SOYEZ acteur DE LA SÉCURITÉ DE L'INFORMATION

Normandie Université

Réponses du QCM final (Session 2)

Q1 : Pour vous, l'information sensible d'une entreprise, est-ce seulement ?

a) L'information qui est connue uniquement de la Direction de cette entreprise

b) L'information signalée par la Défense Nationale.

c) L'information dont la divulgation peut mettre l'entreprise en difficulté.

d) Ce qui touche au secret de fabrication.

R1 : c. L'information sensible est celle dont la divulgation peut mettre l'entreprise en difficulté. Nous disposons tous de données sensibles.

Q2 : Quelle est la meilleure façon de savoir si une information est sensible ?

a) Si la mention « Confidentiel » figure sur le papier d'impression ou sur le répertoire informatique.

b) Si elle m'a été donnée par un directeur.

c) Si elle vous parait bizarre.

R2 : a. Le marquage systématique des documents ou répertoires informatiques en fonction du niveau de sensibilité permet à l'utilisateur d'adapter les mesures de protection. Un document confidentiel ne sera pas mis à la poubelle papier avant d'avoir été broyé.

Q3 : Un mail de ma banque m'avertit que mon compte a été débité de 78 euros par erreur. Pour me faire rembourser, je suis invité à cliquer sur le lien dans le message afin de confirmer mes coordonnées de compte. Quel est le piège à éviter ?

a) Je clique sur le lien et je tombe sur le site de ma banque avec les cases à remplir. Je les remplis, c'est très simple.

b) Je vais sur le site de ma banque en utilisant mes favoris dans mon navigateur pour voir ce qu'il en est.

c) Je détruis le mail sans me soucier de la mise à jour de mes données bancaires.

d) Je téléphone à ma banque et je traite cela par téléphone.

R3 : a. Le piège à éviter est de cliquer sur le lien et de remplir les cases car le site en question n'est pas le site de ma banque mais bien un site contrefait. Cela s'appelle du phishing ou hameçonnage. Il n'y a pas de piège dans les autres propositions de réponse.

Q4 : Mon fils a téléchargé un petit jeu sympa sur Internet que j'amènerais bien au bureau pour montrer aux collègues. Quelle est la meilleure attitude à adopter ?

a) Je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus à la maison.

b) Je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus au bureau.

c) Je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus à la maison ET au bureau.

d) Tout bien réfléchi, je ne l'amène pas au bureau.

R4 : d. Le jeu peut contenir un programme qui fait tout autre chose et n'est pas identifié comme un virus.

Q5 : Je visite des sites Internet pour mon plaisir, mais je crains de récupérer un code malfaisant. Qu'est-ce qui sera le moins risqué ?

a. Télécharger des images

b. Télécharger des logiciels de jeu

c. Visualiser des films

d. Copier/coller les textes dans un logiciel de traitement de texte

R5 : d. Copier/coller un texte évite bien sûr la récupération d'un code malfaisant. Les autres activités peuvent télécharger des logiciels malfaisants. Attention toutefois aux problèmes de droits d'auteur.

Q6 : Je décide de faire un blog sur Internet, pour me défouler un peu. Quelle est la meilleure attitude à adopter ?

a. Je peux enfin donner des noms d'oiseaux à un voisin que je ne supporte pas.

b. Je dois faire attention à ce que j'y mets, certains écrits tombent sous le coup de la loi.

c. Je peux faire un blog anonyme, je ne suis pas en cause si des gens se reconnaissent.

d. Je peux y mettre des blagues sur les blondes, après tout, tout le monde le fait.

R6 : b. Les contenus injurieux, racistes, etc. sont illégaux, il faut faire attention à ce que l'on publie.

Q7 : Je quitte mon poste de travail pour aller déjeuner. Je sais qu'il est recommandé de verrouiller ma session mais j'ai oublié de le faire et j'ai la paresse de revenir depuis le restaurant uniquement pour ça. Est-ce vraiment très imprudent?

a. Oui, parce que l'ordinateur reste actif sous tension et consomme davantage d'électricité.

b. Non, parce que l'ordinateur se verrouille automatiquement au bout d'un certain temps.

c. Non, parce que si je ne suis pas là, je ne suis pas responsable de ce que ferait un visiteur.

d. Oui, parce que n'importe qui aura accès à mes applications et données et en plus s'il fait quelque chose d'illégal, ma responsabilité peut être engagée.

R7 : d. Même si l'ordinateur se verrouille au bout d'un certain temps, ce délai peut être suffisant pour un intrus mal intentionné ou simplement curieux. D'autant plus quand vous vous connectez sur des ordinateurs partagés.

Q8 : Le service informatique de mon entreprise m'a attribué un ordinateur portable pour mon travail c'est pratique. Quelle est la phrase fausse ?

a. Je peux y mettre des données personnelles (photos, ...).

b. Je peux l'apporter à la maison pour travailler dessus en local.

c. Quand j'utilise Internet à la maison sur mon abonnement personnel, les outils de sécurité installés sur l'ordinateur me protègent aussi bien que lorsque je l'utilise au bureau.

d. Je ne laisse personne d'autre que moi utiliser cet ordinateur.

R8 : c. L'affirmation c. est fausse car certains outils de sécurité de votre entreprise ne sont pas dans l'ordinateur. Les autres propositions sont vraies : je peux mettre des données personnelles sur un ordinateur portable professionnel, je peux l'apporter à la maison et personne d'autre que moi ne doit utiliser cet ordinateur.

Q9 : Je reçois un mail d'une personne que je ne connais pas, qui me demande poliment de donner mon avis sur un produit dans le cadre d'une étude de marché. La description du produit est dans un fichier joint: «produit.doc». Quelle est la meilleure attitude à adopter ?

a. Je détruis le mail sans lire la pièce jointe.

b. J'ouvre la pièce jointe pour voir s'il s'agit bien d'une étude de marché.

c. Comme il s'agit d'un fichier «.doc », c'est un document Word, donc je ne crains rien en l'ouvrant.

d. Je renvoie un mail à l'auteur pour avoir plus de détails et vérifier qu'il s'agit bien d'une étude de marché.

R9 : a. Une pièce jointe qu'on n'attend pas est toujours suspecte, y compris un fichier Word qui peut contenir des macros (ou macro-instructions). Envoyer un mail ne fait que confirmer à un inconnu que notre adresse mail est valide.

Q10 : A votre avis, la sécurité de l'information concerne qui ?

a. Seulement les informaticiens.

b. Uniquement les entreprises et administrations du domaine de la Défense.

c. Exclusivement les entreprises qui ont un secret de fabrication.

d. Toutes les organisations.

R10 : d. Toutes les organisations ont des informations à protéger. Dans un environnement professionnel, il faut que chacun se pose la question suivante : "Quelles sont les informations que je crains le plus de perdre, celles sans lesquelles je ne pourrais plus faire mon travail ?". La réponse à cette question permet ensuite de mettre en place des mesures de protection adéquates (sauvegardes par exemple). Et puis chaque organisation possède des données à caractère personnel que la loi impose de protéger.

Q11 : Un employé est fortement soupçonné par sa hiérarchie de stocker des fichiers illicites dans son espace disque privé. Quelle est l'affirmation vraie ?

a. Dans le cadre d'une instruction pénale ou par une décision de justice, un juge peut prendre une ordonnance afin de désigner un huissier de justice pour accéder à cet espace personnel.

b. Sa direction peut mettre en place un logiciel de surveillance de ses mails et de ses accès Internet, sans le lui dire.

c. Sa direction peut demander à l'administrateur système d'inspecter l'espace privé de cet employé pour y trouver des preuves.

d. Sa direction peut lui demander son mot de passe et l'utiliser pour lire ses données en son absence.

R11 : a. La direction de l'employé peut accéder aux espaces professionnels mais ne peut pas accéder à l'espace étiqueté "privé" de l'employé. En général ceci est défini dans la charte informatique de l'entreprise et concerne le droit à la vie privée résiduelle.

Q12: Les services ressources humaines de mon entreprise ont dans leurs bases, des informations me concernant : mon adresse personnelle, le pourcentage de handicap de mes enfants, etc. Quelle est l'affirmation fausse ?

a. Je peux demander à vérifier et modifier ces données n'importe quand.

b. L'INSEE (Institut National de la Statistique et des Études Économiques) , en tant qu'organisme d'État, peut utiliser ces données dans le cadre d'études statistiques.

c. Mon entreprise peut utiliser ces données pour ses propres statistiques, à condition de m'en avertir.

d. Le directeur de mon entreprise peut avoir accès à l'ensemble des données (hors données de santé).

R12 : b. La proposition b. est fausse : si cet usage n'a pas été explicitement prévu et que je n'en ai pas été averti, l'INSEE ne pourra pas utiliser ces données. Les autres affirmations sont vraies.

Q13 : Quelle est la meilleure manière pour protéger l'information confidentielle ?

a. Un bon anti-virus sur mon ordinateur.

b. Un bon système de chiffrement du disque dur de mon ordinateur.

c. Un pare-feu (firewall) efficace et surtout bien configuré sur mon ordinateur.

d. Aucune des techniques ci-dessus ne répond totalement au besoin.

R13 : d. Il ne suffit pas de mettre en place des mesures techniques (antivirus, pare-feu, chiffrement) pour protéger l'information confidentielle mais il faut aussi se protéger par des mesures organisationnelles et de sensibilisation. Un bon système de chiffrement protège éventuellement l'information numérique stockée ou transmise, mais ne protège pas de la fuite de connaissance ou de documents confidentiels sur papier. La question mériterait sans doute d'être reformulée.

Q14 : Un employé désire récupérer à bas prix les outils de traitement de texte utilisés dans sa société. Quelle est la meilleure solution ?

a. Lui faire une copie du logiciel en dehors de heures de bureau, ça ne laisse pas de trace.

b. Le laisser faire une copie à sa guise, du moment que personne ne le sait.

c. Lui proposer des outils libres disponibles en téléchargement.

d. Faire faire une copie du logiciel par le service informatique, ils sauront faire ça discrètement.

R14 : c. C'est la seule solution légale. Il faut l'informer des possibilités offertes par les logiciels libres qui couvriront la majorité de ses besoins.

Q15 : Je reçois un mail m'annonçant que je peux gagner une caisse de champagne. Il suffit d'envoyer un mail à l'adresse qui apparaît dans le message : promochampagne@acces.com. Quelle est la bonne attitude à adopter ?

a. J'envoie un mail le plus vite possible en cliquant sur l'adresse dans le message, je n'ai rien à perdre.

b. C'est sûrement une blague et je réponds à l'expéditeur en lui disant ma façon de penser.

c. Je recopie l'adresse dans ma messagerie et j'envoie un mail pour participer.

d. Je ne réponds pas et je détruis le mail.

R15 : d. Répondre ne ferait que confirmer que mon adresse mail est valide, ce qui est le but recherché par l'attaquant. Si je sais le faire, j'apprends au logiciel de messagerie qu'il s'agit d'un courrier indésirable ou spam. Et je déclare ce mail aux sites qui référencent les phishing.

Q16 : Selon vous, un virus informatique

a. ne peut être réalisé que dans un laboratoire combinant biochimie et informatique.

b. est nécessairement originaire de l'étranger.

c. est un simple programme informatique.

d. nécessite, pour être mis au point, des connaissances en physique quantique.

R16 : c. Un virus informatique n'est pas compliqué à réaliser, il faut donc adopter les bonnes pratiques pour les éviter.

Q17 : Je parle couramment la langue Inuit du Canada. Un mot Inuit sera un excellent mot de passe ! Avant que quelqu'un le devine, il se passera du temps. Cette affirmation est-elle ?

a. Vraie

b. Fausse

R17: b. Les logiciels de cassage de mots de passe contiennent tous les dictionnaires.

Q18 : J'utilise un système d'échange de musique « peer to peer », quelle est la meilleure réponse ?

a. Je ne risque rien car le système est largement répandu.

b. Je mets à la disposition de la communauté d'échange uniquement le répertoire que j'ai spécifié, mes autres données ne risquent rien.

c. Avec un anti-virus, je ne risque rien.

d. Je pars du principe que l'ensemble des données de mon ordinateur peuvent être visibles de l'extérieur.

R18 : d. Le simple fait d'utiliser un système d'échange « peer to peer » expose votre ordinateur aux yeux du monde. En cas de problème avec le logiciel utilisé ou si vous ne maîtrisez pas la configuration du logiciel, vos données personnelles pourraient être visibles de tous.

Q19 : L'administrateur système du service informatique de mon entreprise me demande mon mot de passe au téléphone, pour faire des travaux de maintenance. Quelle est la meilleure attitude à adopter ?

a. Je ne le lui donne pas

b. Je vérifie qu'il s'agit bien de l'administrateur, je le lui donne et je le change juste après.

c. Je le lui donne, mais pas au téléphone, seulement de vive voix.

d. Je le lui donne : l'administrateur a tous les droits. Lui refuser c'est prendre beaucoup de précautions pour pas grand-chose.

R19 : a. La meilleure attitude est de ne pas donner son mot de passe à l'administrateur système. Il n'en a pas besoin, le sien lui donne des droits plus importants que le vôtre. Une demande de mot de passe par téléphone constitue un incident de sécurité qui mérite d'être signalé.

Q20 : Mon fils de 15 ans, bricoleur Internet, a réussi à contourner les défenses informatiques de l'entreprise Grosbras et Fils et a laissé un petit message dans le système pour montrer qu'il est possible d'y pénétrer. Quelle est l'affirmation vraie ?

a. C'est un passe-temps comme un autre, comme il est mineur ce n'est pas grave.

b. Il n'a pas laissé son nom, il n'a aucun risque d'être démasqué.

c. L'entreprise peut porter plainte.

d. Comme il n'y a pas eu destruction de système ou de données, ni de vol d'information, il n'y a rien d'illégal dans cette action.

R20 : c. L'intrusion, voire même la tentative d'intrusion, est condamnée par la loi Godfrain.
Voir aussi article 323.1. du code pénal.

Q21 : A votre avis, qui, dans un service de recherche et développement, est le plus susceptible d'être la cible d'action d'espionnage ?

a. Le directeur du service

b. Les ingénieurs

c. Tout le monde y compris les agents d'entretien

d. Les assistantes

R21 : c. Toute personne ayant accès aux locaux ou à des informations de l'entreprise peut être la cible d'action d'espionnage.

Q22 : Quelle est la meilleure façon de ne pas se faire piéger par des gens qui vous «font parler » ?

a. Considérer tout son entourage comme suspect.

b. Bien identifier l'information sensible pour ne jamais en parler.

c. Se méfier des gens qui vous proposent à boire.

d. Éviter de se faire inviter au restaurant ou dans des soirées.

R22: b. Les autres choix feront de vous un vrai paranoïaque, pas très efficace.

Q23 : Selon vous, l'espionnage économique

a. Concerne toutes les entreprises, les laboratoires de recherche, ...

b. Est peu présent dans la réalité.

c. Ne vise que les entreprises de Défense.

d. Ne concerne vraiment que les grands groupes industriels.

R23 : a. L'espionnage économique concerne toutes les entreprises. Toute entreprise peut être espionnée par exemple par un concurrent pour récupérer des fichiers clients ou pour connaître les prix pratiqués et proposer des prix plus bas.

Q24 : Je suis seul au bureau et personne ne peut m'entendre parler. Je suis appelé au téléphone par un cabinet de recrutement qui cherche un profil qui ressemble au mien. J'ai bien envie de voir si c'est une bonne opportunité pour moi. Quelle est l'attitude à adopter ?

a. Je note leur nom et celui de la personne qui appelle, et je les rappelle ultérieurement après avoir cherché leur numéro dans les pages jaunes.

b. Je discute avec eux pour en savoir un peu plus sur leurs intentions, je prends leur e-mail et je leur envoie mon CV par mail.

c. Je creuse un peu la question en demandant des informations précises sur le poste et je leur envoie mon CV par courrier.

d. Je leur donne toutes les informations pertinentes par téléphone car je ne souhaite pas qu'il y ait une trace d'envoi par la poste ou par e-mail.

R24 : a. Pour s'assurer qu'il ne s'agit pas d'un faux recruteur, il faut vérifier les coordonnées du cabinet de recrutement par un autre moyen (pages jaunes ou autre, les pages jaunes étaient un exemple). Le faux recrutement est une technique classique pour obtenir facilement de l'information sensible sur les activités de votre société. Communiquer des informations sur vos activités professionnelles par téléphone, mail ou courrier papier à une personne non identifiée peut avoir de graves conséquences pour votre entreprise.

Q25 : Je réalise des achats en ligne, au moment du paiement le site marchand me demande de saisir les informations de ma carte bancaire (nom, numéro de carte, date de validité et les 3 chiffres du cryptogramme). Quelle est la vérification la moins efficace pour éviter un site malveillant ?

a. Vérifier la présence du cadenas dans la barre d'adresse de mon navigateur Internet ou en bas à droite de la fenêtre.

b. S'assurer que la mention https:// apparaît au début de l'adresse du site Internet.

c. Regarder les avis des internautes sur le site marchand.

d. Vérifier la réputation du site marchand en faisant des recherches sur Internet et en vérifiant les mentions légales du site.

R25 : c. La vérification la moins efficace est de regarder les avis des internautes sur le site marchand. En effet un site malveillant pourra produire lui-même de faux avis positifs pour tromper ses clients. Les trois autres vérifications sont à faire avant de procéder au paiement.

Q26 : Un technicien que je ne connais pas vient entretenir le radiateur de mon bureau. Quelle est la meilleure attitude à adopter ?

a. Je quitte mon bureau pour qu'il puisse travailler tranquillement.

b. Je vais lui chercher un café pour le remercier.

c. Je lui demande pour quelle société il travaille.

d. Je contacte mon service maintenance pour m'assurer que le technicien est bien habilité à intervenir.

R26 : d. Rien ne prouve que ce technicien n'est pas là pour voler de l'information. Il ne faut pas le laisser seul. Il faut prévenir le service concerné.

Q27 : Votre ami vous dit : « Avec les réseaux sociaux, je suis prudent : pas de données professionnelles sur Facebook, je les réserve à Viadeo ou LinkedIn. Quelle est la seule information vraie ?

a. Facebook présente toutes les garanties de confidentialité : du moment que vous activez les verrouillages appropriés, vos données ne seront jamais utilisées.

b. Facebook est plutôt pour les adolescents, les autres sont des réseaux professionnels et vous pouvez y mettre toutes vos données professionnelles sans vous poser de questions.

c. Il faut être très prudent : même sur les réseaux dits « professionnels » vos données sont visibles par n'importe qui.

d. Toutes les données mises sur les réseaux sociaux peuvent être utilisées par les propriétaires du réseau conformément aux conditions d'utilisation du site dont vous avez pris connaissance.

R27 : d. La proposition d. est la seule affirmation vraie. Vos données mises sur les réseaux sociaux peuvent être utilisées à partir du moment où vous acceptez les conditions générales d'utilisation. Sur la plupart des réseaux sociaux, la politique de confidentialité décrit l'utilisation qui peut être faite de vos données. Par contre les données que vous mettez sur ces réseaux sociaux ne seront pas visibles par n'importe qui, si vous réglez correctement vos paramètres de confidentialité. Sur les réseaux professionnels les données que vous avez choisies de ne pas rendre publiques ne seront visibles que par vos relations ou contacts (les personnes qui font partie de votre réseau) mais pas par n'importe qui.

Q28 : Je trouve une clé USB dans ma boîte à lettres. Quelle est la meilleure action ?

a. Je la connecte à mon ordinateur pour en voir le contenu.

b. Je l'analyse avec un anti-virus, on ne sait jamais.

c. Je la jette, une clé peut contenir un virus.

R28 : c. Mieux vaut ne pas utiliser la clé.

Q29 : J'ai lu dans un magazine informatique qu'un anti-virus gratuit extrêmement efficace peut être téléchargé depuis Internet. Je suis sur l'ordinateur de mon lieu de travail, quelle est la bonne attitude à adopter ?

a. J'en parle à mon responsable informatique et c'est lui qui décide si on l'installe ou pas.

b. Je le télécharge et je l'installe en plus de l'anti-virus existant, ça ne peut pas nuire.

c. Je le télécharge après avoir supprimé l'anti-virus existant pour éviter des conflits.

d. Je le télécharge à la maison et je l'amène au bureau sur une clé USB que j'ai passée à l'anti-virus. Je l'installe ensuite sur mon ordinateur de bureau.

R29 : a. Ne pas toucher soi-même aux moyens de sécurité dans un environnement professionnel si cela ne fait pas partie de nos missions.

Q30 : J'ai reçu un smartphone dernier cri pour mon anniversaire, je décide de vendre l'ancien. Quelle est la meilleure attitude?

a. J'efface les données personnelles de mon ancien smartphone avant de l'envoyer.

b. Je remets mon ancien smartphone en configuration usine.

c. Je n'ai rien à cacher, j'envoie mon ancien smartphone en l'état.

d. je chiffre mon ancien smartphone avant de l'envoyer.

R30 : b. La meilleure attitude est la réinitialisation en configuration usine qui effacera vos données personnelles ainsi que toutes les applications que vous avez installées et les données liées. L'acheteur disposera d'un téléphone vierge et prêt à l'emploi. En effaçant manuellement vos données personnelles vous risquez d'en oublier. Si vous chiffrez votre téléphone, l'acheteur ne pourra pas l'utiliser (sauf si vous lui communiquez aussi le mot de passe ce qui rendrait inutile le chiffrement).