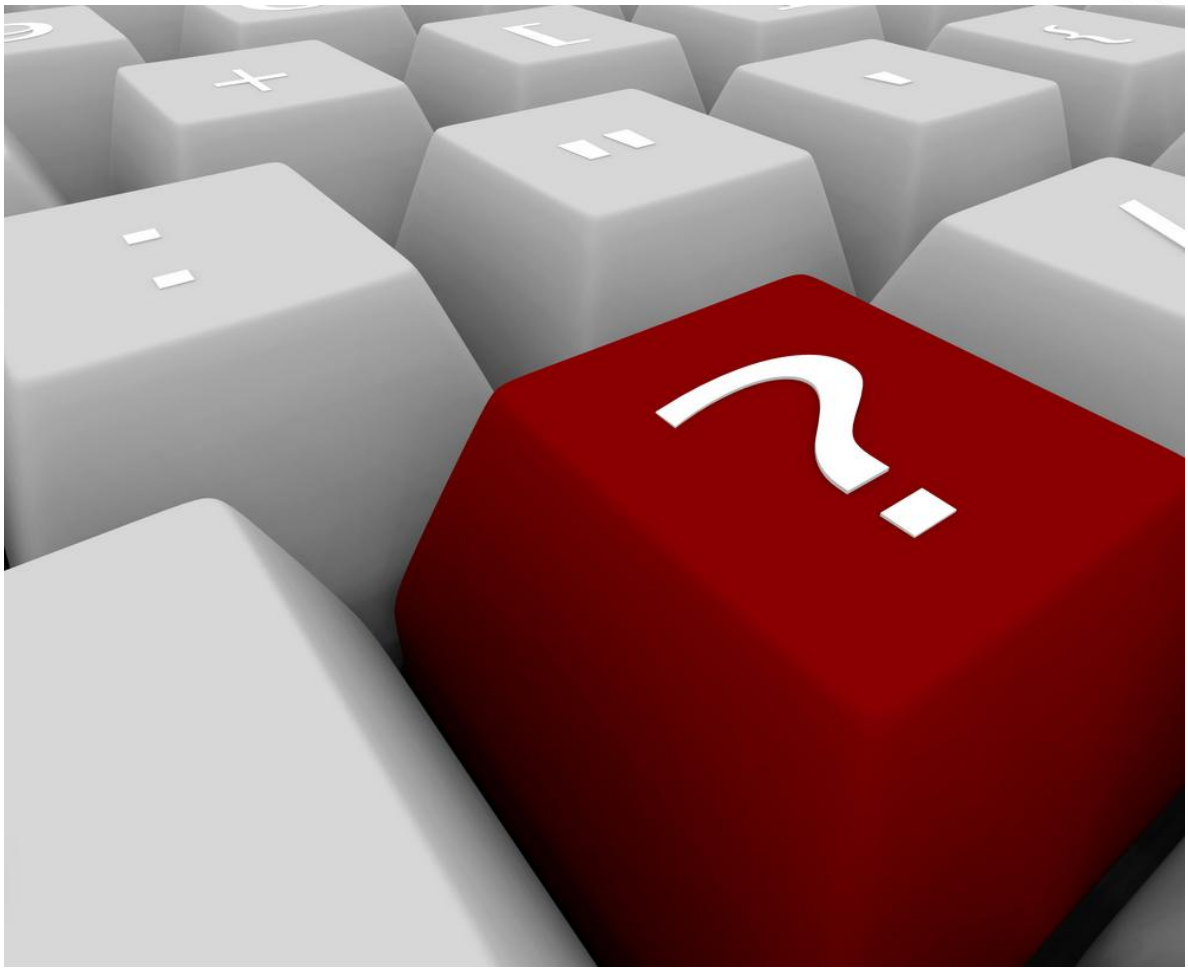
Modèles de quiz de sensibilisation

À destination des parents, des utilisateurs finaux et des PME



enisa
European Network and Information Security Agency

À propos de l'ENISA

L'ENISA (European Network & Information Security Agency) est une agence de l'Union européenne créée en vue de promouvoir le fonctionnement du marché intérieur. Centre d'excellence pour les États membres et les institutions européennes en matière de sécurité des réseaux et de l'information, l'ENISA dispense des avis et des recommandations et intervient en tant que pôle d'information pour les bonnes pratiques. Par ailleurs, l'agence ENISA facilite aussi les contacts entre les institutions européennes, les États membres, le monde des affaires et de l'industrie.

Coordonnées

Pour prendre contact avec l'ENISA ou pour toutes demandes générales concernant la sensibilisation à la sécurité de l'information:

E-mail: KJELL KALMELID, Expert en Sensibilisation — kjell.kalmelid@enisa.europa.eu
Internet: http://www.enisa.europa.eu

Modèles de quiz

Remerciements
Kjell Kalmelid, Expert en Sensibilisation, ENISA et coordinateur de ce document, souhaite remercier très cordialement les quatre auteurs, membres de l'AR Community (communauté de sensibilisation), qui, ensemble, ont élaboré et compilé les modèles de quiz:

- Anna Rywczyńska, NASK, Pologne
- Pierre-Luc Refalo, Hapsis Éducation, France
- Claudio Telmon, CLUSIT, Italie
- Johannes Wiele, Konradin IT-Verlag et Ludwig-Maximilians- Universität Munich, Allemagne.

Des remerciements particuliers vont également à Peter Pfeifhofer, Expert national détaché, ENISA et à Wendy Goucher, Idrach Ltd., Royaume-Uni et membre de l'AR Community, pour la révision des modèles et le feed-back fourni.

Table des matières

Préface

À propos de ce document

Ce document est le fruit du travail conjoint de quatre membres de l'AR Community de l'ENISA. Son but est de fournir un contenu de sensibilisation à la sécurité de l'information sous la forme d'un certain nombre de modèles de quiz.

À propos de l'AR Community

L'AR Community est une communauté gratuitement accessible ouverte aux professionnels actifs dans le domaine de la sécurité de l'information. Elle a été lancée en 2008 par l'ENISA en vue de créer une communauté centrée sur la sécurité de l'information, en ciblant plus particulièrement les professionnels intéressés par les questions liées à la sensibilisation en la matière.

Bien qu'elle vise essentiellement à attirer des membres en Europe, l'AR Community compte aussi plusieurs membres de pays non européens qui partagent tous la même idée: sensibiliser les individus à la sécurité s'avère déterminant pour assurer une réelle sécurité informatique dans toute organisation.

Introduction

Portée

Ce document a pour objet de fournir du contenu de sensibilisation à la sécurité de l'information sous la forme d'un certain nombre de modèles de quiz. Le public cible de ce document est constitué par les organisations désireuses de sensibiliser leurs groupes cibles à la sécurité de l'information.

Objectif

Ces quiz ne doivent pas être considérés comme des autoévaluations exhaustives du niveau de sensibilisation et de connaissances actuel des individus. L'objectif est plus simplement de donner aux répondants une indication quant à leur niveau de sensibilisation et, dans le meilleur des cas, de fournir un outil susceptible de stimuler un intérêt accru pour les valeurs et les risques associés à l'utilisation des ordinateurs et des services en ligne sur l'internet.

Comment utiliser les modèles

Les modèles peuvent être utilisés soit sous forme imprimée, avec un feuillet pour les réponses, ou être mis en œuvre sous la forme d'un quiz web. Chaque quiz comporte un *Texte introductif* qui doit être laissé en l'état ou qui, si la formule du quiz web est privilégiée, sera repris sur la même page que les questions.

IMPORTANT

En plus des informations fournies dans les colonnes Commentaires, veuillez aussi mentionner les sources d'information locales/nationales que vous jugez importantes comme, p.ex. des liens, ainsi que les coordonnées de services d'assistance téléphonique et des autorités locales/nationales. Dans certaines questions, ce type d'information est suggéré entre crochets [INSÉRER POINT DE CONTACT APPROPRIÉ].

Survol des quiz

Chacun des trois quiz proposés est destiné à un groupe cible déterminé: les parents, les utilisateurs et les cadres supérieurs des petites et moyennes entreprises (PME).

Chaque modèle s'articule autour d'un certain nombre de *thèmes* déclinés en *questions*, elles-mêmes suivies d'une rubrique *Commentaires*. Dans certains quiz, cette colonne propose un commentaire vrai/faux, assorti d'informations complémentaires et, parfois, d'un feed-back succinct.

Parents

Thème	Questions	Commentaires
Utilisation du PC par votre enfant	1. Activités en ligne 2. Communication 3. Utilisation du PC 4. Internet et risques 5. Compréhension de l'internet	Faire savoir aux parents dans quelle mesure leur enfant devrait utiliser l'ordinateur et pour quels types d'activités.
Vie privée & Réseaux sociaux	6. Utilisation des sites de réseaux sociaux 7. Créer des profils sans risques 8. Divulgation d'informations	Faire savoir aux parents comment créer des profils sans risques, savez-vous si votre enfant a un profil en ligne, quelles informations votre enfant ne devrait-il pas mettre en ligne?
Contenus illicites	9. Signalement des contenus illicites 10. Confrontation à des contenus illicites	Logiciel de filtrage – savez-vous comment l'utiliser?
Partage de fichiers	11. Utilisation du poste-à-poste	Les enfants téléchargent des contenus multimédias. Les parents sont-ils informés de la législation sur le droit d'auteur? Ce qui est permis et ce qui ne
Cyberintimidation	12. Réaction face à la cyberintimidation	Qu'entraîne le fait de soumettre de fausses informations et/ou d'intimider quelqu'un sur l'internet?

Utilisateurs finaux

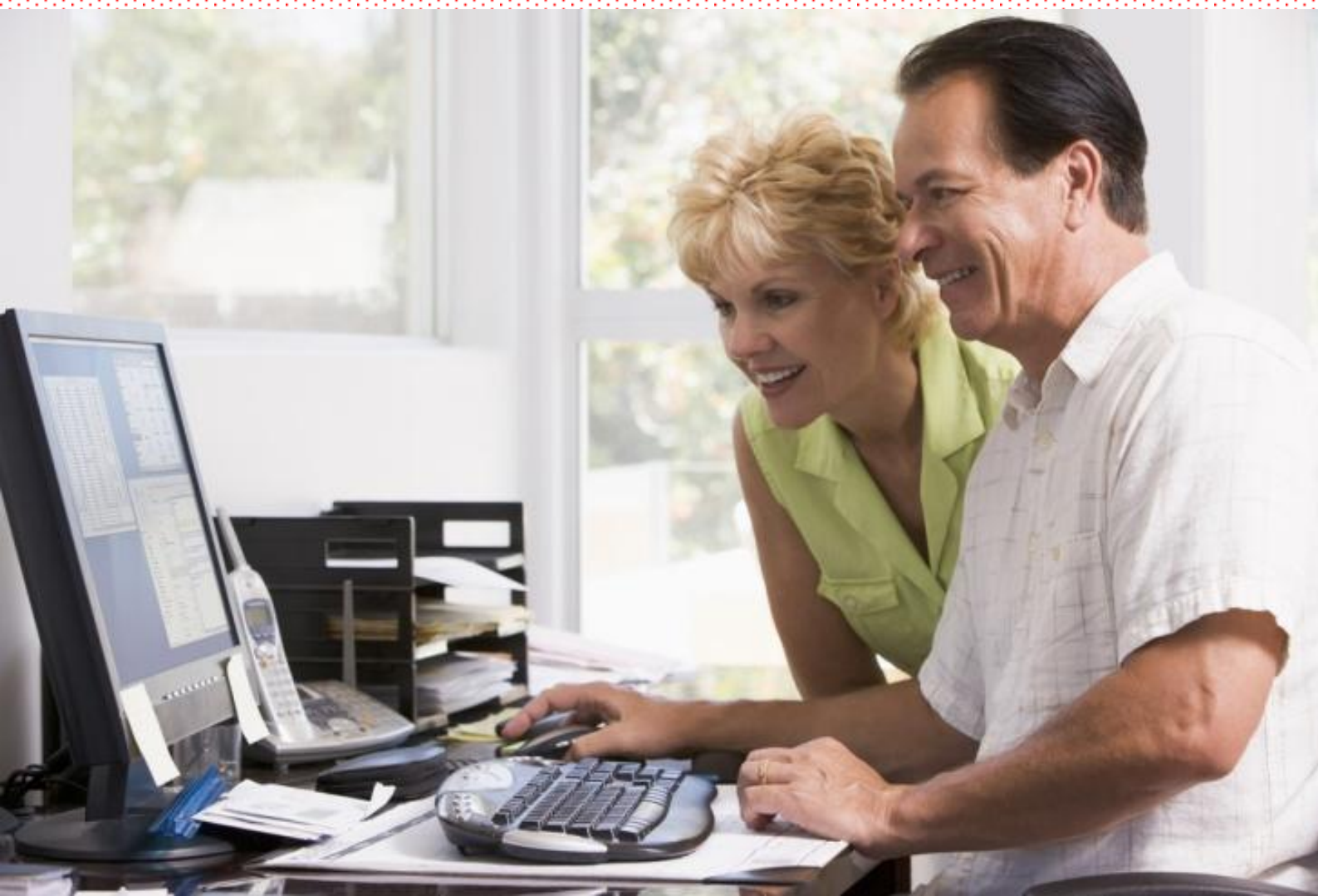
Thème	Questions	Commentaires
Menaces sur l'internet	1. Fichiers joints aux e-mails 2. Applications anti-virus et pare-feux 3. Corrections de programmes/Mises à jour de sécurité 4. Mots de passe	Le répondant connaît-il les différentes menaces et sait-il comment s'en protéger?
Hameçonnage	5. Shopping en ligne sécurisé 6. Compréhension du hameçonnage	Le répondant connaît-il le shopping en ligne sécurisé et la menace des attaques d'hameçonnage?

Protection des informations	7. Back-up 8. Clés USB à mémoire flash 9. Compréhension du chiffrement	Le répondant connaît-il l'importance de la sauvegarde des informations de valeur, les risques et désavantages liés aux clés USB à mémoire flash, et le chiffrement pour protéger les informations?
Aspects juridiques/Droits d'auteur	10. Téléchargement de fichiers	Comment l'internet se compare-t-il au monde réel? Téléchargement de matériels couverts par le droit d'auteur.

PME

Thème	Questions	Commentaires
Profil de risque	1. Actifs informationnels 2. Menaces	Les cadres de PME doivent identifier les informations cruciales et les menaces potentielles.
Aspects juridiques et contractuels	3. Vie privée / Données personnelles 4. Licences logicielles 5. Gestion des contrats	Les cadres de PME doivent être au fait de ce type de responsabilités juridiques.
Aspects humains et organisationnels	6. Gestion des mots de passe 7. E-mail 8. Navigation sur l'internet 9. Ingénierie sociale 10. Appareils mobiles	Plusieurs comportements doivent être adoptés pour réduire les risques liés aux accès et aux communications. Les managers doivent montrer l'exemple à leurs employés.
Outils de sécurité	11. Back-up 12. Anti-virus / logiciels espions 13. Accès à distance sécurisés 14. Chiffrement	Plusieurs technologies sont obligatoires pour protéger le système informatique et les données sensibles. Les cadres de PME doivent comprendre le niveau de sécurité de base à mettre en œuvre.

Quiz Parents



Quiz Parents

Texte introductif au Quiz Parents

Bienvenue dans le Quiz de sensibilisation ENISA Spécial Parents!

Le but de ce quiz est de vous fournir, en votre qualité de parent, un moyen de tester votre sensibilisation à, et vos connaissances concernant un certain nombre d'aspects liés à l'utilisation par votre enfant de l'ordinateur et des services en ligne sur l'internet.

L'internet est une ressource fantastique qui offre une quantité considérable d'informations et de services de valeur. Il comporte toutefois aussi des risques et en tant que parent, vous devriez être conscient de ceux-ci.

Ce quiz ne doit pas être considéré comme une autoévaluation exhaustive de votre niveau de sensibilisation et de connaissances actuel. L'objectif est plus simplement de vous donner une indication quant à votre niveau de sensibilisation et, dans le meilleur des cas, de fournir un outil susceptible de stimuler un intérêt accru pour les valeurs et les risques associés à l'utilisation de l'internet par votre enfant. Nous espérons également que vous trouverez intéressantes et utiles les sources d'information fournies sur ce site web.

Modèles de quiz

N°	Question	Réponses	Commentaires
1	Quelles sont les activités en ligne de votre enfant?	a) Conversation en ligne ou messagerie électronique b) Blogging ou utilisation de sites de réseaux sociaux c) Jeux en ligne d) Recherche d'informations sur l'internet pour des devoirs ou des travaux scolaires e) Plus ou moins tout ce qui précède f) Je ne sais pas	f) Il est généralement recommandé aux parents de rester informés de ce que leurs enfants font en ligne. Demandez à vos enfants ce qu'ils font et de vous montrer comment fonctionnent différentes fonctions, jeux ou autres activités en ligne! De cette manière, votre enfant comprendra que vous êtes vraiment intéressé par ce qu'il/elle fait. C'est aussi important pour vous permettre de savoir si votre enfant est engagé dans des activités qui, à vos yeux, méritent d'être interdites. a)-e). Il semble que votre enfant tire activement parti des avantages de l'informatique. C'est très bien! Vous semblez également savoir ce que fait votre enfant quand il utilise l'ordinateur (a priori, plus vous avez coché de cases, plus vous en savez long à ce sujet). **Conseils de base** Installez votre/vos ordinateur(s) domestique(s) dans des endroits parfaitement visibles, p.ex. dans la salle de séjour ou la cuisine, en sorte de pouvoir surveiller aisé-

N°	Question	Réponses	Commentaires
			ment les activités de votre enfant.
2	Discutez-vous avec votre enfant de ses activités sur l'internet?	a) Oui b) Non c) Parfois	a) et c) C'est très bien que vous discutiez de ces choses avec votre enfant. Continuez à le faire de manière régulière. b) c) Il est très important de discuter régulièrement de ces questions avec votre enfant. C'est en fait la seule façon pour vous d'apprendre quelles sont les activités en ligne de votre enfant et d'être en mesure de comprendre les risques possibles. **Conseils de base** La confiance est essentielle. Instaurez une communication ouverte en sorte que vos enfants vous parlent de leurs activités en ligne et sentent, dans le même temps, qu'ils ont votre confiance pour explorer l'internet de manière responsable.
3	En moyenne, combien de temps votre enfant passe-t-il devant l'ordinateur?	a) Plus de 3 heures/jour b) 2-3 heures/jour c) 1-2 heures/jour d) Le temps dont il/elle a besoin e) Je ne sais pas f) Moins de 1 heure/jour	a) – e) Veillez à rester informé du temps que votre enfant passe devant l'ordinateur. N'oubliez pas que votre enfant a également besoin de sport et d'autres activités physiques. f) Moins de 1 heure/jour ne devrait pas vous préoccuper.

N°	Question	Réponses	Commentaires
			Conseils de base L'utilisation excessive de jeux ou de services en ligne, en particulier la nuit, devrait être un signal vous amenant, en tant que parent, à restreindre l'utilisation de l'internet par votre enfant.
4	Estimez-vous que l'internet est un environnement à risque?	a) Non, les risques sont surestimés b) Oui, absolument c) Il y a des risques, mais aussi des informations, des services et des outils de communication utiles d) Je ne sais pas	a) En effet, les risques sont parfois surestimés, mais il est vrai aussi qu'il est malaisé d'évaluer les risques dans la mesure où de nouveaux services et fonctions sont constamment introduits sur l'internet. b) et c) Il est bien que vous sachiez que l'internet peut être dangereux pour votre enfant, sans oublier toutefois qu'il donne effectivement accès à des informations et des services utiles et fonctionne comme un outil de communication. d) Le mieux que vous puissiez faire est d'essayer d'en apprendre autant que possible sur les risques de l'internet, en commençant par suivre les recommandations de sécurité de votre fournisseur de service et celles de ce site web.
5	Dans quelle mesure pensez-vous	a) Mieux que mon enfant	a) et c) C'est bien que vous soyez conscient

N°	Question	Réponses	Commentaires
	vous connaître la façon d'utiliser l'internet?	b) À peu près comme mon enfant c) Moins bien que mon enfant d) Je ne sais pas	de votre niveau de connaissances par rapport à votre enfant. Une fois de plus, ce qui importe est que vous en appreniez plus sur les risques en ligne et comment les réduire. c) Ne soyez pas déconcerté par le fait que votre enfant semble en savoir beaucoup plus que vous sur l'internet et ses services. Beaucoup de parents sont dans le même cas. d) Si vous ne savez pas, nous vous recommandons de vous asseoir de temps en temps à côté de votre enfant et de l'accompagner dans sa navigation sur le web. Vous devriez très vite trouver la réponse.
6	Quelles informations est-il normal que votre enfant divulgue quand il utilise des sites de réseaux sociaux?	a) Le vrai prénom et seulement la dernière initiale b) Le nom l'école où va votre enfant c) La couleur préférée d) Les vrais prénoms des parents, mais pas leur nom de famille e) La date de naissance, mais pas le nom f) Les noms d'amis ou de membres de la famille g) Le surnom	a), b), d), e) et f) - Faux. Vous devriez expliquer à votre enfant qu'il ne doit jamais divulguer sur l'internet aucune information qui pourrait aider quelqu'un d'autre à l'identifier dans la vie réelle. c) et g) Correct. Un surnom ou une couleur préférée sont des informations qui peuvent être mises sans risques sur l'internet.

N°	Question	Réponses	Commentaires
7	Votre enfant a-t-il créé un profil sans risques sur le site de réseau social qu'il/elle utilise?	a) Oui b) Non c) Je ne sais pas d) Mon enfant n'utilise pas de sites de réseaux sociaux	a) Bien! Vérifiez toutefois que votre enfant sait comment utiliser les sites de réseaux sociaux de manière sûre. Assurez-vous que le profil sans risques de votre enfant répond aux recommandations de base ci-dessous. b) Suivez les conseils de base ci-dessous pour créer un profil sans risques pour votre enfant. c) Le fait d'ignorer comment utiliser les sites de réseaux sociaux en toute sécurité risque d'entraîner des violations de la vie privée de votre enfant. d) Les sites de réseaux sociaux sont extrêmement populaires parmi les enfants et les jeunes. Ils peuvent s'avérer un outil précieux et apporter beaucoup de satisfactions, en permettant, par exemple, de converser en ligne avec des amis aux quatre coins du monde. **Conseils de base pour créer des profils sans risques:** 1. Définissez votre profil comme privé, en sorte que les autres utilisateurs ne puissent voir que le nom d'utilisateur de votre enfant et limitez la divulgation

N°	Question	Réponses	Commentaires
			d'autres informations, comme par exemple une photo de votre enfant. Ne permettez qu'aux amis de votre enfant d'accéder à des informations additionnelles. Veillez à savoir qui sont les amis de votre enfant. 2. Ne mettez jamais de données privées en ligne, telle que nom de famille réel, adresse, photo ou numéros de téléphone. 3. Soyez sélectif avec les photos. Une fois disponibles en ligne, elles restent pour toujours sur l'internet. Respectez la vie privée d'autrui – ne permettez pas à votre enfant de mettre sur le web la photo de quelqu'un d'autre sans demander sa permission. 4. Dites à votre enfant d'encourager ses amis à créer des profils sans risques. N'hésitez pas à discuter de ces questions avec les parents des amis de votre enfant.
8	Quelles informations pouvez-vous divulguer si vous voulez créer un profil sans risques sur des sites de réseaux sociaux?	a) Je peux divulguer mon numéro de téléphone mais pas mon adresse e-mail b) Je peux divulguer mon adresse postale mais pas mon numéro de téléphone c) Je peux dire aux personnes que je rencontre en ligne où je travaille ou dans quelle école	a) - c) Ces éléments d'information sont autant d'exemples de données privées. Vous ne devriez jamais mettre d'informations personnelles en ligne. Si vous décidez toutefois de le faire, veillez alors à ce que ces données ne soient accessibles qu'à des uti-

N°	Question	Réponses	Commentaires
		je suis inscrit d) Je peux divulguer n'importe quelle information personnelle aux personnes en qui j'ai confiance e) Je peux mettre en ligne une photo de moi tant que je ne révèle aucune information personnelle me concernant	lisateurs de confiance. d) Vous ne devriez jamais mettre d'informations personnelles en ligne. Définissez votre profil comme privé, et réservez l'accès des données privées aux personnes que vous connaissez et en qui vous avez confiance. Vous pouvez utiliser votre surnom sur les sites de réseaux sociaux, pour autant que vous n'ajoutiez aucune autre information susceptible de révéler votre identité. e) Une photo de vous est une information personnelle.
9	Savez-vous à qui vous devriez signaler les contenus illicites rencontrés sur l'internet? Une ou plusieurs réponses correctes sont possibles.	a) Oui, à la Police b) Oui, au [NOM DU FOURNISSEUR DE SERVICE INTERNET] (la société qui vous fournit l'accès internet) c) Oui, au [NOM DU SERVICE D'ASSISTANCE TÉLÉPHONIQUE], une équipe qualifiée pour recevoir et réagir aux signalements concernant la présence de contenus illicites sur l'internet d) Non, je ne les signale jamais, je me contente de quitter les sites en question	a) – c) Oui, vous avez raison. Ne restez pas indifférent aux contenus illicites rencontrés sur l'internet. Des contenus impliquant par exemple des éléments de pornographie infantile, de racisme ou de xénophobie devraient être signalés au service d'assistance téléphonique actif dans votre pays, à la Police ou au fournisseur de service internet. d) Rappelez-vous que ce qui se trouve sur l'internet dépend aussi de vous. Ne soyez

N°	Question	Réponses	Commentaires
			pas indifférent aux contenus illicites qu'il vous arrive de rencontrer sur la toile.
10	Votre enfant a-t-il déjà été confronté à des contenus nocifs ou illicites sur l'internet?	a) Oui, à de nombreuses reprises b) Oui, une seule fois c) Non, jamais d) Je ne sais pas	a) et b) Pour préserver votre enfant d'un contact avec des contenus nocifs ou illicites, il faut que vous ayez installé un logiciel de filtrage sur votre ordinateur. Cela ne garantit pas une protection absolue, mais réduit néanmoins les risques d'exposition à ce genre de contenus. c) Cela fait plaisir à entendre. Si vous n'avez pas encore installé de logiciel de filtrage sur votre ordinateur, faites-le. d) Parlez à votre enfant et demandez-lui s'il/elle a déjà été confronté à des contenus qui l'ont bouleversé(e). Si vous n'avez pas encore installé de logiciel de filtrage sur votre ordinateur, faites-le.

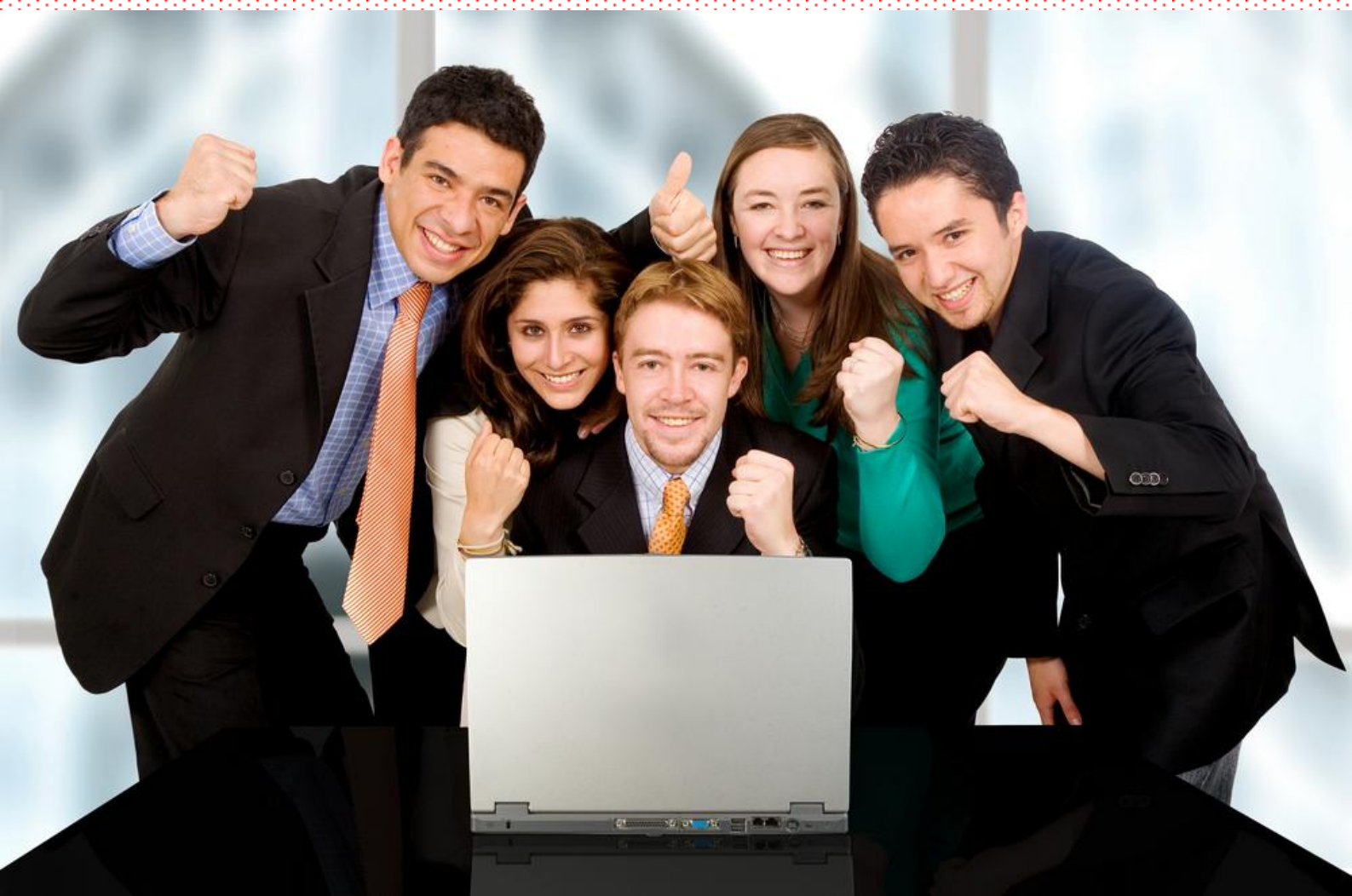
Modèles de quiz

N°	Question	Réponses	Commentaires
11	Que devrait savoir votre enfant lorsqu'il utilise le poste-à-poste?	a) Cela exclut pratiquement la réception de virus sur votre ordinateur b) Le téléchargement de certains fichiers peut être illégal c) Les échanges poste à poste peuvent comporter des contenus illicites ou nocifs d) Le partage de fichiers est plus sûr quand vous êtes équipé d'un pare-feu	a) Faux. Malheureusement, votre ordinateur peut tout aussi bien être infecté par des virus lors d'échanges poste à poste qu'à partir du web ou par le biais d'e-mails. Soyez prudent lorsque vous téléchargez de pair à pair et veillez à toujours soumettre le fichier à un programme antivirus avant de l'ouvrir (l'exécuter). b) Correct. Les matériels couverts par le droit d'auteur, tels que musiques, films ou logiciels, que vous téléchargez à partir de l'internet, sont généralement protégés de la même manière que les matériels accessibles via d'autres médias. Dans beaucoup de pays, il est illégal de télécharger des matériels couverts par le droit d'auteur. Vous devriez expliquer à votre enfant qu'avant de télécharger tout matériel placé par d'autres sur l'internet, il faut veiller à obtenir la permission des propriétaires des droits sur ce matériel, sauf exceptions ou dérogations reconnues au droit d'auteur. c) Correct. Malheureusement, le poste-à-

N°	Question	Réponses	Commentaires
			poste est également utilisé pour diffuser des contenus illicites ou nocifs. d) Correct. Avec un pare-feu installé sur votre ordinateur, vous pouvez au moins réduire le risque qu'il soit infecté par des virus. Un pare-feu est une espèce de filtre à même de screener les logiciels malveillants qui essaient d'atteindre votre ordinateur par l'internet, pour y rechercher les failles et y ouvrir une brèche.
12	Que dois-je faire, en tant que parent, si mon enfant fait l'objet de cyberintimidations lorsqu'il chatte sur l'internet? Une ou plusieurs réponses correctes sont possibles.	a) Vous encouragez votre enfant à ne pas répondre à la cyberintimidation b) Vous effacez immédiatement tous les messages ou images reçus par e-mail qui perturbent votre enfant c) Vous veillez à ce que votre enfant n'utilise que des salons de chat modérés d) Vous encouragez votre enfant à vous parler de la situation e) Vous dites à votre enfant de ne plus utiliser la messagerie électronique et la conversation en ligne pour éviter les cyberintimidations f) Vous contactez [INSÉRER POINT DE CONTACT APPROPRIÉ]	La cyberintimidation est la forme la plus récente de harcèlement, rencontrée en ligne lorsqu'on utilise l'internet ou des téléphones mobiles. a) Correct. Répondre ne mettra vraisemblablement pas fin à l'intimidation. Au contraire, le fait de répondre pourrait encourager les auteurs à poursuivre leur intimidation. b) Faux. Ne jamais effacer les messages ou images reçus par e-mail, mais les enregistrer comme preuves. c) Correct. Dans les salons de chat modérés, un adulte surveille les échanges entre participants. e) Faux. Si vous agissez de la sorte, votre enfant sera privé des opportunités fantas-

N°	Question	Réponses	Commentaires
			tiques offertes par l'internet. f) Correct. Contactez [INSÉRER POINT DE CONTACT APPROPRIÉ]. Ils aident les enfants et les jeunes confrontés à des menaces lorsqu'ils utilisent l'internet et des téléphones mobiles. **Conseils de base** • Encouragez toujours votre enfant à vous parler quand quelque chose de bouleversant ou d'effrayant lui arrive sur l'internet. • Surveillez l'activité en ligne de votre enfant pour vous assurer qu'il/elle ne communique pas avec des personnes qui l'intimident. • Apprenez à votre enfant à protéger sa vie privée en ligne**.** • Apprenez à votre enfant à ne pas répondre aux harcèlements de tous types, tels qu'e-mails négatifs et messages de chat agressifs ou offensants. Si votre enfant fait l'objet d'une cyberintimidation, signalez-le à [INSÉRER UN OU PLUSIEURS POINTS DE CONTACT APPROPRIÉS].

Quiz Utilisateurs finaux



Quiz Utilisateurs finaux

Texte introductif au Quiz Utilisateurs finaux

Bienvenue dans le Quiz de sensibilisation ENISA Spécial Utilisateurs finaux!

Le but de ce quiz est de vous fournir, en votre qualité d'utilisateur final, un moyen de tester votre sensibilisation à, et vos connaissances concernant un certain nombre d'aspects liés à l'utilisation que vous faites de l'ordinateur et des services en ligne sur l'internet.

L'internet est une ressource fantastique qui offre une quantité considérable d'informations et de services utiles. Il comporte toutefois aussi des risques dont vous devriez être conscient.

Ce quiz ne doit pas être considéré comme une autoévaluation exhaustive de votre niveau de sensibilisation et de connaissances actuel. L'objectif est plus simplement de vous donner une indication quant à votre niveau de sensibilisation et, dans le meilleur des cas, de fournir un outil susceptible de stimuler un intérêt accru pour les valeurs et les risques associés à l'utilisation de l'internet. Nous espérons également que vous trouverez intéressantes et utiles les sources d'information fournies sur ce site web.

N°	Question	Réponse	Commentaires
1	***Fichiers joints dans les e-mails*** Veuillez sélectionner ci-dessous la réponse qui, d'après vous, correspond le mieux aux risques associés aux pièces jointes des e-mails. Une ou plusieurs réponses correctes sont possibles.	1. Seuls les fichiers joints ayant l'extension .EXE posent un risque réel 2. Tous les fichiers joints sont potentiellement nocifs et peuvent contenir des virus 3. Si je connais l'expéditeur et que j'ai confiance en lui, je peux toujours ouvrir la pièce jointe 4. L'ouverture des pièces jointes est sans risques si un pare-feu est installé sur l'ordinateur 5. Un programme anti-virus réduit le risque d'être infecté par des virus contenus dans les pièces jointes aux e-mails	1. Faux. Un grand nombre et une variété importante d'autres extensions de fichiers doivent être considérés avec suspicion lorsque qu'ils sont reçus dans un e-mail. À moins de l'avoir demandée ou que vous l'attendiez, vous ne devriez pas ouvrir ce type de pièce jointe. 2. Correct. C'est malheureusement vrai. D'où l'importance, aussi, d'avoir un logiciel anti-virus installé sur votre ordinateur. 3. Faux. Même si vous connaissez et faites confiance à l'expéditeur, il peut, sans le vouloir et à son insu, vous envoyer ou vous faire suivre une pièce jointe contenant un virus. 4. Faux. Un pare-feu ne scanne pas le contenu des pièces jointes aux e-mails. 5. Correct. Les logiciels anti-virus réduisent de manière substantielle le risque d'être infecté par des virus informatiques. Même s'il ne constitue pas une garantie absolue contre les infections, il est fortement recommandé que vous investissiez dans un logiciel anti-virus.
2	***Applications anti-virus et pare-feu*** Vérifiez ce que vous savez à propos des logiciels anti-virus et des pare-feu.	1. Les logiciels anti-virus recherchent les virus sur vos disques durs et protègent votre réseau privé 2. Un pare-feu protège les ressources d'un réseau privé des utilisateurs d'autres ré-	1. Faux. Les logiciels anti-virus ne protègent pas votre réseau privé. Ils recherchent uniquement les virus sur votre ordinateur. 2. Correct. Un pare-feu est un système situé entre votre réseau informatique et l'internet.

N°	Question	Réponse	Commentaires
		seaux 3. Les logiciels anti-virus ne devraient jamais être utilisés avec un pare-feu 4. Un pare-feu recherche les virus sur vos disques durs et protège les ressources d'un réseau privé des utilisateurs d'autres réseaux 5. Les logiciels anti-virus recherchent les virus sur vos disques durs	Le pare-feu analyse les données entrant et quittant le réseau et rejette les informations provenant de sources non sécurisées et inconnues. 3. Faux. Vous devez utiliser à la fois un logiciel anti-virus et un pare-feu. 4. Faux. Un pare-feu ne recherche pas les virus. 5. Correct. Les logiciels anti-virus scannent vos disques durs et vous alertent quand des virus sont détectés. Beaucoup de logiciels anti-virus recherchent également les logiciels espions et les logiciels publicitaires.
3	***Corrections de programmes (patches) / Mises à jour de sécurité*** Quelle(s) fin(s) de phrase convient/conviennent le mieux? "Il est important d'installer les corrections de programmes sur votre ordinateur parce que…"	1. Elles rendent votre ordinateur moins vulnérable aux attaques de virus 2. Les patches éliminent les virus 3. Cela réduit le spam dans votre boîte de réception 4. Cela résout les problèmes au niveau d'un programme informatique ou de ses données de support 5. Tout ce qui précède	1. Correct. Installer les corrections de programmes sur votre ordinateur élimine les points faibles dans votre système coopératif ou vos applications, rendant ainsi votre ordinateur moins vulnérable aux attaques de virus. 2. Faux. Installer les corrections de programmes n'élimine pas les virus de votre ordinateur. Pour éliminer les virus, vous devez installer un logiciel anti-virus. 3. Faux. Un patch résout simplement une faille de sécurité dans votre système d'exploitation

N°	Question	Réponse	Commentaires
			ou vos applications. Il est sans effet sur le type d'informations que vous recevez par e-mail. 4. Correct. Un patch résout certains problèmes dans le code d'un programme informatique. 5. Faux.
4	***Mots de passe*** Quels sont, parmi les éléments suivants, ceux qui devraient être inclus dans un mot de passe sûr?	1. Votre nom 2. Une combinaison de minuscules et de majuscules 3. Votre numéro de téléphone 4. Votre plaque d'immatriculation lue à l'envers 5. N'importe quelle combinaison de lettres ou de chiffres, pour autant que le mot de passe comporte au minimum cinq caractères 6. Une combinaison d'un certain nombre de caractères alphanumériques	1. Faux. Vous ne devez pas utiliser un mot lié directement à votre identité. 2. Correct. En utilisant à la fois des minuscules et des majuscules, le nombre de combinaisons augmente, de même que la solidité de votre mot de passe. 3. Faux. Vous ne devez pas utiliser de combinaisons de caractères liées directement à votre identité. 4. Faux. Vous ne devez pas utiliser de combinaisons de caractères liées directement à votre identité, même si elles sont épelées à l'envers. 5. Faux. On considère qu'un mot de passe de cinq caractères seulement n'est pas suffisamment sûr. Il doit se composer d'au moins sept caractères et si possible, plus. 6. Correct. Un mot de passe solide est composé d'une combinaison de lettres et de chiffres, en

Modèles de quiz de sensibilisation

N°	Question	Réponse	Commentaires
			minuscules et en majuscules.
5	***Shopping en ligne sécurisé*** Qu'est-ce qui vous indique que vous êtes en train de faire du shopping en ligne de manière sécurisée?	1. Je connais la société 2. Ils vendent des produits qualitatifs de marques réputées 3. En haut de la page, il y a une bannière indiquant «Site web sécurisé» 4. L'adresse/URL du site web commence par https://... 5. Tout ce qui précède	1. Correct. Traitez toujours avec des sociétés que vous connaissez et des sites de confiance. 2. Faux. La qualité des biens proposés n'implique pas que le vendeur soit sérieux ni que le site soit sécurisé. 3. Faux. Vous ne devriez jamais vous fier uniquement à une bannière, mais vérifier effectivement la sécurisation du site web. Par exemple, contrôlez que la société a indiqué une adresse et un numéro de téléphone. Si vous avez des doutes sur la société, appelez le numéro de téléphone et posez des questions pour déterminer si l'entreprise est fiable. Vous pouvez aussi contacter [INSÉRER LE NOM D'UNE ORGANISATION / ASSOCIATION / AUTORITÉ APPROPRIÉE] pour vérifier la légitimité de la société. 4. Correct. Le "s" qui suit "http" indique que le site web est sécurisé avec SSL (Security Socket Layer), qui est une méthode de sécurisa-

N°	Question	Réponse	Commentaires
			tion par chiffrement de la connexion entre vous et le serveur web de la société. En outre, vous devez vérifier la présence, en bas de l'écran, d'un cadenas fermé. Si le cadenas est ouvert, vous devez considérer qu'il ne s'agit pas d'un site sécurisé. 5. Faux. Seules les réponses 1 et 4 sont correctes. **Conseils de base** • Achetez auprès de sociétés que connaissez. • Vérifier que la connexion est toujours sécurisée avec SSL. • Lisez les politiques du site en matière de protection de la vie privée et de sécurité pour savoir comment la société traite les informations sensibles comme les numéros des cartes de crédit et les données personnelles. • Imprimez toujours des copies de vos commandes. • Connaissez vos droits. Vos transactions en ligne sont régies par la législation [AJOUTER DES INFORMATIONS SUR LES LOIS, RÉGLEMENTATIONS, ETC. EN VIGUEUR

N°	Question	Réponse	Commentaires
			PROTÉGEANT L'UTILISATEUR DE CARTES DE CRÉDIT LORS DU SHOPPING EN LIGNE].
6	***Hameçonnage*** Testez vos connaissances sur les tentatives d'hameçonnage et les façons de vous protéger.	1. La société légitime mentionnée dans l'e-mail apparaît bien dans le champ «Envoyé par» 2. Si j'utilise un logiciel anti-virus, je suis à l'abri des tentatives d'hameçonnage 3. En général, ils demandent des informations personnelles telles que noms d'utilisateur, mots de passe et numéros de cartes de crédit 4. Les e-mails contenant des liens/URL vers des adresses web sont plus dangereux que les autres 5. En général, l'expéditeur demande que vous répondiez dans les quelques jours qui suivent 6. Tout ce qui précède	1. Correct. Rappelez-vous comme il est simple de modifier les informations de ce champ dans n'importe quel e-mail client. 2. Faux. L'utilisation d'un logiciel anti-virus réduit toutefois le risque d'infection virale et peut vous avertir si un message contient des liens ou des pièces jointes. 3. Correct. Rappelez-vous, les banques et les sociétés légitimes ne vous demandent jamais de communiquer des informations personnelles par e-mail ni de modifier vos justificatifs d'identité tels que noms d'utilisateur ou mots de passe. Si vous recevez une telle demande, effacez immédiatement l'e-mail de votre boîte de réception et de la poubelle de votre messagerie afin d'éviter tout clic malencontreux. 4. Correct. Vous ne devez jamais cliquer sur les liens incorporés dans le texte de l'e-mail. Dans une tentative d'hameçonnage, le texte du lien ne correspond pas à un site web légitime. Restez toutefois vigilant face à tout message vous demandant de communiquer des informations

N°	Question	Réponse	Commentaires
			sensibles. 5. Faux. Dans la plupart des cas, les hameçonneurs veulent que vous réagissiez immédiatement. Considérez ce genre de démarche comme un signal d'alarme. 6. Faux. Seules les réponses 1, 3 et 4 sont correctes. **Conseils de base:** En suivant l'approche LIST, vous réduirez à coup sûr le risque d'être victime d'une tentative d'hameçonnage. Posez-vous ces questions lorsque vous recevez des e-mails suspects. **Légitimité:** La demande semble-t-elle légitime et habituelle? Par exemple, est-il naturel qu'on vous demande cette information, et comment serait-il normal que vous la fournissiez? **Importance**: Quelle est la valeur de l'information qu'il vous est demandé de fournir ou de la tâche qu'il vous est demandé d'exécuter, et quels pourraient en être les usages abusifs? **Source**: Croyez-vous vraiment que la source de la demande est authentique? Pouvez-vous trouver un moyen de le vérifier? **Timing**: Devez-vous répondre aussitôt? Si vous avez toujours des doutes, prenez le temps de

N°	Question	Réponse	Commentaires
			faire des vérifications ou demandez de l'aide. Si vous recevez un e-mail et que vous croyez qu'il s'agit d'une tentative d'hameçonnage, veuillez contacter: [INSÉRER LE NOM D'UNE ORGANISATION / ASSOCIATION / AUTORITÉ APPROPRIÉE].
7	***Back-Up*** Vérifiez ce que vous savez à propos de la sauvegarde des données.	1. Vous ne devez sauvegarder que les photos que vous stockez sur l'ordinateur 2. Toute information que vous estimez importante doit être sauvegardée 3. Les fichiers que je n'envisage pas de modifier à l'avenir ne doivent être sauvegardés qu'une seule fois 4. Vous ne devriez jamais utiliser un CD-RW comme support de stockage externe 5. Vos fichiers de sauvegarde doivent se trouver dans la même pièce que les fichiers originaux au cas où vous en auriez besoin	1. Faux. Vous devez sauvegarder tous les fichiers qui ont de l'importance pour vous. 2. Correct. Par exemple: • Photos • Logiciels ou musiques que vous avez achetés ou téléchargés à partir de l'internet. • Annuaire e-mail • E-mails et courriers. 3. Correct. Toutefois, plus vous avez de copies de sauvegarde, mieux c'est. 4. Faux. Les CD-RW sont un excellent support de stockage. Ils peuvent emmagasiner des volumes relativement importants de données et sont très abordables à l'achat. Il existe beaucoup d'autres supports de stockage, chacun avec leurs avantages et désavantages, par exemple:

N°	Question	Réponse	Commentaires
			• Disques extérieurs • Clés USB à mémoire flash • Back-Up et stockage en ligne. 5. Faux. Il vaut toujours mieux conserver vos copies de sauvegarde dans une autre pièce que celle où se trouve votre ordinateur. Idéalement, vous devriez avoir plusieurs copies de sauvegarde conservées dans des endroits distincts. Si vous conservez par exemple des documents importants dans un coffre bancaire, vous devriez aussi y déposer un back-up de vos fichiers.
8	***Clés USB à mémoire flash*** Les clés USB à mémoire flash sont un support de stockage de plus en plus populaire pour les données. Mais êtes-vous au fait des risques et des inconvénients qui leur sont associés?	1. Elles ne conviennent pas pour le stockage de photos 2. Elles peuvent contenir des virus 3. Elles sont onéreuses au vu de leur capacité de stockage 4. Elles s'égarent ou se perdent facilement 5. Les clés USB à mémoire flash constituent une modalité de stockage sûre car elles sont chiffrées	1. Faux. Comme sur un disque dur, vous pouvez stocker n'importe quel type de fichiers sur une clé USB à mémoire flash. C'est un des avantages offerts par les clés USB à mémoire flash. 2. Correct. Avant d'utiliser une clé USB à mémoire flash pour la première fois, vous devez la soumettre à un scan anti-virus. Vous devriez également le faire après avoir copié des fichiers à partir d'un ordinateur dont vous n'êtes pas absolument sûr. 3. Faux. Un des principaux avantages des clés USB à mémoire flash est leur prix relativement bas au regard de la capacité de stockage offerte.

N°	Question	Réponse	Commentaires
			4. Correct. Leur taille compacte, qui est parfois un avantage, les rend aussi fatalement plus faciles à égarer ou à perdre. 5. Faux. Normalement, les clés USB à mémoire flash ne sont pas fournies avec une fonctionnalité de chiffrement. Pour protéger les données, vous devez encrypter vous-même les fichiers stockés sur les clés USB à mémoire flash en utilisant un matériel ou logiciel de chiffrement. Si vous perdez votre clé, personne ne pourra alors récupérer les données qu'elle contient. Si vous disposez aussi en parallèle d'un autre back-up de ces fichiers, vous ne risquez plus de perdre des informations importantes.
9	***Chiffrement*** Le chiffrement, ou encryptage, offre un moyen de protéger les informations, mais que savez-vous à ce sujet?	1. Le chiffrement est onéreux pour les utilisateurs domestiques 2. De manière générale, les fichiers chiffrés ne peuvent pas être lus par d'autres personnes 3. Toutes les données ne se prêtent pas à l'encryptage 4. Les e-mails ne doivent pas être encryptés, à moins qu'ils ne soient envoyés avec des pièces jointes 5. Le chiffrement protège la confidentialité des	1. Faux. Un logiciel de chiffrement n'est pas nécessairement coûteux. Il existe même des logiciels de chiffrement gratuits. Lorsque vous choisissez un logiciel de chiffrement, assurez-vous que le code source est publiquement disponible. Cela permet aux experts en programmation et chiffrement de l'examiner pour détecter les "portes dérobées" et les bogues. 2. Correct. Le logiciel de chiffrement de fichiers le plus populaire utilise des algorithmes très puissants qui sont virtuellement impossibles à

N°	Question	Réponse	Commentaires
		informations	craquer. 3. Faux. Toutes les données peuvent être encryptées. Certains logiciels de chiffrement ne sont toutefois destinés qu'à l'encryptage des e-mails alors que d'autres réalisent aussi le chiffrement des fichiers et même des disques durs. 4. Faux. C'est vous qui décidez des types de données qui seront encryptés. 5. Correct. Le chiffrement est une méthode qui protège contre la divulgation non autorisée des informations.
10	***Téléchargement de fichiers*** L'internet constitue une ressource phénoménale avec toutes ces informations disponibles d'un simple clic. Mais êtes-vous conscient de l'aspect «droit d'auteur» associé au téléchargement de fichiers?	1. Il est illégal de télécharger sans autorisation des matériels publiés et protégés par le droit d'auteur 2. Il est illégal de télécharger sans autorisation des matériels couverts par le droit d'auteur 3. Il est légal de télécharger de la musique aussi longtemps qu'elle n'est pas au format MP3 4. Il est illégal de partager/mettre sur le net sans autorisation des matériels publiés et protégés par le droit d'auteur 5. Les logiciels ne sont pas couverts par le droit d'auteur, seuls les textes, les mu-	[LES COMMENTAIRES DES RÉPONSES DOIVENT ÊTRE AJOUTÉS ET ADAPTÉS EN FONCTION DES LOIS APPLICABLES DANS VOTRE PAYS]. 1. 2. 3. 4. 5.

Modèles de quiz de sensibilisation

N°	Question	Réponse	Commentaires
		siques, les photos et les films le sont	

Quiz PME

Modèles de quiz

Texte introductif au Quiz PME

Bienvenue dans le Quiz de sensibilisation ENISA Spécial Cadres supérieurs PME!

Le but de ce quiz est de vous fournir, en votre qualité de cadre supérieur d'une petite ou moyenne entreprise, un moyen de tester votre sensibilisation à, et vos connaissances concernant un certain nombre d'aspects liés à votre utilisation de l'ordinateur et de l'internet en tant qu'outils au service de vos activités professionnelles. Ces outils sont précieux en cela qu'ils accroissent la capacité de votre entreprise à communiquer et à être compétitive sur le marché européen et mondial. Ils comportent toutefois aussi des risques, dont il convient que vous soyez conscient.

Ce quiz ne doit pas être considéré comme une autoévaluation exhaustive de votre niveau de sensibilisation et de connaissances actuel. L'objectif est plus simplement de vous donner une indication quant à votre niveau de sensibilisation et, dans le meilleur des cas, de fournir un outil susceptible de stimuler un intérêt accru pour les aspects importants et les risques associés à l'utilisation de l'internet. Nous espérons également que vous trouverez intéressantes et utiles les sources d'information fournies sur ce site web.

Profil de risque

La gestion de la sécurité des réseaux et de l'information relève fondamentalement de la gestion du risque, et à ce titre, elle postule que l'on identifie les actifs importants de l'entreprise qui pourraient être compromis par des failles des systèmes informatiques. Outre les processus de production, l'information est un actif de grande valeur qui peut être aisément mis en péril par les défaillances des systèmes informatiques.

Parmi les informations de valeur figurent, par exemple, les bases de données regroupant les informations des fournisseurs et les annuaires rassemblant les données clients (également sur les appareils mobiles), les informations financières, les modèles industriels et les plans d'activité commerciale. L'information est un actif et en tant que tel, elle est exposée à de nombreuses menaces, telles que risques naturels, criminalité, défaillances des systèmes et erreurs humaines.

N°	Question	Réponses	Commentaires
1	Savez-vous quelles informations importantes sont traitées sur vos systèmes informatiques, et où?	a) Oui, nous disposons d'un inventaire détaillé des informations importantes, que nous utilisons p.ex. pour les back-ups b) Oui, nous savons que certains systèmes sont cruciaux parce qu'ils traitent des informations de grande importance c) Non, nous savons qu'il y a des informations importantes sur nos systèmes, mais nous ne savons pas exactement lesquelles et où d) Non, nous n'avons pas vraiment d'informations de grande importance dans nos systèmes e) Je ne sais pas	Une connaissance détaillée des informations importantes traitées sur les systèmes informatiques est à la base d'une gestion correcte du risque. Cette connaissance permet une implémentation adéquate des contrôles (p.ex. mécanismes de protection) et des investissements efficaces. Connaissez votre ennemi. Vous serez alors à même d'investir dans les contre-mesures les plus adéquates.

N°	Question	Réponses	Commentaires
2	Quels sont, parmi les acteurs suivants, ceux qui représentent la plus grande menace pour vos informations d'entreprise?	a) Les concurrents, car la concurrence est très forte sur ce marché b) Les partenaires, parce les données doivent être partagées avec de nombreux intervenants c) Les criminels, parce que ma société développe des activités commerciales pour les personnes d) Les employés, parce qu'ils peuvent provoquer une fuite d'information de manière intentionnelle ou non e) Aucun f) Je ne sais pas	

Aspects juridiques et contractuels

Tout cadre supérieur doit respecter la loi et se conformer aux obligations légales. En matière de sécurité des réseaux et de l'information, plusieurs lois européennes et/ou nationales doivent être prises en considération et appliquées ensuite aux activités de l'entreprise. Connaissez-vous vos responsabilités juridiques concernant la sécurité de l'information?

N°	Question	Réponses	Commentaires
3	Êtes-vous au fait des règlementations sur la protection de la vie privée applicables dans votre pays / en Europe (concernant les données clients)? Êtes-vous conscient de leur impact sur le management informatique?	a) Oui, ce processus est sous contrôle b) Non, nous ne nous occupons pas de ce genre d'aspects juridiques c) En partie, un chantier d'amélioration a été mis en œuvre récemment d) Je ne sais pas	La conformité aux dispositions réglementaires concernant la sécurité des réseaux et de l'information ne cesse de gagner en importance. Les cadres supérieurs doivent être conscients de leurs responsabilités juridiques en la matière. La protection des données personnelles et la gestion des licences logicielles sont fondamentales dans ce domaine. En cas d'externalisation, les obligations des sous-traitants doivent être clairement définies dans des contrats. Est notamment visée la manipulation durant les activités de maintenance des données sensibles présentes dans les systèmes informatiques.
4	Êtes-vous au fait des règlementations sur le droit d'auteur applicables dans votre pays / en Europe (concernant les logiciels et les contenus numériques)?	a) Oui, ce processus est sous contrôle b) Non, nous ne nous occupons pas de ce genre d'aspects juridiques c) En partie, un chantier d'amélioration a été mis en œuvre récemment d) Je ne sais pas	
5	Avez-vous prévu des obligations contractuelles pour protéger la sécurité des réseaux et de l'information lorsque vos systèmes sont sous-traités, p.ex. pour la maintenance?	a) Oui, ce processus est sous contrôle b) Non, nous ne sous-traitons pas c) En partie, un chantier d'amélioration a été mis en œuvre récemment d) Je ne sais pas	

Aspects humains et organisationnels

Les outils de sécurité sont très utiles pour protéger les réseaux et les systèmes d'information. Il n'en reste pas moins que, comme dans le cas de la conduite automobile, seul le comportement des conducteurs peut réduire sérieusement le taux d'accidents. Vos employés devraient donc être sensibilisés à, et avoir une compréhension de base de la manière dont les informations et les ordinateurs doivent être traités.

Comment, dans votre entreprise, la politique de sécurité de l'information reflète-t-elle (de manière explicite ou implicite) les questions ci-dessous?

N°	Question	Réponses	Commentaires
6	Le mot de passe que vous utilisez pour accéder à vos données d'entreprise est connu:	a) De vous seul b) De quelques collègues c) Par un administrateur système d) Par des membres de la famille	Le fait d'adopter un certain nombre d'attitudes de base et d'être attentif à quelques situations à risque peut réduire considérablement les risques pesant sur la sécurité de l'information. Les cadres supérieurs jouent un rôle important dans le développement d'une culture de sécurité de l'information dans la mesure où ils doivent montrer l'exemple. À l'instar d'un pays étranger, l'internet est un nouvel environnement: dans lequel vous devez développer l'attitude adéquate qui aidera à prévenir les fraudes et les risques. Commencez par définir une politique de sécurité. Vous trouverez ici plus d'informations à ce sujet: [AJOUTER PLUS D'INFORMATIONS ET/OU INSÉRER DES LIENS PERMETTANT D'ACCÉDER À PLUS D'INFORMATIONS]
7	Utilisez-vous votre webmail privé à des fins professionnelles?	a) Jamais b) Parfois c) Fréquemment d) Chaque jour	
8	Traitez-vous de questions professionnelles sur des réseaux sociaux ou des groupes de news?	a) Jamais b) Parfois c) Fréquemment d) Chaque jour	
9	Comment réagissez-vous si vous recevez un appel téléphonique ou un e-mail vous demandant de communiquer des informations d'entreprise?	a) Je ne réponds jamais b) Je réponds aux questions qu'on me pose c) Je demande des détails avant de répondre d) Je prends conseil auprès d'un collègue ou d'un ami e) Je ne sais pas	
10	Vos appareils mobiles (PDA, ordinateurs portables, clés USB) sont-ils toujours sous contrôle et surveillés quand ils ne sont pas utilisés?	a) Oui b) Non c) Parfois d) Je ne dispose pas de ce genre d'appareils e) Je ne sais pas	

Outils de sécurité

Une fois les actifs informationnels identifiés, quelques techniques de base peuvent les protéger efficacement. Des attaques de virus ou de logiciels espions, une intrusion sur le réseau ou des vols/divulgations d'informations risquent en effet d'exercer un impact sur les activités de l'entreprise.

Êtes-vous au fait des outils de sécurité qui visent à protéger les appareils et les informations sensibles?

N°	Question	Réponses	Commentaires
11	La sauvegarde des données sensibles a lieu:	a) Tous les jours b) Toutes les semaines c) Tous les mois d) Jamais e) Je ne sais pas	Certaines solutions de base protègent de manière satisfaisante les systèmes d'information des entreprises. Ceux qui sont cités dans les questions sont aujourd'hui faciles à utiliser et économiques. Ne pas les utiliser augmentera considérablement le risque de défaillance des systèmes et de préjudices pourtant facilement évitables.
12	Des logiciels anti-virus et anti-spyware sont installés et mis à jour:	a) Sur les PC b) Sur les ordinateurs portables c) Sur les serveurs de fichiers d) Sur les serveurs de messagerie e) Je ne sais pas	
13	Des accès à distance sécurisés sont installés sur les PDA et les ordinateurs portables (VPN et authentification forte)	a) Oui b) Non c) En cours d) Je ne sais pas	

N°	Question	Réponses	Commentaires
14	Le chiffrement est utilisé pour encrypter:	a) Données sur les PC b) Données sur ordinateurs portables, PDA et autres appareils mobiles c) Données sur les serveurs de fichiers d) E-mails e) Je ne sais pas	

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu