

## 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

## 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 COGNIAT</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>

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



## 1. Quizz pour le module 1 : « Cybersécurité : notions de base »

1. Sélectionner ci-dessous les enjeux de la cybersécurité ?
  - 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. Si vous étiez victime d'une attaque cybercriminelle, quelles pourraient être les conséquences (impacts) sur votre vie privée ? (deux exemples)
3. Citer les trois principaux besoins de sécurité.
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 ;
  - b. Fort.
6. 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 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 objet qui n'a aucune vulnérabilité (faiblesse):



- 
- a. Vrai ;
  - b. Faux.
8. Toutes les organisations et tous les individus font face aux mêmes menaces :
- a. Vrai ;
  - b. Faux.
9. Entourer les attaques qui sont généralement de type " ciblée " :
- a. Phishing ou hameçonnage ;
  - b. Ransomware ou rançongiciel ;
  - c. Social engineering ou ingénierie sociale ;
10. Entourer les attaques qui sont généralement de type « non ciblées » :
- a. Intrusion informatique ;
  - b. Virus informatique ;
  - c. Dénégation de service distribué ;
  - d. Phishing ou hameçonnage.
11. Entourer les éléments facilitateurs des fraudes internes
- 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 moyens (vecteurs d'infection) par lesquels les virus informatiques peuvent être transmis d'un système compromis (ou d'un attaquant) à un système sain.
14. Qu'est-ce qu'un botnet?
15. Vous devez systématiquement donner votre accord avant de faire partie d'un réseau de botnets?
- a. Vrai ;
  - b. Faux.



16. En France, la cybersécurité ne concerne que les entreprises du secteur privé et les individus
- Vrai ;
  - 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 :
- Vigipirate ;
  - Godfrain ;
  - Hadopi ;
  - 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 :
- J'encours des sanctions ;
  - Seul l'intrus encourt des sanctions ;
  - L'intrus et moi encourons des sanctions ;
  - Aucune sanction n'est encourue.
19. Donner un exemple de données à caractère personnel.
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. Auprès de quel organisme devez-vous faire une déclaration?
- Gendarmerie ;
  - Université ;
  - CNIL ;
  - Hadopi.