



UNIVERSITÉ DE  
RENNES 1



UBO  
université de Bretagne  
occidentale



INSA

INSTITUT NATIONAL  
DES SCIENCES  
APPLIQUÉES  
RENNES



Business  
Services

## Quizz pour le cours de Sensibilisation et initiation à la cybersécurité



# CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Version 1.0

17/02/2015

Orange Consulting

114, rue Marcadet - 75018 Paris

Tél. : (33) 1 56 55 45 00 - Fax : (33) 1 56 55 45 01

Université européenne de Bretagne

5 Boulevard Laennec - 35000 Rennes

Tel. : +33 (0)2 23 23 79 79 - F : +33 (0)2 23 44 84 55



## Contributeurs

Organisme	Nom
<i>Université européenne de Bretagne</i>	<b>Dominique LE TALLEC, Aline BOUCARD</b>
<i>Université de Rennes 1</i>	<b>Gilles LESVENTES, Sébastien GAMBS</b>
<i>Université de Bretagne Occidentale</i>	<b>Laurent NANA</b>
<i>Université de Bretagne Sud</i>	<b>Guy COGNAT</b>
<i>Télécom Bretagne</i>	<b>Frédéric CUPPENS, Nora CUPPENS, Gouenou COATRIEUX</b>
<i>Ecole Normale Supérieure Rennes</i>	<b>David PICHARDIE</b>
<i>INSA Rennes</i>	<b>Gildas AVOINE</b>
<i>Orange Consulting</i>	<b>Alain MARCAY, David BOUCHER</b>



1. Entourer les exemples d'enjeu de la cybersécurité ? (Slide 7 - Les enjeux de la sécurité des S.I.)
- a. Augmenter les risques pesant sur le Système d'information
  - b. Révéler les secrets
  - c. Rendre difficile la vie des utilisateurs en ajoutant plusieurs contraintes comme les mots de passe longs et complexes

**d. Protéger le système d'information**

2. Exemple d'impacts sur la vie privée (voir Slide 13 - "Les impacts de la cybercriminalité sur la vie privée):
- a. Impact sur l'image / le caractère / la vie privée :
    - i. Diffamation de caractère
    - ii. Divulgence d'informations personnelles (photos dénudées)
    - iii. Harcèlement
  - b. Impact sur l'identité:
    - i. Usurpation d'identité

3. Quels sont les trois principaux besoins de sécurité (**Voir slide 23 - 24**)
- a. D: Disponibilité
  - b. I : Intégrité
  - c. C : Confidentialité

Avec un critère complémentaire : P pour Preuve

4. Entourer la (ou les) phrase(s) correcte(s)
- a. Le chiffrement permet de garantir que la donnée sera toujours disponible/accessible

**b. La sécurité physique permet d'assurer la disponibilité des équipements et des données**

- c. La signature électronique permet de garantir la confidentialité de la donnée

**d. Les dénis de service distribués (DDoS) portent atteinte à la disponibilité des données**

5. Vous développez un site web [www.asso-etudiants-touristes.org](http://www.asso-etudiants-touristes.org) pour une association qui regroupe les étudiants souhaitant effectuer des voyages ensemble à l'étranger. Sur ce site on retrouve les informations concernant les voyages proposés telles que : le pays, les villes à visiter, le prix du transport, les conditions d'hébergement, les dates potentielles du voyage. Ces informations ont un besoin en confidentialité :

**a. Faible**

- d. Fort



6. Je viens de développer un site web pour une association qui regroupe les étudiants souhaitant effectuer des voyages en groupe à l'étranger. Les informations relatives aux étudiants inscrits sur le site (login et mot de passe, nom, prénom, numéro de téléphone, adresse), ont un besoin en confidentialité :
- a. Faible
  - b. Fort**
7. Je peux réussir une attaque sur un bien qui n'a aucune vulnérabilité (voir Slide 34 - Notions de vulnérabilité, menace, attaque - attaque):
- a. Vrai
  - b. Faux**
8. Toutes les organisations et tous les individus font face aux mêmes menaces (voir slide 40 - Exemples de sources de menaces):
- a. Vrai
  - b. Faux**
9. Entourer les attaques généralement de type " ciblée " (slide 42 - 52: Panorama de quelques menaces):
- a. Phishing ou hameçonnage
  - b. Ransomware ou rançongiciel
  - c. Social engineering ou ingénierie sociale**
10. Entourer les attaques généralement de type non " ciblée " (slide 42 - 52: Panorama de quelques menaces):
- a. Intrusion informatique
  - d. Virus informatique**
  - b. Déni de service distribué
  - c. Phishing ou hameçonnage**
11. Quels sont les éléments facilitateurs de fraudes internes (Slide 47 - Panorama de quelques menaces : Fraude interne)
- a. Des comptes utilisateurs partagés entre plusieurs personnes**
  - b. L'existence de procédures de contrôle interne
  - c. Peu ou pas de surveillance interne**
  - d. Une absence ou une faiblesse de supervision des actions internes**



12. Entourer les éléments qui peuvent réduire ou empêcher des fraudes internes

**a. Une gestion stricte et une revue des habilitations**

**b. Une séparation des rôles des utilisateurs**

c. Peu ou pas de surveillance interne

**d. Des comptes utilisateurs individuels pour chacun**

13. Citer deux vecteurs d'infection de virus (Slide - Panorama de quelques menaces : Virus informatique)

**a. Une pièce jointe attaché à un message électronique**

**b. Un support amovible infecté par exemple une clé USB**

**c. Un site web malveillant ou ayant des pages web corrompues**

**d. Un partage réseau ouvert**

**e. Un système vulnérable**

14. Qu'est-ce qu'un botnet? (Slide - Panorama de quelques menaces : Dénégation de service distribué)

**Un botnet est un réseau d'ordinateurs infectés et contrôlés par une personne malveillante.**

15. Vous devez systématiquement donner votre accord avant de faire partir d'un réseau de botnets? (Slide 52 - Panorama de quelques menaces : Dénégation de service distribué – illustration d'un botnet)

a. Vrai

**b. Faux**

16. En France, la cybersécurité ne concerne que les entreprises du secteur privé et les individus (Slide 54 : L'organisation de la sécurité en France)

a. Vrai

**b. Faux**

17. L'usage d'outils pour obtenir les clés Wifi et accéder au réseau Wifi du voisin tombe sous le coup de la loi (Slide 58 - Dispositif juridique français de lutte contre la cybercriminalité):

a. Vigipirate

**b. Godfrain**

c. Hadopi

d. Patriot act

18. Mon réseau wifi personnel est mal sécurisé, par exemple par l'usage d'une clé Wifi faible (exemple: 12345678). Une personne (intrus) se connecte à mon réseau pour effectuer des actions malveillantes comme attaquer un site gouvernemental :



- a. J'encours des sanctions
- b. Seul l'intrus encourt des sanctions

**c. L'intrus et moi encourons des sanctions.**

- d. Aucune sanction n'est encourue

19. Donner un exemple de données à caractère personnel

- a. Nom, prénom
- b. Nom, téléphone
- c. Date de naissance et commune
- d. Lieu de naissance
- e. Nationalité ou pays de naissance des parents ou des grands parents
- f. Adresse
- g. N° carte d'identité / N° de passeport / N° de permis de conduire, ...
- h. Empreinte digitale
- i. <http://www.cil.cnrs.fr/CIL/spip.php?rubrique299>

20. Lors de la création du site Web de notre association étudiante, si vous stockez les informations suivantes pour chaque membre : nom, prénom, adresse, adresse email. Après de quel organisme devez-vous faire une déclaration (Slide 60 - 64 : Droit de protection des données à caractère personnel)?

- a. Gendarmerie
- b. Université

**c. CNIL**

- d. Hadopi