LE « PHISHING »

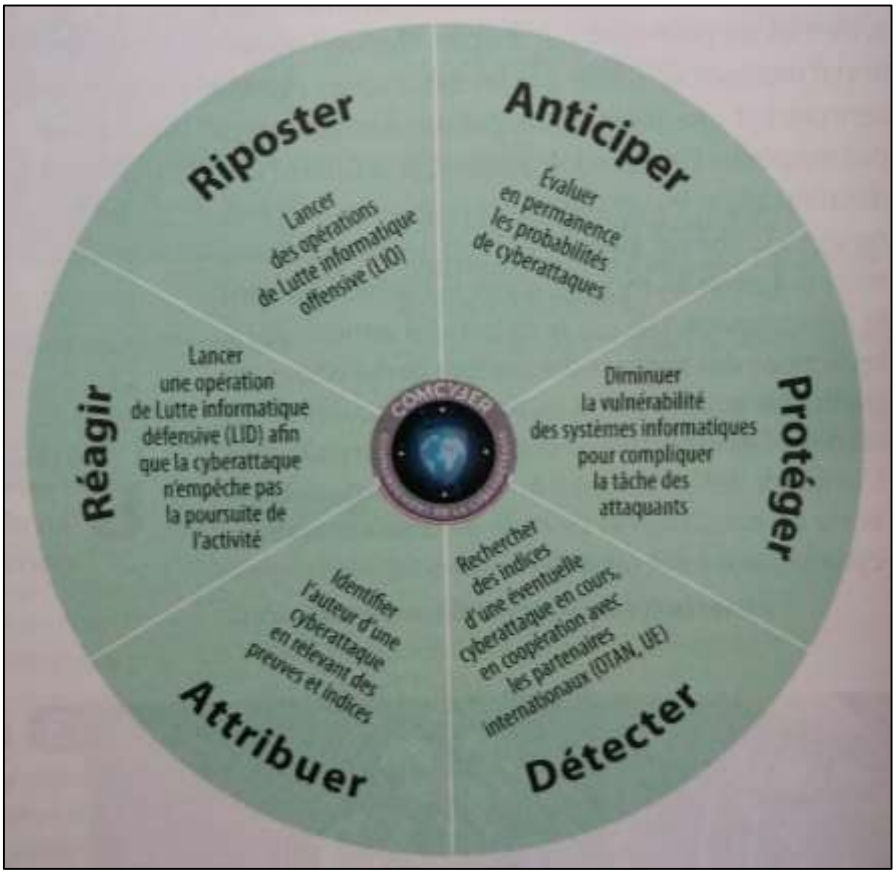
Doc1. Les hackers* profitent de la popularité de Zoom

Les cybercriminels tentent de tromper les utilisateurs de Zoom, alors que la plateforme de vidéoconférence gagne en popularité depuis le confinement et la généralisation du télétravail. […]
En mars, le nombre de participants à une réunion Zoom a atteint plus de 200 millions, contre 10 millions en décembre. Dans de nombreux cas, elle est utilisée par des personnes qui travaillent à distance pour la première fois. Mais la croissance soudaine de la popularité de Zoom n'est pas passée inaperçue, et les cybercriminels ciblent de plus en plus les utilisateurs de la plateforme. […]
Les télétravailleurs s'attendant à recevoir des invitations pour les conférences téléphoniques de Zoom, les attaquants profitent alors d'envoyer des e-mails de phishing contenant des liens vers de fausses pages de connexion qui visent à voler les noms d'utilisateur et les mots de passe saisis. Les attaquants peuvent ensuite exploiter ces informations pour accéder aux comptes des entreprises et mener d'autres attaques. […]
Le coronavirus est devenu le thème en vogue dans les cyberattaques ; non seulement les attaquants utilisent de faux domaines sur ce thème, mais plus généralement le sujet est très exploité pour les cyberattaques. De nombreux messages prétendant provenir de professionnels de la santé, de prestataires logistiques et autres, par exemple, sont envoyés dans l'objectif de voler des informations financières, installer des logiciels malveillants ou commettre d'autres cyberattaques.

* hacker : pirate informatique, individu capable de s'introduire dans un réseau et de le détourner.

Source : https://www.zdnet.fr/actualites/cybersecurite-les-hackers-profitent-de-la-popularite-de-zoom-pour-leurs-campagnes-de-phishing-39901809.htm

Doc2. Les six missions de commandement de la cyberdéfense française



Source : Ministère des Armées, 2020.

Doc3. La cyberdéfense, un enjeu majeur pour le ministère des Armées

Florence Parly
Ministre des Armées

Ce sont plus de deux incidents de sécurité par jour qui touchent tout autant notre ministère (des armées) que nos opérations extérieures. Certaines attaques sont le fruit de groupes malveillants. D'autres de hackers isolés. Mais certaines, nous le savons, viennent d'Etats pour le moins indiscrets, pour le moins décomplexés. La guerre cyber a commencé et la France doit être prête à y combattre. Nous nous réservons le droit de riposter. Nous serons aussi prêts à employer en opérations extérieures l'arme cyber à des fins offensives, isolément ou en appui de nos moyens conventionnels, pour en démultiplier les effets dans le plus strict respect des normes du droit international public.

Source : Discours de Florence Parly, Ministre des Armées, 18 janvier 2019.

Doc4. Formation d'ingénieur cyberdéfense

Le master mention informatique, parcours cybersécurité est une formation organisée par la CyberSchool et dont le diplôme est délivré par l'Université de Rennes 1. Il forme des futurs experts, ingénieurs et scientifiques en cybersécurité.
La formation est ouverte aux étudiant.e.s en formation initiale ainsi qu'aux salarié.e.s et demandeur.euse.s d'emploi en formation continue.

Les compétences développées portent sur les domaines suivants :

- administration des réseaux ;
- cryptographie pour la sécurité ;
- méthodologie de la sécurité ;
- sécurité des attaques informatiques ;
- internet des objets ;
- sécurité des systèmes ;
- ingénierie des logiciels pour les systèmes et réseaux.

À l'issue du parcours les étudiants sont capables de concevoir, réaliser et valider la robustesse et la sécurisation de systèmes informatiques de types très variés, depuis les serveurs jusqu'aux objets connectés.

Source : https://formations.univ-rennes1.fr/master-mention-informatique-parcours-cybersecurite-cybersecurity-cse

CONSIGNES :

Vous devez constituer un ensemble de 5 cartes sur le thème du « phishing » :

- une carte définition,
- une carte situation,
- une carte mission,
- une carte action,
- une carte formation.

Compétences mobilisées :

* Raisonner, justifier une démarche et les choix effectués
* Analyser et comprendre un document pour en extraire des informations
* Pratiquer différents langages
* Coopérer et mutualiser

Guide sur le contenu des différentes cartes :

- Carte définition : Doc1, proposez une définition du « phishing ».
- Carte situation : Doc1, résumez brièvement un cas concret de situation du « phishing ».
- Carte mission : Doc2, identifiez parmi les six missions de commandement de la cyberdéfense française, celle qui vous semble être la plus efficace pour contrer le « phishing ».
- Carte action : Doc3, résumez la stratégie qui peut être appliquée à l'échelle européenne pour contrer le « phishing ».
- Carte formation : Doc4, présentez un métier de la cyberdéfense.

Pour compléter et affiner vos réponses vous pouvez utiliser d'autres outils : manuel, dictionnaire, ordinateur. Une fois les 5 cartes réalisées, un élève ou plusieurs élèves rapporteurs présenteront à l'oral le travail de leur groupe à l'ensemble de la classe.

Toutes vos réponses doivent être rédigées sur les patrons de cartes ci-dessous.

LE « PHISHING »

① Carte définition

Source : https://www.zdnet.fr/actualites/cybersecurite-les-hackers-profitent-de-la-popularite-de-zoom-pour-leurs-campagnes-de-phishing-39901809.htm

LE « PHISHING »

② Carte situation

Source : https://www.zdnet.fr/actualites/cybersecurite-les-hackers-profitent-de-la-popularite-de-zoom-pour-leurs-campagnes-de-phishing-39901809.htm

LE « PHISHING »
③ Carte mission

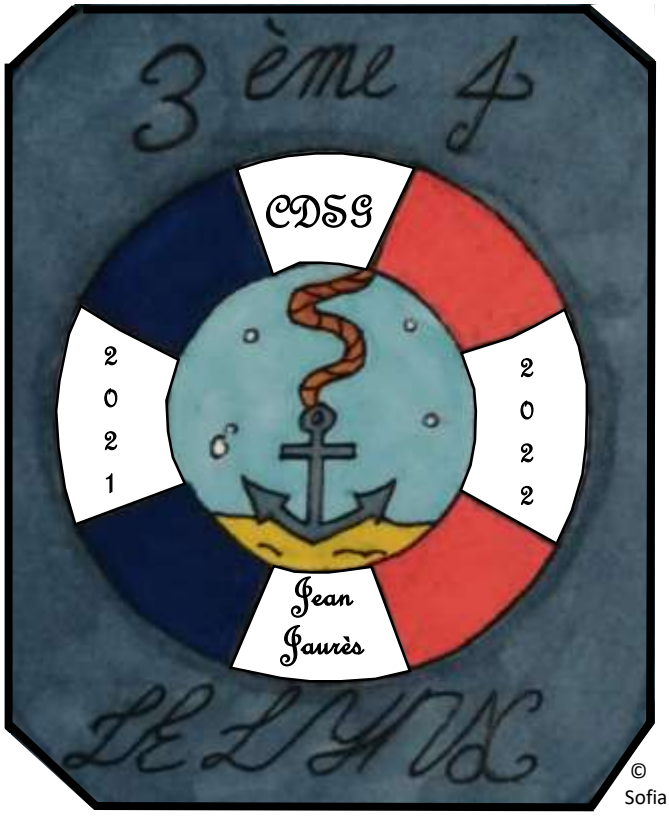
Source : Ministère des Armées, 2020.

LE « PHISHING »
④ Carte action

Source : Discours de Florence Parly, Ministre des Armées, 18 janvier 2019.

LE « PHISHING »
⑤ Carte formation

Source : https://formations.univ-rennes1.fr/master-mention-informatique-parcours-cybersecurite-cybersecurity-cse



© Sofia