en tout lieu. Ici, la devise « Formation continue » ne s'arrête jamais. Autre avantage : Le transfert de connaissances est nettement plus important qu'avec les formations en ligne classiques. En d'autres mots : Au lieu de passer leur temps à regarder par la fenêtre dans le train lors d'un voyage d'affaires, les collaborateurs peuvent aussi utiliser ce temps de manière productive et travailler sur leur sensibilisation à la sécurité. Grâce à un système de gestion de l'apprentissage bien structuré et à une interface utilisateur simple, les élèves peuvent reprendre directement là où ils s'étaient arrêtés. Les formations peuvent être consultées à tout moment et en tout lieu et comportent de petites récompenses lorsqu'une formation est terminée. Il s'agit par exemple de certificats pour des unités de formation achevées. Grâce à l'utilisation d'éléments de ludification et d'une narration captivante dans les formations, le plaisir est également au rendez-vous.

Pour un thème central comme la sécurité informatique, cela signifie ce qui suit : L'utilisateur n'est armé efficacement contre les cyberattaques que si les connaissances nécessaires à la protection peuvent être consultées à tout moment. C'est pourquoi les formations en ligne modernes ne se contentent pas de donner aux élèves la possibilité d'apprendre efficacement, mais elles leur permettent également de toujours accéder aux connaissances - car la situation en matière de menaces est très dynamique. C'est pourquoi les systèmes de gestion de l'apprentissage modernes fonctionnent comme des ouvrages de référence. En cas d'e-mail suspect, les personnes concernées peuvent consulter le chapitre de formation « Caractéristiques des e-mails suspects » et voir si un e-mail dans la boîte de réception remplit toutes ou certaines des caractéristiques. Dans le chapitre suivant, les élèves apprennent comment traiter les e-mails suspects : Signalez l'incident à votre service informatique.

D'un point de vue cognitif, le processus peut s'expliquer de la manière suivante : Les élèves ont toujours les connaissances de l'apprentissage en ligne sous la main et l'e-mail a suscité de la méfiance pour cette raison. Ils se souviennent parfaitement de l'unité d'apprentissage en ligne correspondante, qui explique comment reconnaître les e-mails suspects. La méthode d'apprentissage moderne a ainsi aidé à reconnaître une véritable attaque et à y faire face correctement.

© Copyright 2023 G DATA CyberDefense AG.

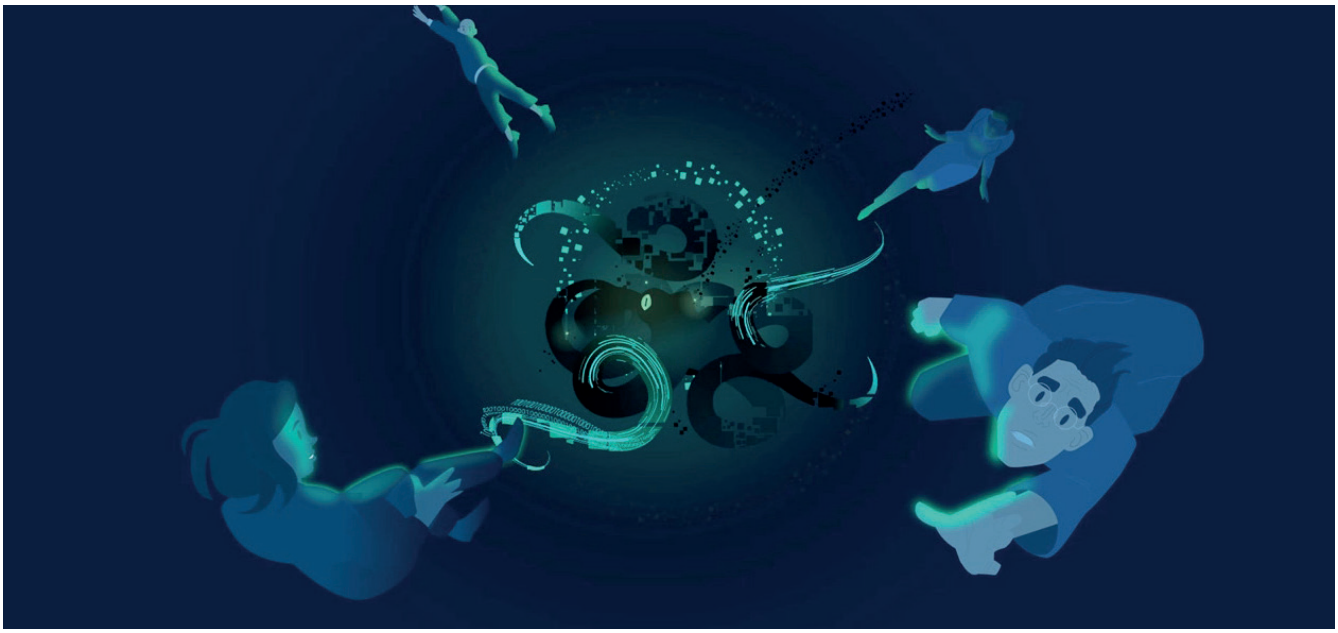
POURQUOI LE STORYTELLING AMÉLIORE LA RÉUSSITE DE L'APPRENTISSAGE

Depuis l'école, nous savons déjà que chaque personne apprend différemment. Certains préfèrent apprendre de manière classique avec des textes et des chiffres, tandis que d'autres préfèrent apprendre de manière plus exploratoire, c'est-à-dire à travers une histoire qui leur est racontée au sujet d'un thème précis. Au final, chacun apprend à sa manière - il n'y a pas de bonne ou de mauvaise approche. Une méthode est jugée bonne lorsqu'elle permet à la personne d'apprendre.

Il apparaît toutefois qu'une majorité tend vers la deuxième approche d'apprentissage. Les jeunes, en particulier, ont tendance à apprendre de manière plus exploratoire, car ils sont entourés au quotidien de scénarios narratifs, notamment sur les réseaux sociaux (Instagram par exemple), sur les portails de streaming et dans les jeux vidéo. Depuis toujours, l'être humain raconte des histoires. Aujourd'hui encore, nous racontons à nos enfants des contes et autres histoires pour les endormir. Nous consommons des histoires sous forme de films, de séries, de livres, de bandes dessinées ou nous nous les racontons mutuellement. Notre vie n'est qu'une collection d'histoires : Ainsi, il est prouvé que jusqu'à deux tiers de nos conversations quotidiennes se composent d'histoires. Une grande partie de ces histoires transmettent consciemment ou inconsciemment des connaissances. Aujourd'hui, on remarque particulièrement l'efficacité du recours à la narration en tant qu'outil d'apprentissage et d'enseignement dans le domaine numérique, par exemple dans les apprentissages en ligne.

C'est pourquoi de nombreux apprentissages en ligne suivent l'approche du « storytelling ». Chaque unité d'apprentissage est alors associée à une histoire correspondante, dans laquelle tous les chiffres, dates et faits importants sont bien intégrés. Dans le cadre du storytelling, on utilise généralement des personnages spécialement créés, de sorte que les élèves n'apprennent pas seulement par le biais d'une histoire racontée, mais de manière à associer ce qu'ils ont appris à des personnes qui leur sont familières. Nous nous souvenons mieux de certaines expériences et de certains événements lorsqu'ils sont associés à des personnes et à des environnements ou à d'autres stimuli (odeurs, etc.). À retenir : Notre cerveau ne fait pas la différence entre ce que nous vivons nous-mêmes et ce que vit un personnage. C'est pourquoi nous mémorisons si bien les informations.

Parmi tous les avantages du storytelling, une règle s'applique tout particulièrement : « La brièveté est la clé de la réussite. » Même la meilleure des histoires peut rapidement devenir ennuyeuse si elle est trop longue et grandiloquente. Cette approche s'applique tout particulièrement aux formations en ligne : Un thème, par exemple l'hameçonnage, est d'une part raconté à travers une histoire correspondante - avec des personnages, et d'autre part, plusieurs séances de formation sont nécessaires pour traiter tous les contenus en détail. En effet, les unités d'apprentissage de plus de dix minutes provoquent une baisse de l'attention, tout comme le suspense de l'histoire. Et l'apprentissage en pâtit.

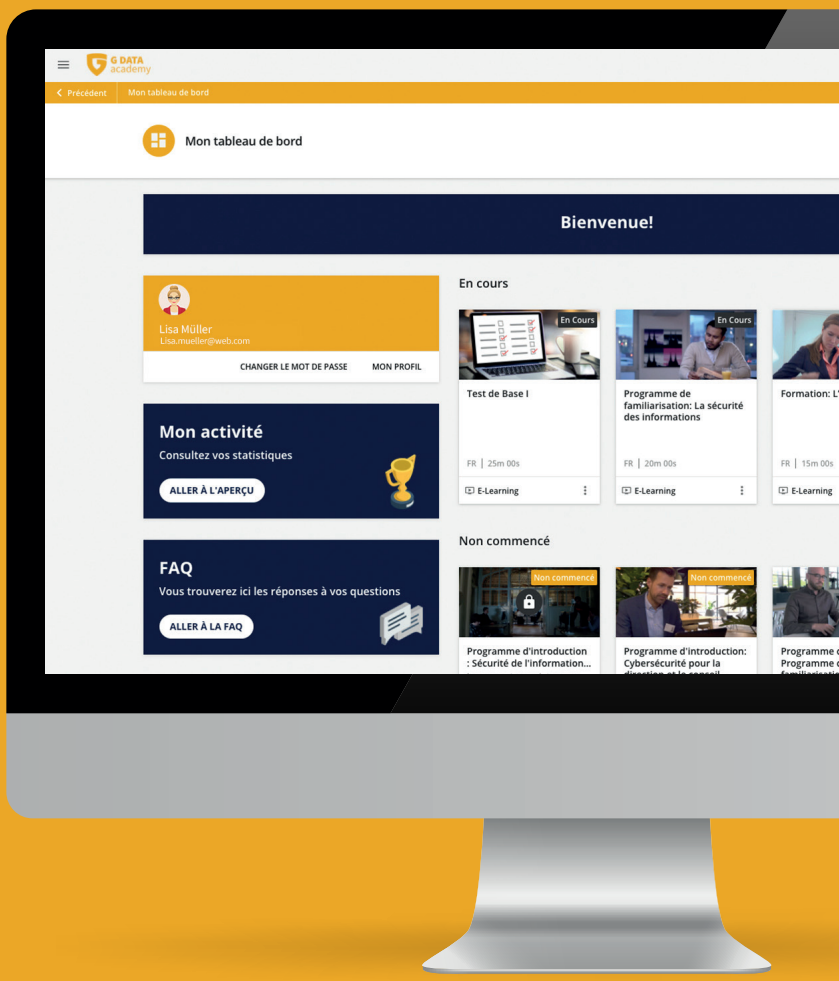


© Copyright 2023 G DATA CyberDefense AG.

G DATA academy

Nous avons éveillé votre curiosité ?
N‘hésitez pas à tester par vous-même nos formations et à voir comment nous utilisons des récits et approches ludiques dans nos contenus d‘apprentissage.

Cliquez ici pour obtenir une version d‘essai
gdata.fr/awareness-training



© Copyright 2023 G DATA CyberDefense AG.