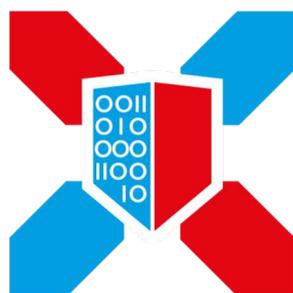


nc3.lu

National Cybersecurity
Competence Center
LUXEMBOURG

Initiation à la Sécurité de l'Information

Script de la sensibilisation à la sécurité de l'information



LHC

**Luxembourg House
of Cybersecurity**

Slide 1 :

Présentation de la formation, introduction, le contexte. Si nécessaire, il faut présenter l'entreprise, sinon le service proposant la formation.

Slide 2 :

Le formateur peut se présenter, lui et son cursus, son CV.

Slide 3 :

Exercice de participation :

Faire estimer aux participants la valeur de leur téléphone. Expliquer qu'ils sont inestimables par les informations qu'ils contiennent.

Explication de la sécurité de l'information, ce qu'elle concerne, les domaines que cela concerne.

Exercice de participation :

Demander à l'audience ce que représente la sécurité pour eux.

- Expliquer que la sécurité n'est pas un état, c'est un sentiment. « Nous ne sommes pas en sécurité, nous nous sentons en sécurité. »

Demander à l'audience ce que peut être une information, demander des exemples d'information.

- Expliquer que des informations peuvent être de nature médicale (exemple personnel, une maladie grave ...), elles peuvent être plus importantes (schéma de drones, plans militaires, plan de centrale nucléaire ...)

Expliquer la nécessité et l'importance de protéger les informations, même celles qui semblent insignifiantes à première vue. Donner les conséquences malheureuses liées à la perte des données citées en exemple.

Slide 4 :

Généraliser les différents conséquences et types de conséquences liés à un problème de sécurité de l'information, avec la perte de confiance, des sanctions économique ou légale. Chacun peut être responsable. Expliquer que ces conséquences sont professionnelles, mais aussi et surtout personnelles.

Slide 5 :

Transition de la sécurité de l'information vers les risques. Exprimer que protéger l'information revient à gérer et à comprendre les différents risques. Explication du vocabulaire utilisé dans le domaine : Le traitement du risque. Définition d'un risque

Slide 6 :

Décomposer le risque pour mieux l'expliquer, et le faire par l'exemple.

Vulnérabilité :

Exemples :

- Clé sous le tapis/pot de fleurs : Expliquer une histoire qui pourrait expliquer une raison de le faire, comme vouloir donner les clés à un proche.
- Erreur Humaine

Menace :

Exemples :

- Cambrioleur : Indiquer comment les cambrioleurs font pour préparer un cambriolage. Étude des habitudes, des lumières, des alentours, déguisement éventuel, tentative de toquer/sonner, tentative d'ouvrir la porte, passer par derrière ... utilisation du monde connecté, comme les objets connectés (comme un jouet connecté qui parle à l'enfant, pour lui faire ouvrir la porte, ou des pots de fleurs connectés pour vérifier si la plante est arrosée ...etc.).
- Voiture

Impact :

Exemples :

- Vol de biens
- Blessure/Mort

Exercice de participation :

Réflexion avec le groupe de travail sur des exemples de risque de tous les jours.

En prenant les exemples, montrer qu'il est impossible d'influer sur les menaces et les impacts : il est globalement seulement possible de jouer sur les vulnérabilités.

Slide 7 :

Formalisation des risques existants, et exemples des catégories.

Slide 8 :

Expliquer les différents dangers les plus communs. Éventuellement, il est possible de monter des histoires, de les raconter en faisant participer les personnes en montant de fausses histoires (bien qu'il soit nécessaire d'obtenir l'accord des personnes auparavant).

Mises à jour :

Les appareils technologiques (ordinateur et logiciels, laptop, smartphone et application, voiture, GPS ...) contiennent du code qui est souvent incomplet, ou avec des cas imprévus ou des failles imprévues. Besoin de mise à jour pour réparer les failles existantes.

Exemple :

- Lors de l'achat d'une maison, nous regardons si cette dernière est complète : murs, toit, fenêtres, vitres, électricité, plomberie ...). Lors de l'achat d'un téléphone, nous sommes encore au stade où nous regardons l'apparence, les composants, ce qui revient à s'assurer de la tapisserie et de la finesse du téléphone, sans regarder des détails plus techniques. Si une maison vaut une certaine somme, et un téléphone vaut beaucoup moins, il contient très souvent les données d'une vie qui sont inestimables (photos, données personnelles, comptes utilisateur comme Amazon ou PayPal ...)

Conseils à donner :

- Mettre à jour les différents appareils, les logiciels, tant pour le téléphone, les ordinateurs, pour s'assurer d'avoir les dernières protections possibles.

Pause Café :

Ne pas verrouiller son ordinateur, laisser accessible son téléphone, c'est donner la possibilité à n'importe qui de se faire passer pour nous. Dans le même genre, donner ses accès, ou faire confiance aveugle peut être très dangereux.

Exemple :

- Deux employés se battent pour une promotion dans un domaine avec des données sensibles, comme la comptabilité d'une entreprise. L'un des deux devient le supérieur de l'autre par la promotion, mais il laisse son ordinateur accessible lors d'une absence pour une pause café, avec le délégué du personnel. Par vengeance, son collègue accède à son ordinateur, et envoie un mail insultant à la direction. La direction, après connaissance du mail, demande des explications et témoignages. De par la nature de confidentialité des informations et de la confiance accordée, le responsable est la personne partie en pause café qui n'aura pas verrouillé son ordinateur.

Exercice de participation :

Nommer les acteurs dans l'histoire avec des personnes de l'audience.

Conseils à donner :

- Verrouiller son ordinateur dès lors d'une absence, mais également le téléphone pour éviter un vol d'identité.

Mot de passe :

Le mot de passe est comme une clé protégeant tout une vie virtuelle. 80% des mots de passe sont facilement trouvable quelque part sur le bureau d'un individu (photographie, objet, document, post-it ...). Il est le même entre les différents accès.

Exemple :

- ➔ Les mots de passe sont facilement récupérables en posant de simples questions. Une étude a été faite sur la possibilité de récupérer un mot de passe avec un testeur sur la sécurité de mot de passe, dans la rue. Le taux de récupération est supérieur à 60%.

Conseils à donner :

- ➔ Les mots de passe doivent être complexifiés, changés de temps à autre, et ne doivent pas être laissés par défaut. Ils ne doivent pas être facilement devinables. Les mots de passe ne doivent être donnés à personne.

Slide 9 :

Plan sur les points abordés lors de l'initiation de la sécurité de l'information.

Slide 10 :

Expliquer à quel point il est possible et facile de profiter des différents points cités pour parvenir à ces fins, et ce par des exemples.

Exemple :

- ➔ Les spams peuvent illustrer les différentes faiblesses de l'homme. La curiosité est représentée par des offres promotionnelles qui peuvent donner envie de cliquer, la vanité par des sommes offertes suite à une histoire tragique. La fainéantise est utilisée par des liens facilement accessibles, et la libido par différentes publicités ou images évocatrices. La peur est utilisée par des menaces récentes, comme la sextortion, et la pitié est utilisée par les histoires tragiques. Globalement, toutes les vulnérabilités sont humaines principalement.

Exercice de participation :

Il est possible de commencer une histoire concernant les vulnérabilités humaines. Expliquer qu'une personne (A) est amoureuse d'une autre (B), et qu'elle est amie avec une dernière (C). La personne qui est aimée (B) part en vacances, et a un profil Facebook réservé aux amis. La personne amoureuse (A) se confie à son ami (C), dans un bar, où la discussion est entendue par une personne malveillante (E). Interrompre ici l'histoire, et la reprendre **Slide 12**.

Construire un spam (simple) avec l'audience, pour montrer à quel point cela est facilement possible, mais aussi expliquer les ficelles utilisées par les pirates.

Conseils à donner :

- ➔ Réfléchir avant de répondre à un message. Répondre à un spam, c'est être sur une liste d'adresse mail valide qui peut être victime d'un spam. Ne jamais payer, c'est un moyen d'être sur une liste de bon payeur, et de se voir redemander de l'argent, tout en participant à une activité criminelle.

Slide 11 :

Exercice de participation :

Demander à une personne si elle ne viendrait pas de telle ville, avec pour objectif d'obtenir le lieu de l'habitation. Demander innocemment le quartier une fois le nom de la ville obtenue.

Demander ce qui se passerait si une clé USB était simplement laissée devant les locaux, vraisemblablement abandonnés. Expliquer les dangers d'utiliser un tel dispositif.

Parler du social engineering. Expliquer les différentes possibilités de manipulations de la langue, et autres techniques psychologiques possibles

Exemple :

- ➔ Parler de Gilbert Chikli, « l'inventeur » de la fraude au président. Expliquer la façon de réaliser une telle fraude, en prenant des exemples types d'appels ou de phrase utilisés : « Je compte sur vous », « vous ne devez en parler à personne, c'est une mission secrète », « j'ai une parfaite confiance en vous » ... De plus, expliquer cette façon d'être insistant et ne pas laisser le temps de réfléchir.

Conseils à donner :

- ➔ Communiquer dès lors d'une suspicion d'un problème quelconque. Il est nécessaire de recontacter une personne par les moyens connus en cas de suspicion ou d'un fait étrange ou interpellant, pour s'assurer que c'est bien la personne légitime qui a fait la demande.

Slide 12 :

Exercice de participation :

Reprendre l'histoire laissée Slide 10. La personne-espionne (E) va alors se faire passer pour l'ami de l'amoureux (C), et lui envoyer un lien avec le profil de la personne partie en vacances (B), en jouant sur la libido (photo en bikini/short) ou la peur (vue avec une autre personne qu'on ne connaît pas sur des photos). Lancer la vidéo pour expliquer ce qui pourrait se passer :

Vidéo : <https://www.youtube.com/watch?v=iqoFbVLUHY>

Montrer à quel point il faut faire attention aux URL, avant de cliquer, et toujours vérifier les sources avant toutes actions. Expliquer également qu'un mot de passe connu sera testé sur d'autres services.

Exercice de participation :

Les préparer à lire rapidement ce qui est indiqué, et le montrer comme un exercice.

Slide 13 :

Exercice de participation :

Faire lire rapidement la slide aux personnes tour à tour, sans leur laisser le temps de réfléchir. Expliquer que malgré la conscience de ces phénomènes, il faut toujours bien faire attention, et toujours regarder attentivement avant de cliquer à un endroit.

Conseils à donner :

- ➔ Toujours regarder attentivement, et surtout, prendre le temps de bien lire.

Slide 14 :

Exemple :

- ➔ Faux remboursement proposé par l'Administration des contributions directes : Un faux site a été reproduit, avec la demande d'une carte bancaire, qui pouvait être facilement donnée.

Exercice de participation :

Demander si les personnes se feraient avoir par une telle fraude, et demander ce qu'il en serait de leurs parents ou leurs grands-parents.

Slide 15 :

Exemple :

- ➔ Exemple de ce qui peut être vu couramment. Le premier est un ordinateur d'une personne qui possède beaucoup de responsabilités, et donc, beaucoup de données personnelles. Le second est visible dans un train, lors de voyage ou de déplacement, ou toutes les données sont visibles, et non protégées.

Conseils à donner :

- ➔ En public, il est nécessaire de faire attention à ce qu'on permet aux externes de voir et d'entendre. Toute information donnée peut être réutilisée contre nous.

Slide 16 :

Exercice de participation :

Demander les différents problèmes liés à cette image.

Une photographie qui a été publiée sur Facebook sans prendre en compte que les écrans sont visibles, que le WiFi est accessible au tableau, mais aussi que la GDPR n'est même pas respectée a priori.

Conseils à donner :

- ➔ Il faut toujours demander l'autorisation de prendre une image, mais également de la diffuser. De plus, il est nécessaire de vérifier ce qui est sur la photo.

Slide 17 :

Liste une bonne partie des pièges qui peuvent être faits sur les appareils mobiles. L'oubli et la perte de matériel, la discussion dans des lieux publics, les données non chiffrées en cas de vol, qui deviennent accessibles à tous.

Vidéo : <https://www.youtube.com/watch?v=GBUiBEv-cM0>

Exercice de participation :

- ➔ Créer un réseau WiFi avec le téléphone, avec un SSID similaire aux réseaux existants, et montrer au groupe qu'il est visible sur leur téléphone, et ainsi leur montrer avec quelle facilité cela est faisable.

Conseils à donner :

- ➔ Il ne faut pas se connecter à un réseau que nous ne maîtrisons pas, et privilégier les données du forfait. Sinon, il faut s'assurer de ne pas envoyer de données confidentielles.

Exercice de participation :

- ➔ Induire un exercice de brainstorming, avec comme principal objectif de montrer la facilité de réalisation simple :
 - Vous êtes un détective privé, et travaillez pour le compte de l'état. Vous disposez de tous les moyens, y compris illégaux, pour récupérer les données médicales d'une personne. Comment feriez-vous ?
 - Votre meilleur ami soupçonne sa/son conjoint d'avoir une relation extra-conjugale, et vous demande de l'aider à le découvrir. Vous disposez de tous les moyens, y compris illégaux, pour le faire. Comment feriez-vous ?

----- Pause -----

- ➔ Faire un débriefing sur les différentes façons qui ont été pensées. Écrire sur un tableau les idées. Éventuellement, préciser en quoi les données récoltées peuvent détruire les personnes.

Exemple de résolution possible :

- ➔ Le médecin de la cible a été approché sous l'identité de l'OMS (Organisation Mondiale de la Santé) pour obtenir le dossier médical de la personne ciblée, après quelques recherches sur l'identité de personnes y travaillant (écumage de Facebook, LinkedIn) pour ajouter des détails crédibles à l'appel. L'appel exprimait le fait qu'une maladie rare pouvait se cacher derrière le dossier médical, et qu'il fallait qu'il soit transmis dans les moindres détails pour disposer de toutes les informations nécessaires. (Exemple de Fraude au président, Social Engineering)
- ➔ Le téléphone de la personne soupçonné a été récupéré. Le code de verrouillage a été demandé au conjoint, ou a été déduit par la date de naissance de la personne. Des messages compromettants, des images ont été trouvés. D'autres preuves sont trouvées dans l'historique de localisation du téléphone. (Exemple de récupération des données sur une machine où nous possédons toute notre vie.)

Slide 18 :

Exercice de participation :

Faire une démonstration de comment il peut être facile, avec des outils en ligne, de craquer un mot de passe. Montrer comment il peut être facile d'accéder à un robot.txt, ou nous pouvons apprendre où sont stockés des fichiers de mots de passe. Récupérer le mot de passe, et expliquer que comme tous les mots de passe sont les mêmes, il devient possible d'accéder à toute la vie personnelle. Prendre et illustrer l'exemple, en réalisant une petite démonstration avec un hash de mot de passe déjà calculé à l'avance.

Exemple : 179909b745f81f03f177a3079e0ce5e3:ef749ff9a048bad0dd80807fc49e1c0d

www.bikes.com

<https://crackstation.net/>

Slide 19 :

Des cas qui se sont produits, réels, de leak de mot de passe, sur des sites connus ou célèbres, et qui sont testés et repris sous de nombreux sites. Expliquer que c'est bien pour cela qu'il est nécessaire de changer ces mots de passe.

Exercice de participation :

Qui dispose d'un compte sur au moins l'un des sites qui est cité ? Récupérer certains mots de passe peut-être très faciles.

Conseils à donner :

- ➔ Changer les mots de passe pour ceux qui ne l'auraient pas encore fait.

Slide 20 :

Pourquoi les pirates font-ils cela ? Quelles sont les raisons de faire de tels actes ? Expliquer que les motivations principales sont financières. Certains, plus rare, le font pour la gloire ou pour dénoncer ou promouvoir une opinion ou une idée.

Slide 21 :

Exemple de ce que rapporte en moyenne une vague de phishing.

Slide 22 :

Cycle de revente des données avant la GDPR qui était fait en Europe. Ceci est toujours fait hors Europe.

Exemple :

- Une personne écrit sur Facebook un commentaire avec une envie de faire du sport. Facebook revend alors la donnée à des Brokers, qui revendent les données aux entreprises de Marketing. Ces dernières vont alors le vendre à des organismes spécialisés dans le sport, qui enverra alors une publicité pour tenter de convaincre la personne l'utilité de faire du sport. Les données restent dans ces organismes, et avant la GDPR, sont quasiment intraçable.

Slide 23 :

L'or a rapporté, le pétrole a rapporté, et aujourd'hui, les données rapportent et sont l'or de demain.

Slide 24 :

Explication rapide et succincte du Deep Web, et du navigateur Tor. S'il y a des choses illégales dans le Deep Web (achat de produits illégaux, comme la drogue, des organes, des armes à feu ...), il reste principalement un outil pour rester anonyme. Mais accepter d'y participer, c'est aussi accepter de devenir un relais pour d'éventuels criminels.

Slide 25 :

Prix disponibles du Deep Web, et des différents produits et services disponible. Les prix baissent de plus en plus, et sont de plus en plus concurrentiels.

Slide 26 :

La facilité et la possibilité d'acheter des cartes de crédit volées, ce qui peut être fait par les plus jeunes.

Exemple :

- Il n'est pas rare de voir des adolescents qui, pour commander un article ou un service hors de leur portée, achètent ce genre de carte de crédit volée, pour que leurs parents ne puissent pas voir la facture.

Conseils à donner :

- Les enfants ont le besoin d'être accompagnés et guidés pour expliquer les dangers liés à tout ça.

Slide 27 :

Exercice de participation :

Est-ce que vous reconnaissez ces appareils ? Les utilisez-vous de façon courante dans votre vie ? Pourtant, si vous y mettez votre carte, vos informations de votre carte bancaire seront volées. Comment ses cartes des crédits peuvent être volées. Que ce soit les sites web, qui d'un côté sont volables sur différents sites internet, ou encore via des distributeurs de billets officiels, des lecteurs de cartes.

Exemple :

- Il est aussi possible de voler de l'argent avec le paiement sans contact. Allez dans le métro, avec un terminal de paiement NFC, et vous pourrez voler jusqu'à 30€ par carte sans contact.

Slide 28 :

Expliquer l'application Blippar, qui peut montrer où se sont rencontrées deux personnes par le passé en croisant les historiques de localisation des téléphones.

Exercice de participation :

Avec les personnes dans le groupe, faire une démonstration avec l'Iphone. Les faire aller dans « Réglages » > « Confidentialité » > « Service de localisation » > « Services système » > « Lieux Importants ». Ces lieux et historiques peuvent être utilisés par des applications desquelles nous ne lisons pas les conditions d'utilisation que nous acceptons. Expliquer que les téléphones Android ne sont pas en reste, et des mails Google peuvent indiquer les trajets faits durant le mois.

Slide 29 :

Exemple :

→ Exemple d'aberrations, avec des selfies de nus qui sont faits pour des demandes de crédits.

Insister également sur l'importance de protéger les plus jeunes de ce genre de pratique, de l'impossibilité de supprimer les données, et la nécessité de les accompagner dans l'utilisation des appareils et d'internet.

Slide 30 :

Expliquer le problème de l'Internet of Things. Tous les objets connectés sont attaquables d'une façon ou d'une autre, voir donne des informations. Expliquer que peu de constructeurs sont soucieux de ces problématiques, car plus concentrés sur d'autres problèmes.

Exemple :

→ Il est possible d'accéder aux données d'un Pacemaker, de le lire, mais surtout de les modifier, ces données n'ont pas une protection suffisante.

→ Un pot de fleurs connecté peut renseigner un voleur sur les absences de présence dans un domicile.

Slide 31 :

Exemple :

→ Autre exemple de piratage, avec les voitures connectées. Le problème est surtout que les constructeurs ne sécurisent pas, car ils ne pensent pas à la sécurité dès le départ. Et la tâche est complexifiée par après. (Security by design)

Slide 32 :

L'utilisation de ses piratages n'est pas que dans le monde des actifs, mais des enfants ou des seniors, qui sont aussi touchés. Les jouets connectés en sont un exemple possible. Un pirate cherchera à attaquer sur le point faible des personnes, et pour beaucoup, le point faible d'une personne est ses enfants.

Exemple :

→ Des cambrioleurs ont utilisé un jouet connecté, en le faisant pleurer, pour raconter une histoire triste à un enfant. Sa femme a été écrasée, et ses petits cherchent la maison de l'enfant. Une demande lui est faite d'ouvrir la porte, sans le dire à ses parents. Les cambrioleurs n'ont alors pas à forcer la porte.

Slide 33 :

Des objets deviennent connectés, parfois de façon inutile a priori, mais gagnent des accès pour beaucoup plus de monde que leur possesseur.

Exemple :

→ Parfois, de vraies prises d'otage sont possibles, comme baisser la température de la maison avec des moyens simples quand elle est connectée, en plein hiver, pour forcer à payer des rançons ou donner des informations de l'entreprise.

Slide 34 :

Exemple :

- Des caméras qui assurent notre protection (et parfois personnelles) sont accessibles sur internet, et peuvent diffuser des informations oscillant entre le privé ou l'accessibilité d'un endroit. Montrer à quel point cela peut-être important de renforcer les mots de passe. Des sites internet diffusent aujourd'hui des vidéos des caméras de surveillance très mal protégées.

Conseils à donner :

- Globalement, il faut changer les accès par défaut, et s'assurer de la bonne protection d'un produit avant de le prendre.

Slide 35 :

Exemple :

- Autres exemples sur les drones, même ceux de l'armée américaine, qui peuvent donner de précieuses informations. Les drones disposent de caméras, qui sont activées en permanence et peuvent donner des informations sur les colis, les achats des différentes personnes ... Le vol d'inauguration a même été diffusé en ligne.

Slide 36 :

Comment se protéger, cette slide est importante, car elle explique comment se protéger, mais surtout elle permet de montrer qu'il ne faut pas juste entièrement se déconnecter, mais simplement faire attention et suivre des règles de vies simples.

Exemple :

- Prendre l'exemple de la plage. Au départ, les dangers de la plage et des vacances à la plage n'étaient pas connus correctement : vent, marées, danger solaire ... Mais au moment de la prise de conscience, les vacanciers ne se sont pas arrêtés d'aller à la plage, ils ont pris des mesures contre les risques exposés. Internet doit être traité de la même façon, il faut prendre des précautions, et non nier tous les avantages ou le confort que cela peut nous apporter.

Conseils à donner :

- Adapter son comportement à l'extérieur en évitant de parler ou de montrer de données trop confidentielles, mais aussi à l'intérieur, en s'assurant de la protection des données tant personnelles que professionnelles.
- Les règles données par le service informatique doivent être correctement respectées : Elles sont surtout là pour protéger l'entreprise, mais aussi, et surtout les différentes personnes.
- Alerter le service informatique en cas d'un doute de piratage, ou en cas d'agissement bizarre pour être sûr que rien de suspect ou de grave ne se produit.

Slide 37 :

Rappeler la loi pour montrer que pirater est interdit, et ne devrait pas être fait sous aucun prétexte.

Exercice de participation :

Induire une personne aléatoirement prise dans l'audience à tenter de rentrer un code sur un téléphone qui n'est pas le sien (exemple : celui du formateur). Expliquer que ce simple geste coûte autant que le fait de rentrer dans le téléphone, et expliquer les différentes peines encourues.

Slide 38 :

Rappeler les conseils généraux sur ce qu'il faut faire de façon globale.

Slide 39 :

Récupérer et répondre les différentes questions posées.