Jeu sérieux proposé par la CCI Normandie pour sensibiliser à l'intelligence économique

http://www.jeu-ie.cci.fr/

Ce jeu permet de découvrir les bonnes pratiques dans plusieurs domaines à partir de 8 mini-jeux :

1- Le vol de matériel : • la sécurité des locaux (sensibiliser, protéger, détecter, le réseau des référents sûreté)
• hygiène informatique

2- La copie : • la clause de confidentialité (vis-à-vis d'un salarié et vis-à-vis d'un partenaire)
• la clause d'exclusivité

3- Le vol d'informations : • protéger ses données en déplacement
• sauvegarder ses données

4- Le piratage du site web : • la sécurisation des sites web
• la gestion de crise

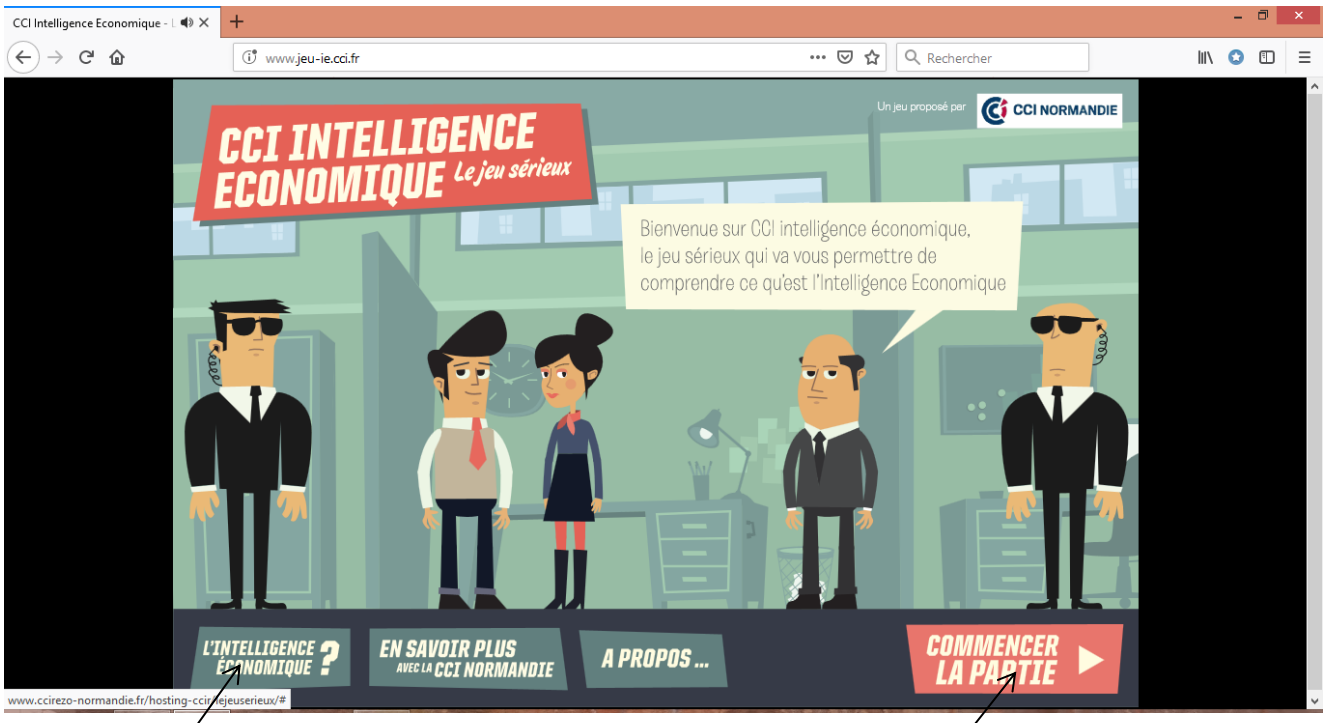
5- La concurrence déloyale : • la clause de non-concurrence (définition, application, sanctions)
• les outils de la propriété industrielle

6- L'escroquerie : • les faux ordres de virement informatique (définition, règles à suivre, reconnaître une attaque et que faire en cas d'attaque)

7- La Rançon : • externalisation et sécurité des systèmes d'information

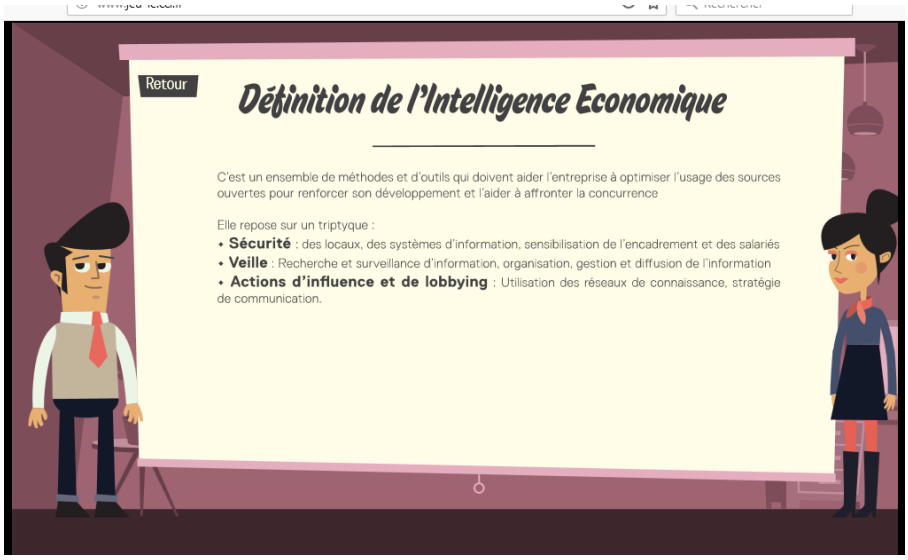
8- La stratégie offensive : • la communication en 10 points
• les réseaux sociaux et la e réputation (point de vue du salarié et de l'entreprise)

Mode d'emploi : **les 8 étapes vont être présentées ci-dessous ainsi que les définitions auxquelles les joueurs ont accès tout au long du process.**

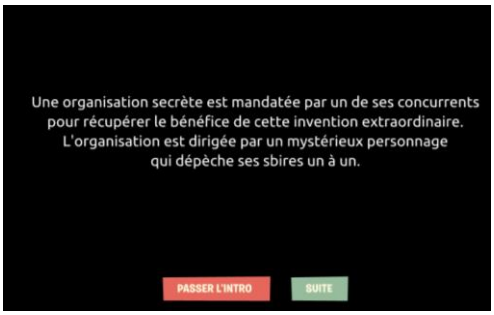


En cliquant on obtient la définition

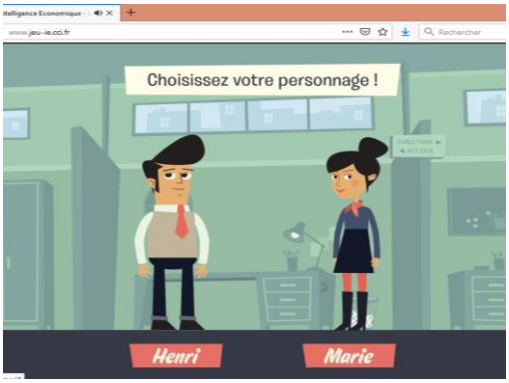
Permet de lancer le jeu

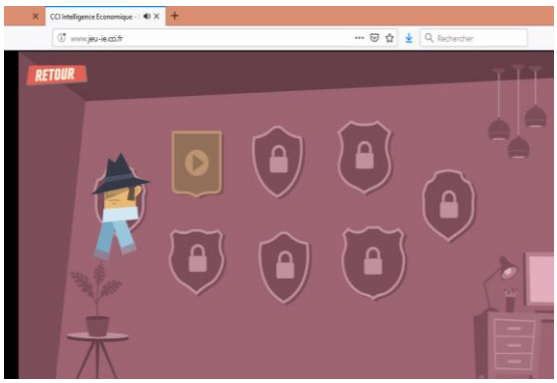


Lorsque le jeu est lancé plusieurs pages de présentation sont proposées (extrait ci-dessous). En cliquant sur SUITE les pages se succèdent et en cliquant sur PASSER L'INTRO on arrive directement au début de la partie.

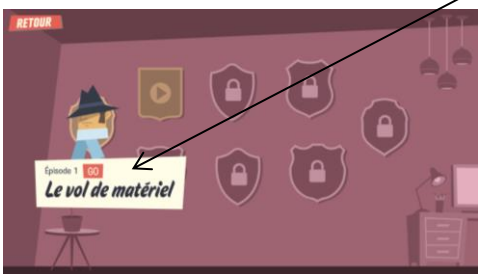


Puis il est demandé de choisir son personnage et le jeu peut commencer.

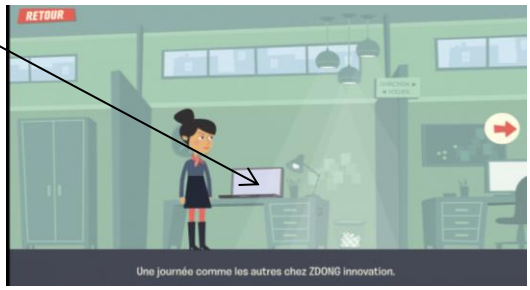




Cliquer

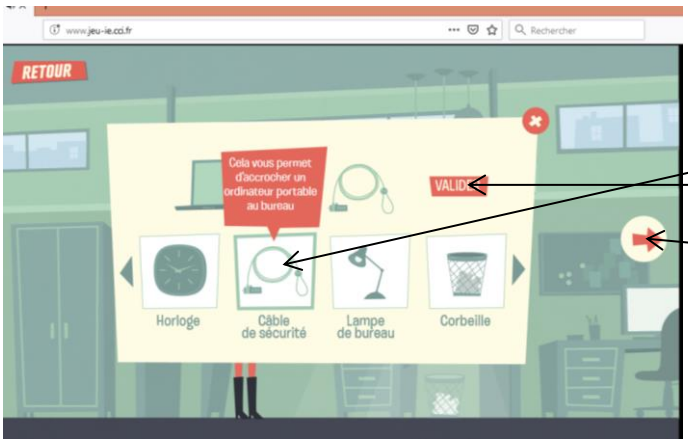


Cliquer



Cliquer sur les éléments que l'on juge nécessaires à valider. Ce sera toujours de cette façon que l'on validera les bons choix ou non…

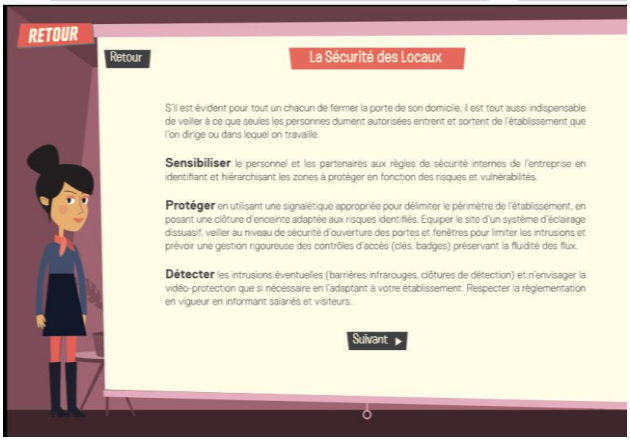
Voir exemple ci-dessous

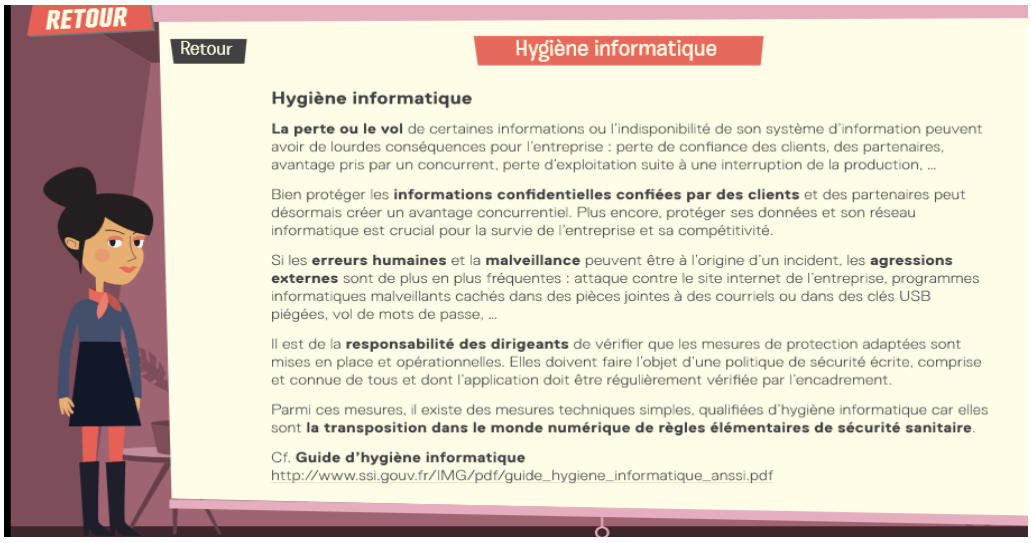


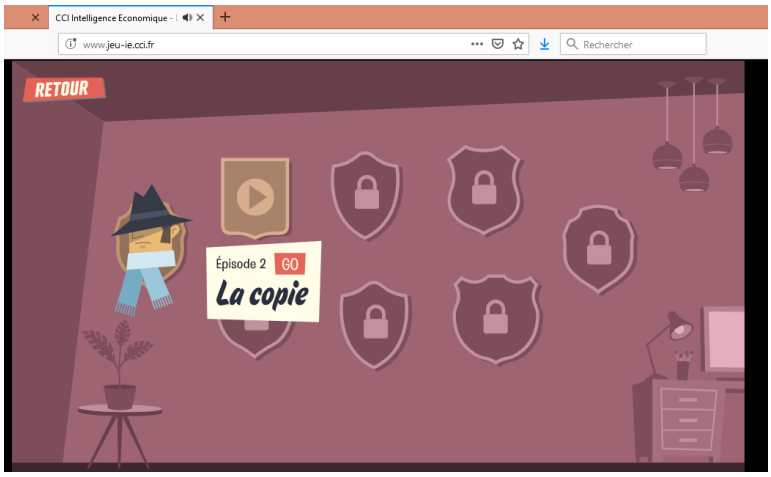
En cliquant sur Associer avec un objet on obtient une liste d'objets.
Cliquer sur l'objet de son choix puis Valider

Cliquer sur la flèche rouge

Une fois l'ensemble des étapes franchies les résultats s'affichent.
S'ils sont de couleur rouge la réponse est inexacte.
Les explications sont à portée de clic.
Choisir Rejouer si les réponses sont inexactes.
Choisir Menu pour passer à l'étape suivante.

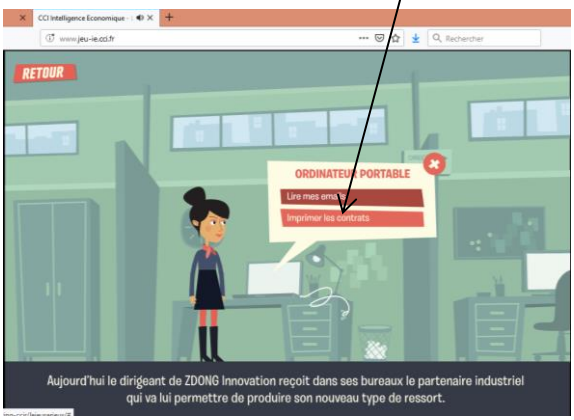


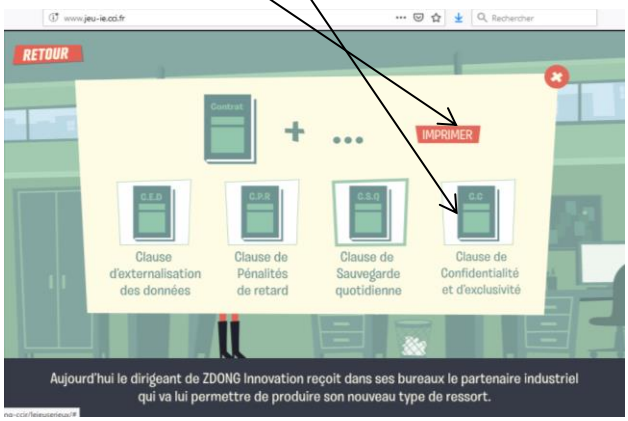


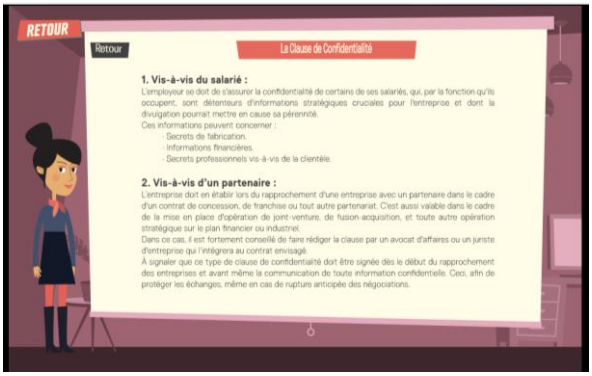


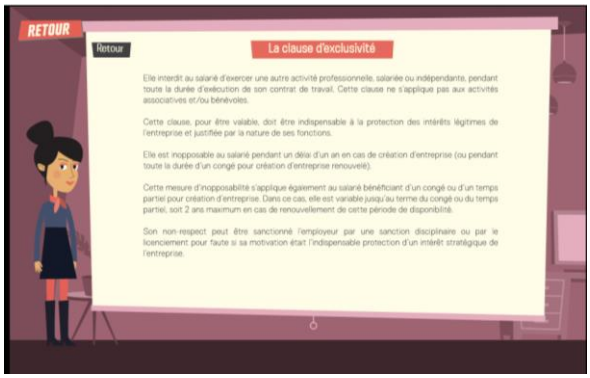
Après avoir lu les mails cliquer sur Imprimer les contrats

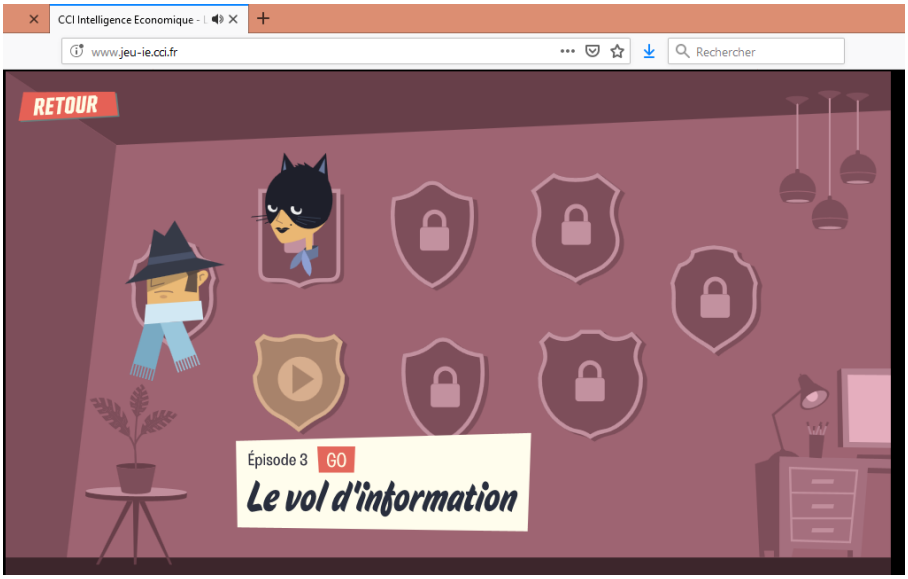
Choisir la clause de confidentialité et d'exclusivité puis Imprimer

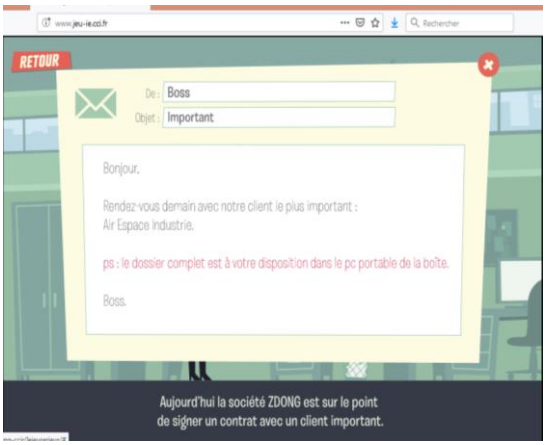


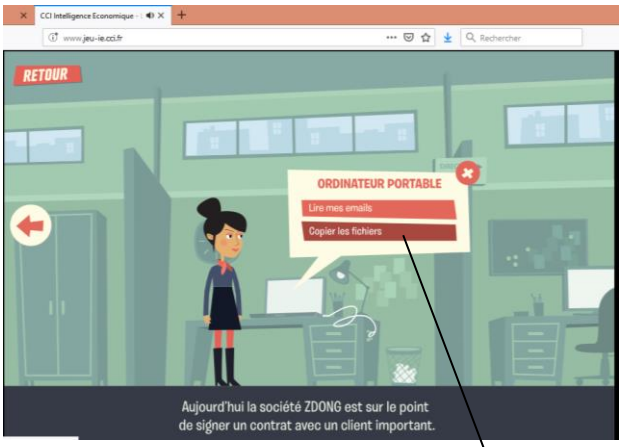


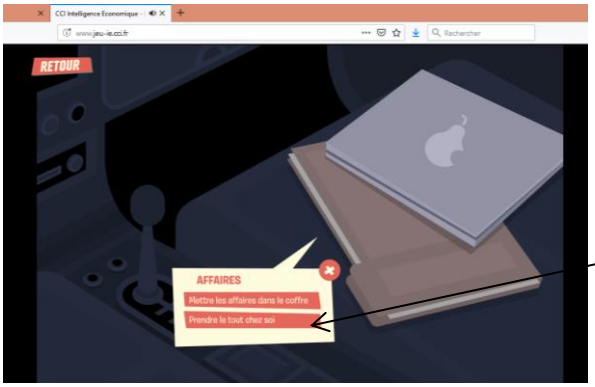






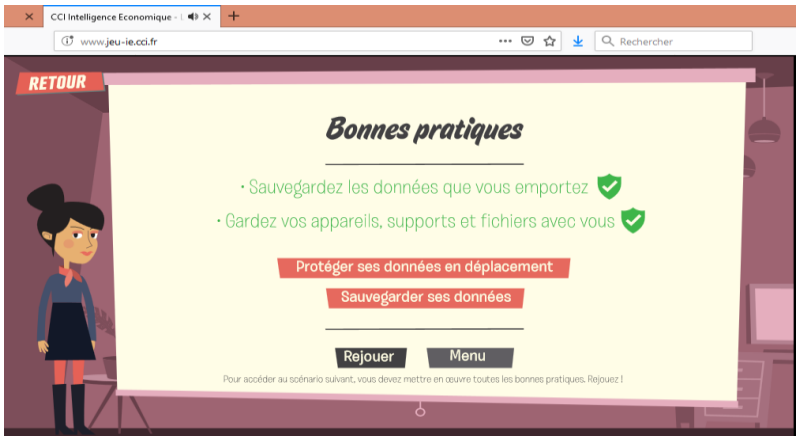


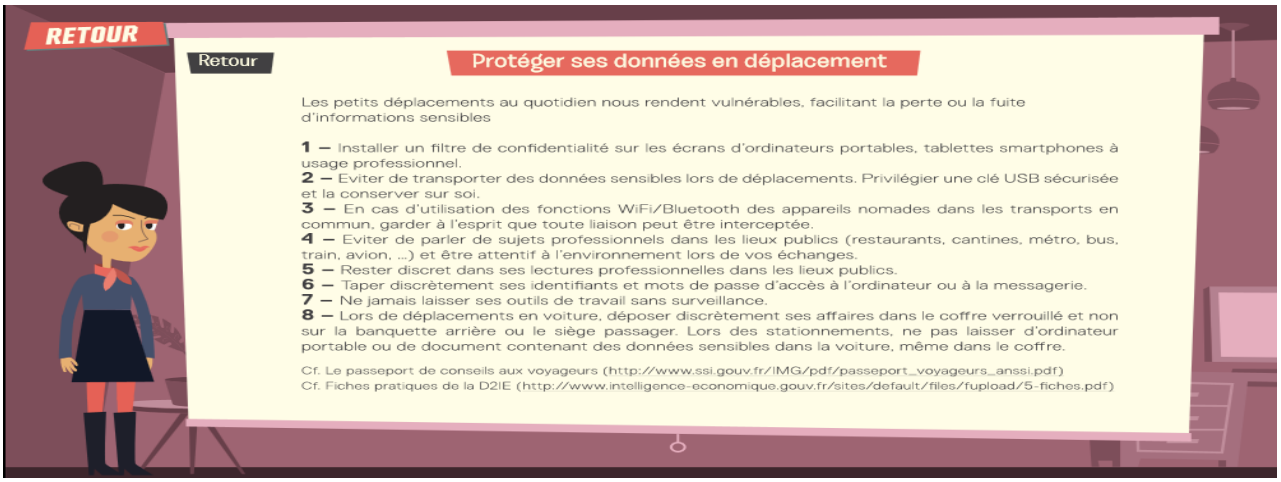


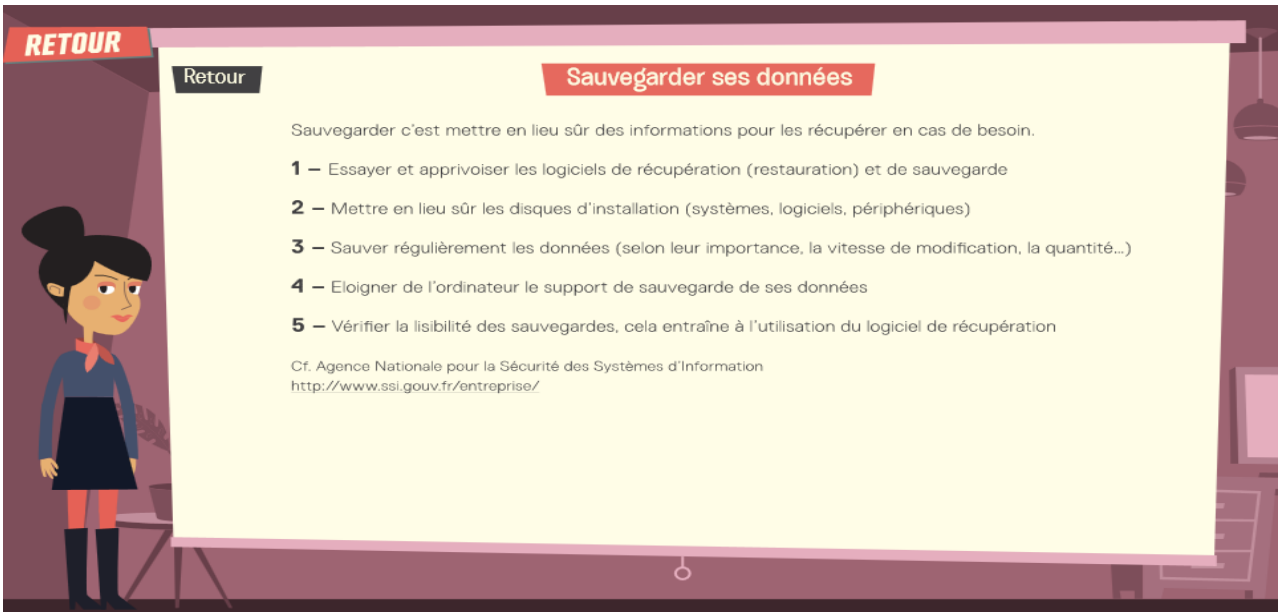


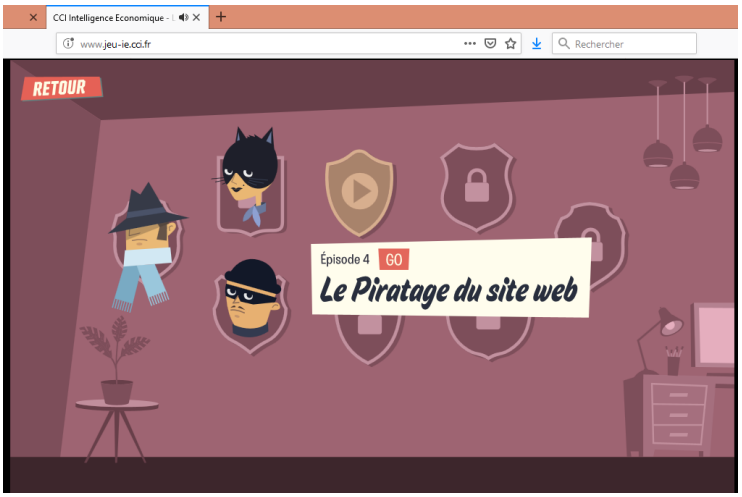
Après avoir lu les mails cliquer sur Copier les fichiers

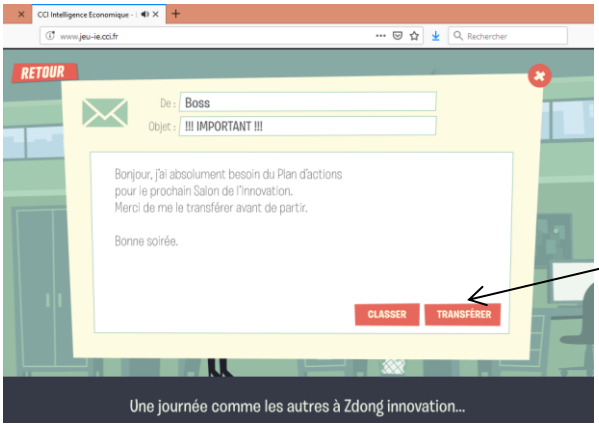
Choisir Prendre le tout chez soi


CCI Intelligence Economique
www.jeu-ie.cci.fr
Rechercher
RETOUR
Bonnes pratiques
• Sauvegardez les données que vous emportez
• Gardez vos appareils, supports et fichiers avec vous
Protéger ses données en déplacement
Sauvegarder ses données
Rejouer
Menu
Pour accéder au scénario suivant, vous devez mettre en œuvre toutes les bonnes pratiques. Rejouez !


RETOUR
Retour
Protéger ses données en déplacement
Les petits déplacements au quotidien nous rendent vulnérables, facilitant la perte ou la fuite d'informations sensibles
1 – Installer un filtre de confidentialité sur les écrans d'ordinateurs portables, tablettes smartphones à usage professionnel.
2 – Eviter de transporter des données sensibles lors de déplacements. Privilégier une clé USB sécurisée et la conserver sur soi.
3 – En cas d'utilisation des fonctions WiFi/Bluetooth des appareils nomades dans les transports en commun, garder à l'esprit que toute liaison peut être interceptée.
4 – Eviter de parler de sujets professionnels dans les lieux publics (restaurants, cantines, métro, bus, train, avion, ...) et être attentif à l'environnement lors de vos échanges.
5 – Rester discret dans ses lectures professionnelles dans les lieux publics.
6 – Taper discrètement ses identifiants et mots de passe d'accès à l'ordinateur ou à la messagerie.
7 – Ne jamais laisser ses outils de travail sans surveillance.
8 – Lors de déplacements en voiture, déposer discrètement ses affaires dans le coffre verrouillé et non sur la banquette arrière ou le siège passager. Lors des stationnements, ne pas laisser d'ordinateur portable ou de document contenant des données sensibles dans la voiture, même dans le coffre.
Cf. Le passeport de conseils aux voyageurs (http://www.ssi.gouv.fr/IMG/pdf/passeport_voyageurs_anssi.pdf)
Cf. Fiches pratiques de la D2IE (http://www.intelligence-economique.gouv.fr/sites/default/files/fupload/5-fiches.pdf)

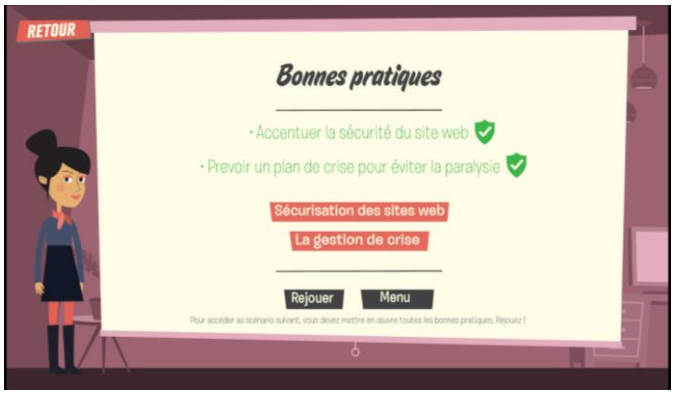

RETOUR
Retour
Sauvegarder ses données
Sauvegarder c'est mettre en lieu sûr des informations pour les récupérer en cas de besoin.
1 – Essayer et apprivoiser les logiciels de récupération (restauration) et de sauvegarde
2 – Mettre en lieu sûr les disques d'installation (systèmes, logiciels, périphériques)
3 – Sauver régulièrement les données (selon leur importance, la vitesse de modification, la quantité...)
4 – Eloigner de l'ordinateur le support de sauvegarde de ses données
5 – Vérifier la lisibilité des sauvegardes, cela entraîne à l'utilisation du logiciel de récupération
Cf. Agence Nationale pour la Sécurité des Systèmes d'Information
http://www.ssi.gouv.fr/entreprise/

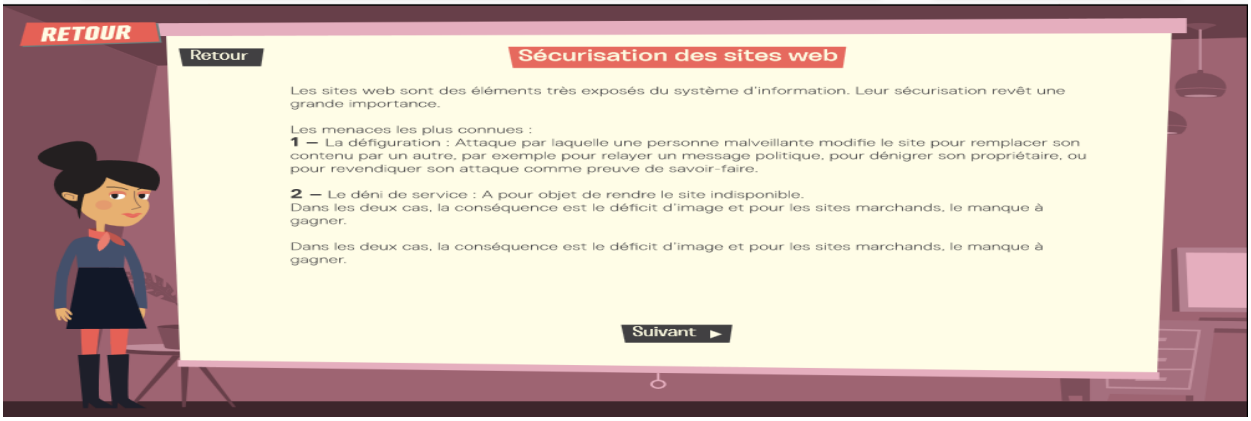




Après avoir lu chaque mail cliquer sur TRANSFERER

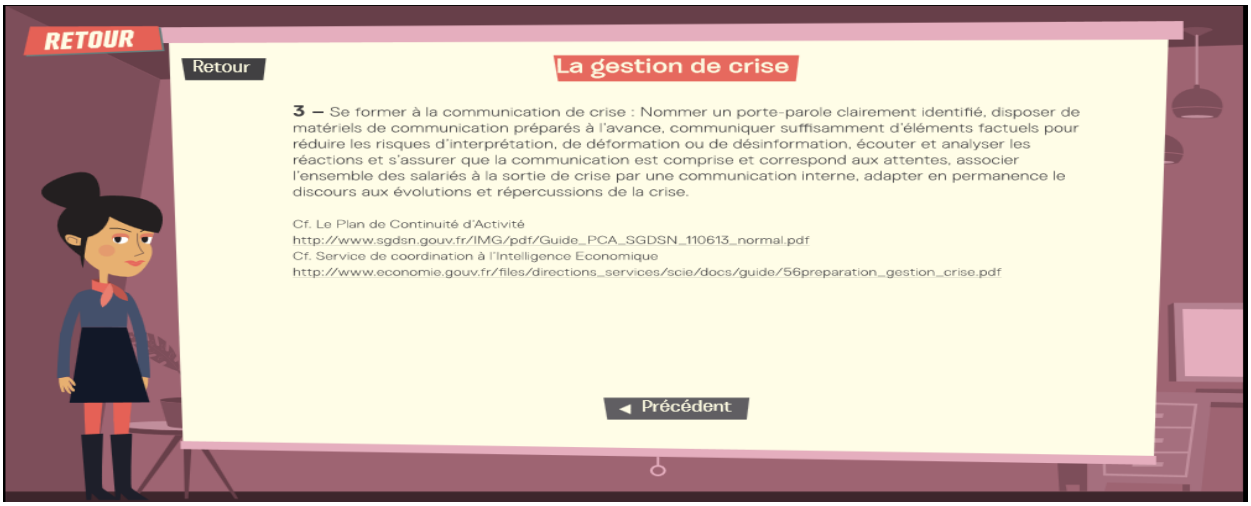
Voici le mail si tous les mails ont bien été transférés

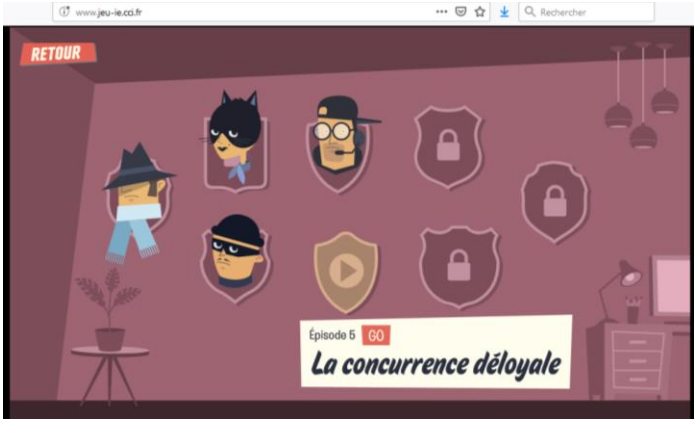


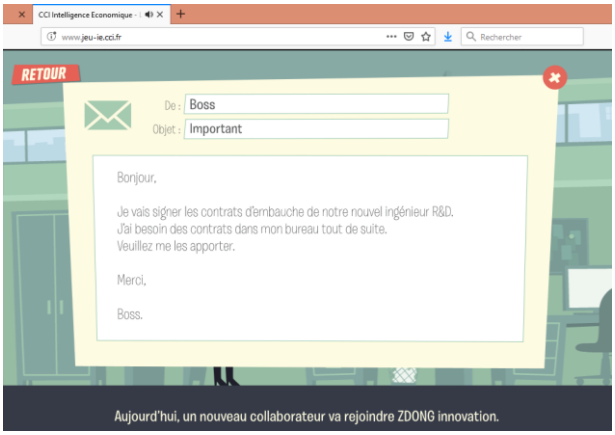

RETOUR
Retour
Sécurisation des sites web
Les sites web sont des éléments très exposés du système d'information. Leur sécurisation revêt une grande importance.
Les menaces les plus connues :
1 – La défiguration : Attaque par laquelle une personne malveillante modifie le site pour remplacer son contenu par un autre, par exemple pour relayer un message politique, pour dénigrer son propriétaire, ou pour revendiquer son attaque comme preuve de savoir-faire.
2 – Le déni de service : A pour objet de rendre le site indisponible.
Dans les deux cas, la conséquence est le déficit d'image et pour les sites marchands, le manque à gagner.
Dans les deux cas, la conséquence est le déficit d'image et pour les sites marchands, le manque à gagner.
Suivant

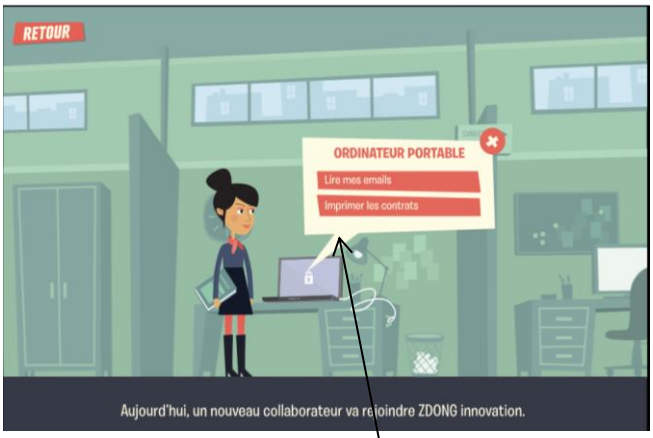

RETOUR
Retour
Sécurisation des sites web
Des scénarios d'attaque plus insidieux peuvent utiliser le site web comme porte d'entrée vers le système d'information de l'hébergeur ou du propriétaire du site. Il peut aussi être utilisé comme relais dans une attaque vers un tiers ou comme dépôt de contenus illégaux, mettant ainsi le propriétaire du site en difficulté.
Enfin, l'attaque peut aussi viser à tendre un piège aux clients habituels du site.
La protection contre ces menaces passe par des mesures préventives et par des mécanismes permettant de détecter des tentatives d'attaque.
Cf. Recommandations pour la sécurisation des sites web
http://www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf
Précédent

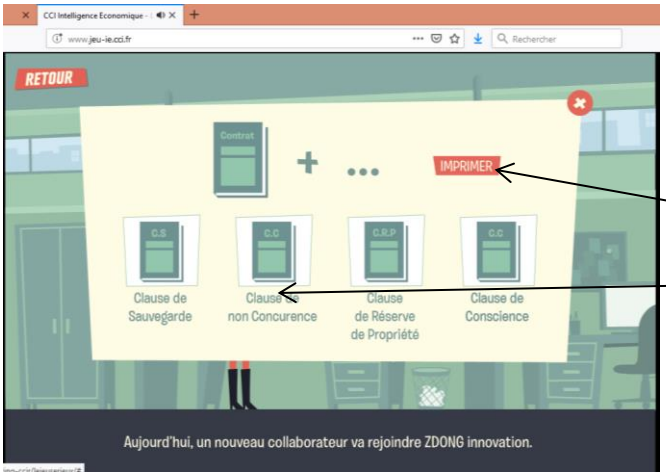

RETOUR
Retour
La gestion de crise
Les entreprises sont exposées à une diversité de risques (économiques, techniques, technologiques, humains, réglementaires, environnementaux, sociaux, informationnels, informatiques, ...) qu'il n'est pas toujours possible d'anticiper et qui peuvent avoir des conséquences fortement dommageables : perte de marchés, perte de savoir-faire, perte de crédibilité, ...
Lorsque la crise survient, l'entreprise doit savoir réagir très vite. Sa capacité de réaction et l'efficacité de son action sont liées à son degré de préparation.
C'est pourquoi l'entreprise doit identifier le plus en amont possible ses vulnérabilités et les menaces associées et prévoir comment réagir.
1 – Identifier les activités critiques de l'entreprise et ses vulnérabilités : Activités qui doivent être assurées pour ne pas mettre en péril la pérennité de l'entreprise.
2 – Constituer la boîte à outils d'urgence : Annuaires de responsables, plans des lieux, moyens extérieurs mobilisables, ... et le plan de continuation de l'activité (liste des mesures à prendre, plan de récupération des données informatiques, ...)
Suivant


RETOUR
Retour
La gestion de crise
3 – Se former à la communication de crise : Nommer un porte-parole clairement identifié, disposer de matériels de communication préparés à l'avance, communiquer suffisamment d'éléments factuels pour réduire les risques d'interprétation, de déformation ou de désinformation, écouter et analyser les réactions et s'assurer que la communication est comprise et correspond aux attentes, associer l'ensemble des salariés à la sortie de crise par une communication interne, adapter en permanence le discours aux évolutions et répercussions de la crise.
Cf. Le Plan de Continuité d'Activité
http://www.sgdsn.gouv.fr/IMG/pdf/Guide_PCA_SGDSN_110613_normal.pdf
Cf. Service de coordination à l'Intelligence Economique
http://www.economie.gouv.fr/files/directions_services/scie/docs/guide/56preparation_gestion_crise.pdf
Précédent

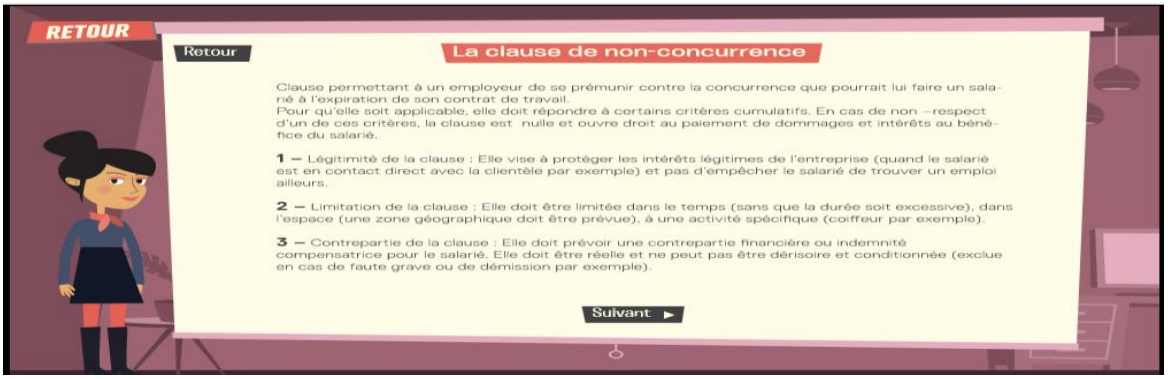


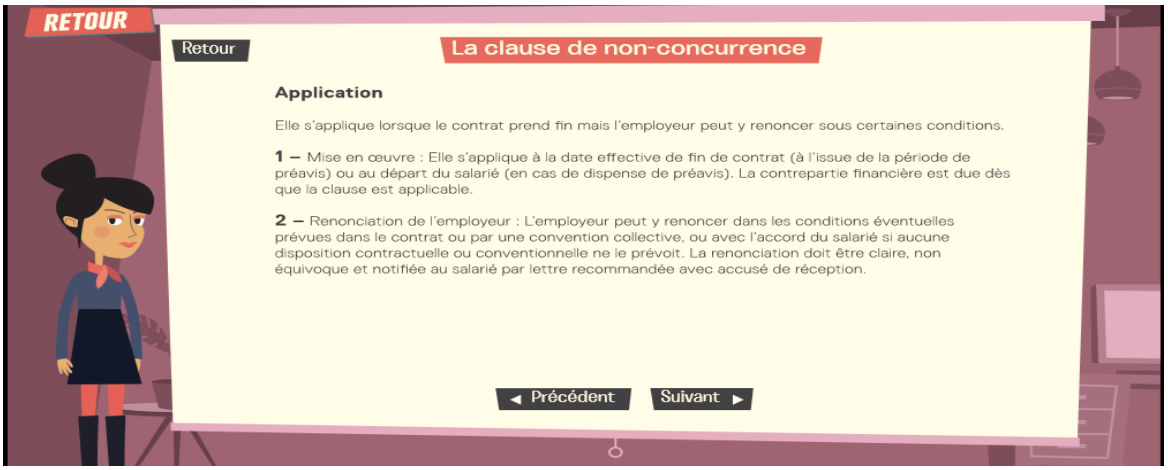




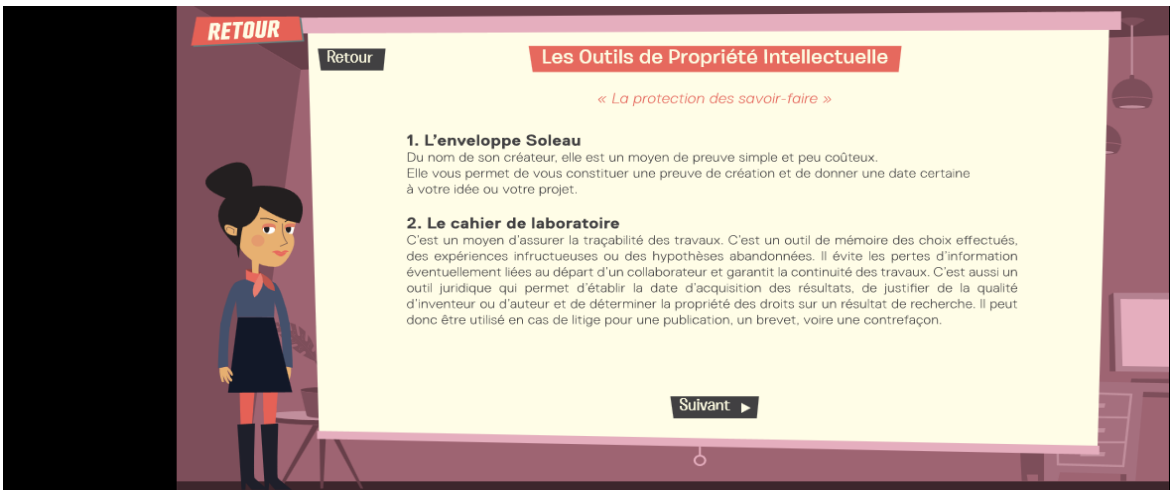


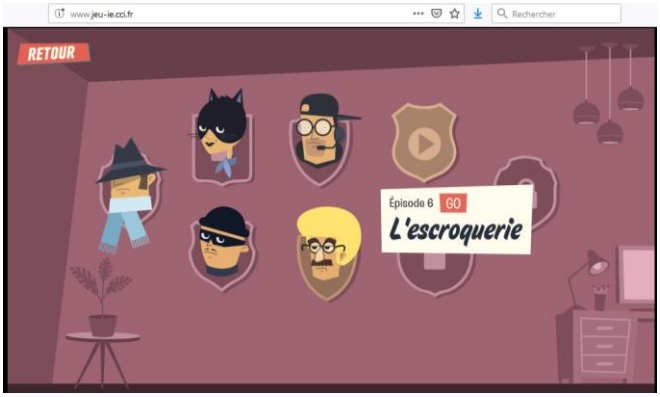
Une fois le mail lu cliquer sur Imprimer les contrats.
Puis choisir Clause de non concurrence et Imprimer

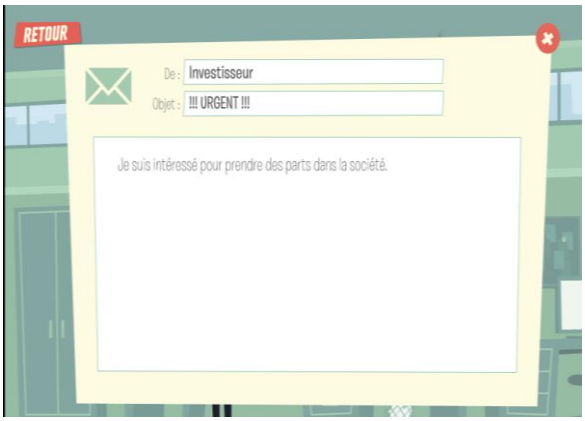

RETOUR
Retour
La clause de non-concurrence
Clause permettant à un employeur de se prémunir contre la concurrence que pourrait lui faire un salarié à l'expiration de son contrat de travail.
Pour qu'elle soit applicable, elle doit répondre à certains critères cumulatifs. En cas de non –respect d'un de ces critères, la clause est nulle et ouvre droit au paiement de dommages et intérêts au bénéfice du salarié.
1 – Légitimité de la clause : Elle vise à protéger les intérêts légitimes de l'entreprise (quand le salarié est en contact direct avec la clientèle par exemple) et pas d'empêcher le salarié de trouver un emploi ailleurs.
2 – Limitation de la clause : Elle doit être limitée dans le temps (sans que la durée soit excessive), dans l'espace (une zone géographique doit être prévue), à une activité spécifique (coiffeur par exemple).
3 – Contrepartie de la clause : Elle doit prévoir une contrepartie financière ou indemnité compensatrice pour le salarié. Elle doit être réelle et ne peut pas être dérisoire et conditionnée (exclue en cas de faute grave ou de démission par exemple).
Suivant


RETOUR
Retour
La clause de non-concurrence
Application
Elle s'applique lorsque le contrat prend fin mais l'employeur peut y renoncer sous certaines conditions.
1 – Mise en œuvre : Elle s'applique à la date effective de fin de contrat (à l'issue de la période de préavis) ou au départ du salarié (en cas de dispense de préavis). La contrepartie financière est due dès que la clause est applicable.
2 – Renonciation de l'employeur : L'employeur peut y renoncer dans les conditions éventuelles prévues dans le contrat ou par une convention collective, ou avec l'accord du salarié si aucune disposition contractuelle ou conventionnelle ne le prévoit. La renonciation doit être claire, non équivoque et notifiée au salarié par lettre recommandée avec accusé de réception.
Précédent
Suivant

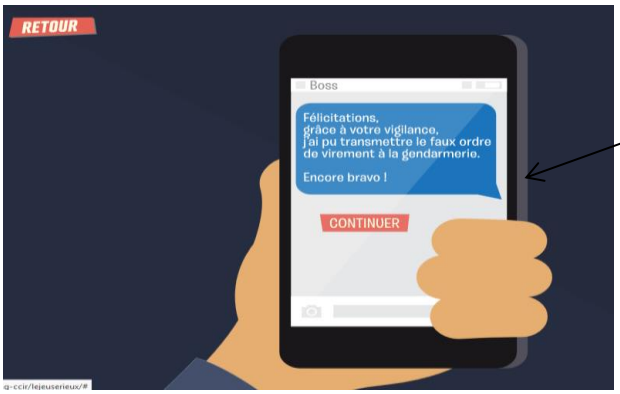

RETOUR
Retour
La clause de non-concurrence
Sanction en cas de non-respect
1 – La violation d'une clause de non-concurrence par le salarié entraîne la restitution de l'indemnité compensatrice.
2 – Le juge peut condamner le salarié au versement de dommages et intérêts.
Cf. Les fiches de la D2IE
http://www.intelligence-economique.gouv.fr/sites/default/files/fupload/20-fiches.pdf
Précédent


RETOUR
Retour
Les Outils de Propriété Intellectuelle
« La protection des savoir-faire »
1. L'enveloppe Soleau
Du nom de son créateur, elle est un moyen de preuve simple et peu coûteux.
Elle vous permet de vous constituer une preuve de création et de donner une date certaine à votre idée ou votre projet.
2. Le cahier de laboratoire
C'est un moyen d'assurer la traçabilité des travaux. C'est un outil de mémoire des choix effectués, des expériences infructueuses ou des hypothèses abandonnées. Il évite les pertes d'information éventuellement liées au départ d'un collaborateur et garantit la continuité des travaux. C'est aussi un outil juridique qui permet d'établir la date d'acquisition des résultats, de justifier de la qualité d'inventeur ou d'auteur et de déterminer la propriété des droits sur un résultat de recherche. Il peut donc être utilisé en cas de litige pour une publication, un brevet, voire une contrefaçon.
Suivant

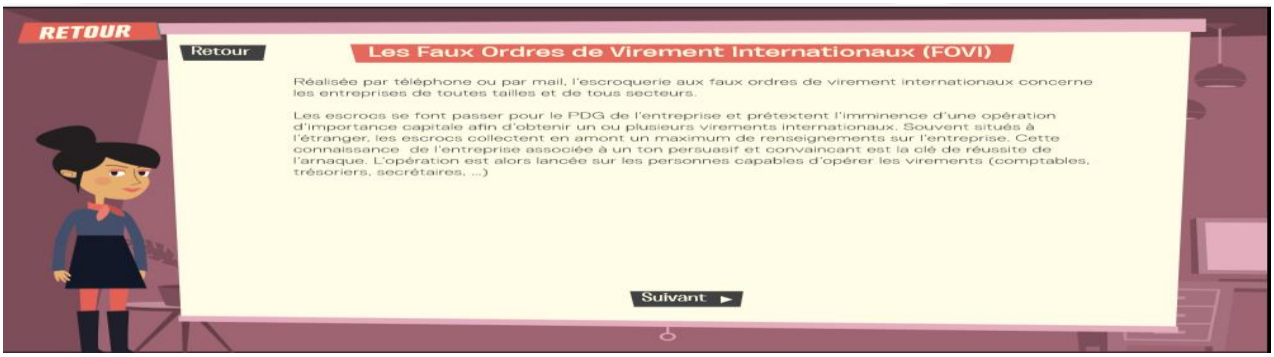




Comme déjà vu précédemment choisir TRANSFERER et ce message s'affichera

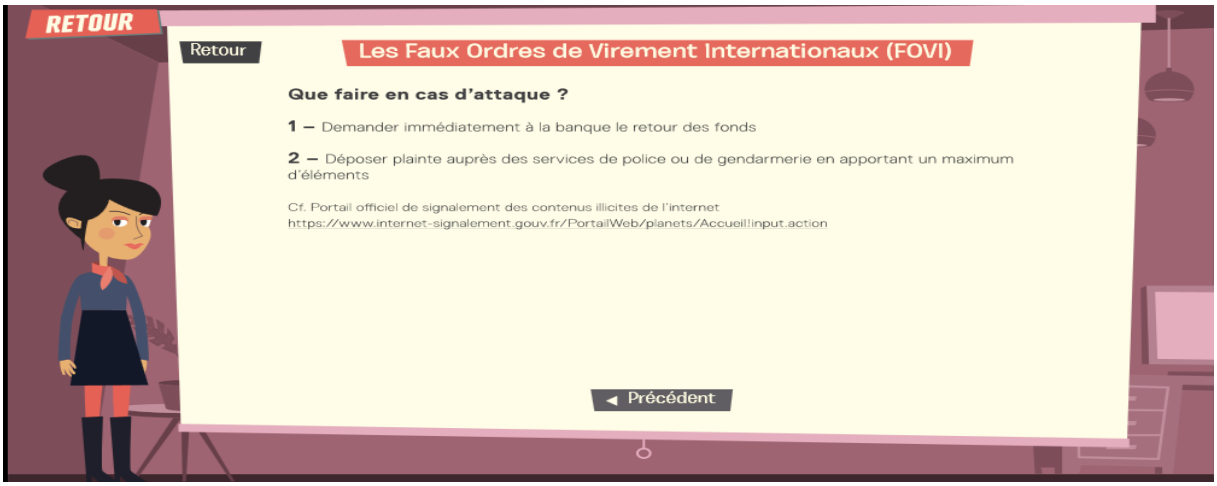


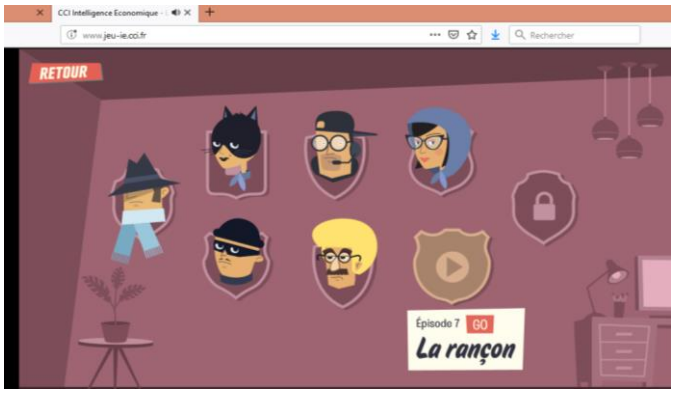

RETOUR
Bonnes pratiques
• Ne jamais déroger aux procédures de virements financiers
Les Faux Ordres de Virement Internationaux (FOVI)
Rejouer
Menu
Pour accéder au scénario suivant, vous devez mettre en œuvre toutes les bonnes pratiques. Rejouez !

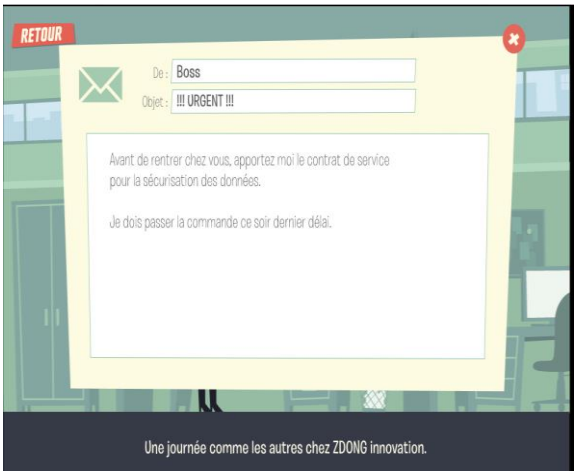

RETOUR
Retour
Les Faux Ordres de Virement Internationaux (FOVI)
Réalisée par téléphone ou par mail, l'escroquerie aux faux ordres de virement internationaux concerne les entreprises de toutes tailles et de tous secteurs.
Les escrocs se font passer pour le PDG de l'entreprise et prétextent l'imminence d'une opération d'importance capitale afin d'obtenir un ou plusieurs virements internationaux. Souvent situés à l'étranger, les escrocs collectent en amont un maximum de renseignements sur l'entreprise. Cette connaissance de l'entreprise associée à un ton persuasif et convaincant est la clé de réussite de l'arnaque. L'opération est alors lancée sur les personnes capables d'opérer les virements (comptables, trésoriers, secrétaires, ...)
Suivant

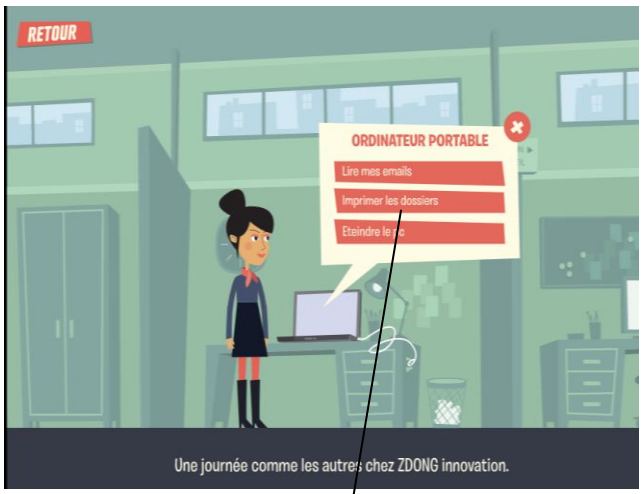

RETOUR
Retour
Les Faux Ordres de Virement Internationaux (FOVI)
Quelques règles simples
1 – rappeler aux collaborateurs la nécessité d'avoir un usage prudent des réseaux sociaux privés et professionnels. Les alerter sur l'importance de ne pas y divulguer d'informations concernant le fonctionnement de l'entreprise.
2 – Sensibiliser régulièrement les employés des services comptables, trésorerie, secrétariat, standard, de ce type d'escroquerie. Prendre l'habitude d'en informer les remplaçants sur ces postes.
3 – Instaurer des procédures de vérification et de signatures multiples pour les paiements internationaux.
4 – Rompre la chaîne des mails pour les courriers se rapportant à des virements internationaux en saisissant soi-même l'adresse habituelle du donneur d'ordre.
5 – Maintenir à jour le système de sécurité informatique.
6 – Accentuer la vigilance sur les périodes de congés scolaires, les jours fériés et les jours de paiement des loyers.
Précédent
Suivant

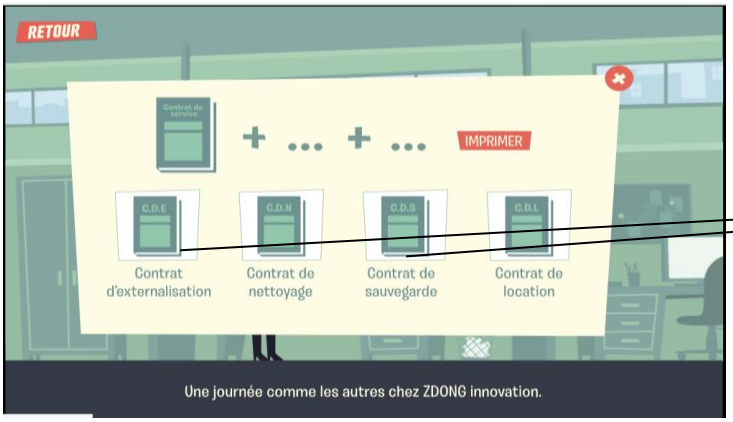

RETOUR
Retour
Les Faux Ordres de Virement Internationaux (FOVI)
Reconnaître les signes d'une attaque
1 – Une demande de virement à l'international, non planifiée, au caractère urgent et confidentiel : Contacter son interlocuteur habituel avec les coordonnées connues de la société.
2 – Se méfier de tout changement de coordonnées téléphoniques ou mails. La communication d'un nouveau numéro à indicatif français n'est pas une garantie.
3 – Se méfier d'un contact qui fera usage de flatterie ou de menace dans le but de manipuler son interlocuteur.
4 – Pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera une abondance de détails sur l'entreprise et son environnement : données personnelles concernant le chef d'entreprise ou ses collaborateurs
Précédent
Suivant



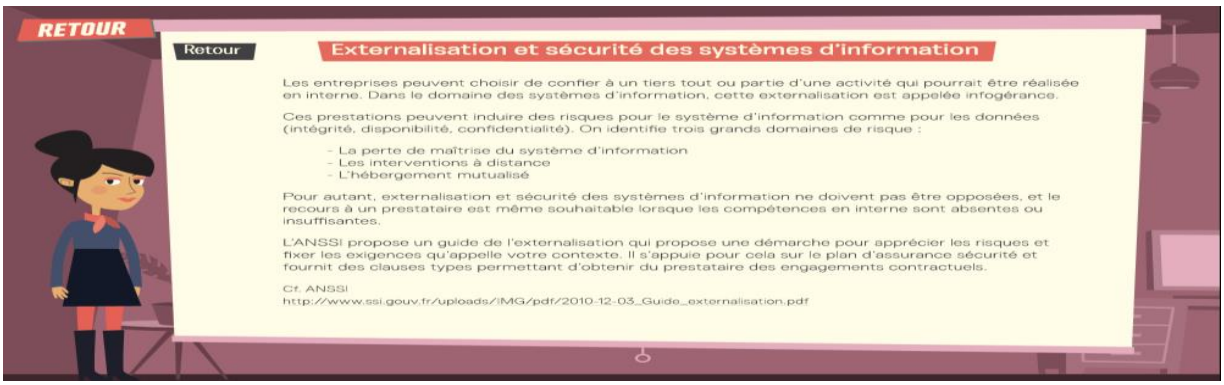


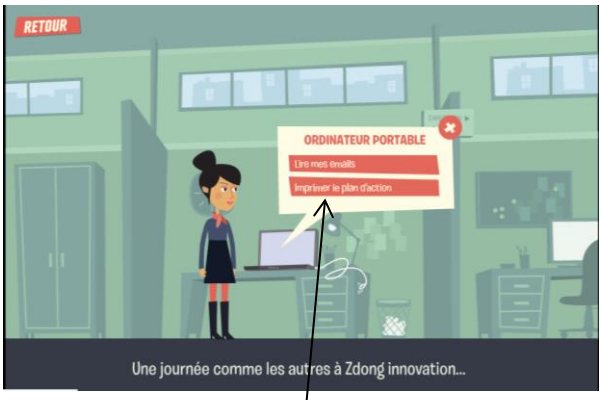


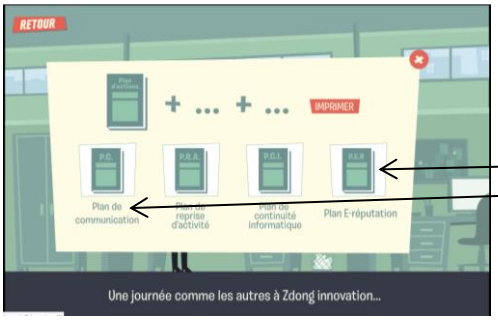




Choisir Imprimer les dossiers
Sélectionner C.D.E. et C.D.S
Choisir Imprimer

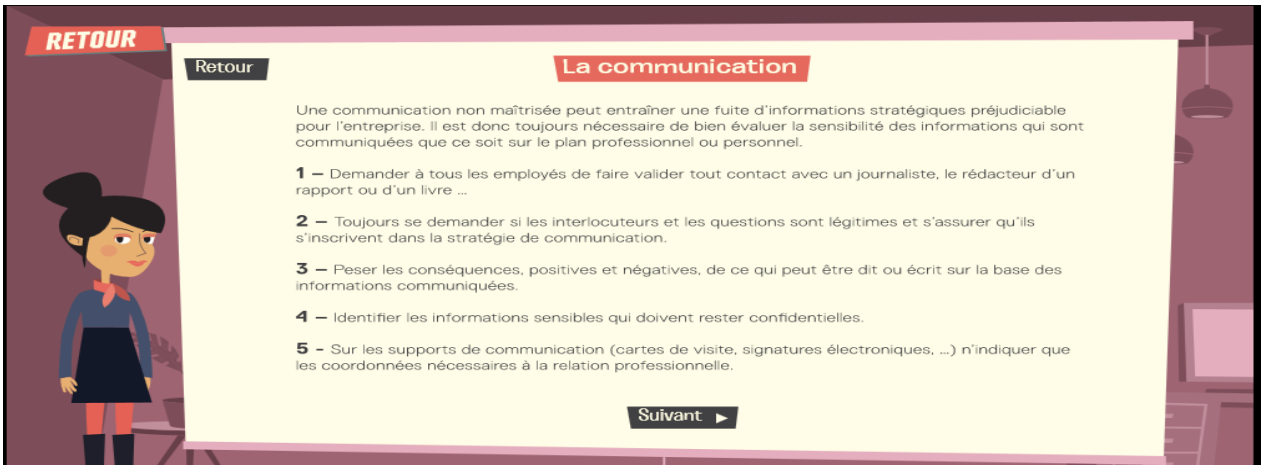


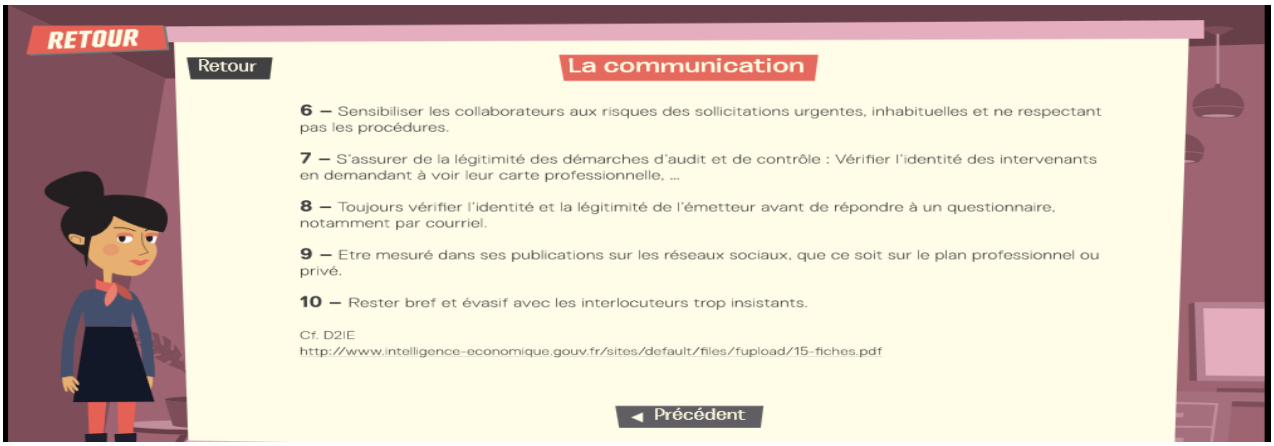




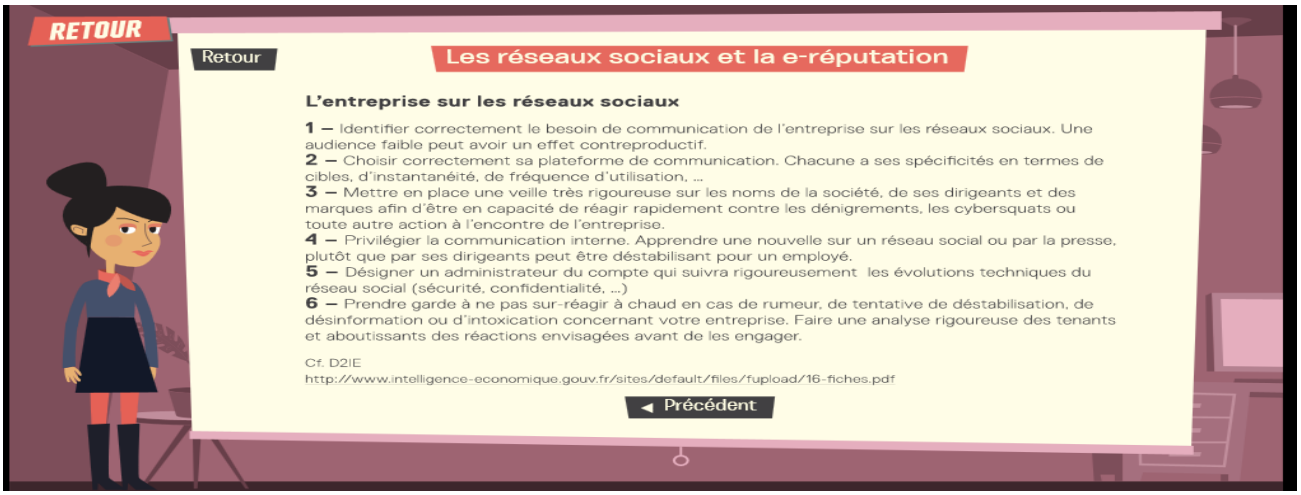
Choisir Imprimer le plan d'action
Sélectionner P.C. et P.E.R.
Choisir Imprimer


RETOUR
Bonnes pratiques
• La communication d'influence
• Outils de veille e-reputation
La communication
Les réseaux sociaux et la e-réputation
Rejouer
Menu
Pour accéder au scénario suivant, vous devez mettre en œuvre toutes les bonnes pratiques. Rejouez !


RETOUR
Retour
La communication
Une communication non maîtrisée peut entraîner une fuite d'informations stratégiques préjudiciable pour l'entreprise. Il est donc toujours nécessaire de bien évaluer la sensibilité des informations qui sont communiquées que ce soit sur le plan professionnel ou personnel.
1 – Demander à tous les employés de faire valider tout contact avec un journaliste, le rédacteur d'un rapport ou d'un livre ...
2 – Toujours se demander si les interlocuteurs et les questions sont légitimes et s'assurer qu'ils s'inscrivent dans la stratégie de communication.
3 – Peser les conséquences, positives et négatives, de ce qui peut être dit ou écrit sur la base des informations communiquées.
4 – Identifier les informations sensibles qui doivent rester confidentielles.
5 - Sur les supports de communication (cartes de visite, signatures électroniques, ...) n'indiquer que les coordonnées nécessaires à la relation professionnelle.
Suivant


RETOUR
Retour
La communication
6 – Sensibiliser les collaborateurs aux risques des sollicitations urgentes, inhabituelles et ne respectant pas les procédures.
7 – S'assurer de la légitimité des démarches d'audit et de contrôle : Vérifier l'identité des intervenants en demandant à voir leur carte professionnelle, ...
8 – Toujours vérifier l'identité et la légitimité de l'émetteur avant de répondre à un questionnaire, notamment par courriel.
9 – Etre mesuré dans ses publications sur les réseaux sociaux, que ce soit sur le plan professionnel ou privé.
10 – Rester bref et évasif avec les interlocuteurs trop insistants.
Cf. D2IE
http://www.intelligence-economique.gouv.fr/sites/default/files/fupload/15-fiches.pdf
Précédent


RETOUR
Retour
Les réseaux sociaux et la e-réputation
L'utilisation des réseaux sociaux peut être privée et/ou professionnelle. Il faut néanmoins être bien conscient qu'une utilisation considérée comme privée peut bien souvent avoir des répercussions professionnelles.
Le salarié sur les réseaux sociaux
1 – Sensibiliser les personnels en lien avec l'entreprise grâce à une charte d'utilisation des réseaux sociaux. Leur rappeler les lois et devoirs de tout employé comme par exemple la loyauté, la discrétion ou le devoir de réserve.
2 – Prendre conscience qu'une information (texte, photo, ...) publiée sur internet n'appartient plus à celui qui la met en ligne et peut difficilement être effacée.
3 – Eviter de communiquer des informations personnelles précises sur les réseaux sociaux (date et lieu de naissance, numéro de téléphone, ...)
4 – Etre attentif aux données de géolocalisation ouvertes sur les réseaux sociaux. Elles peuvent apporter des renseignements sur son emploi du temps professionnel : absence, vacances, mission, ...
5 – Veiller à ce que les informations publiées sur les réseaux sociaux ne comportent pas d'information sensible concernant l'entreprise : organigramme précis, systèmes techniques utilisés, mission à l'étranger, contrat en cours de négociation, conflit social frémissant, ...
Suivant


RETOUR
Retour
Les réseaux sociaux et la e-réputation
L'entreprise sur les réseaux sociaux
1 – Identifier correctement le besoin de communication de l'entreprise sur les réseaux sociaux. Une audience faible peut avoir un effet contreproductif.
2 – Choisir correctement sa plateforme de communication. Chacune a ses spécificités en termes de cibles, d'instantanéité, de fréquence d'utilisation, ...
3 – Mettre en place une veille très rigoureuse sur les noms de la société, de ses dirigeants et des marques afin d'être en capacité de réagir rapidement contre les dénigrements, les cybersquats ou toute autre action à l'encontre de l'entreprise.
4 – Privilégier la communication interne. Apprendre une nouvelle sur un réseau social ou par la presse, plutôt que par ses dirigeants peut être déstabilisant pour un employé.
5 – Désigner un administrateur du compte qui suivra rigoureusement les évolutions techniques du réseau social (sécurité, confidentialité, ...)
6 – Prendre garde à ne pas sur-réagir à chaud en cas de rumeur, de tentative de déstabilisation, de désinformation ou d'intoxication concernant votre entreprise. Faire une analyse rigoureuse des tenants et aboutissants des réactions envisagées avant de les engager.
Cf. D2IE
http://www.intelligence-economique.gouv.fr/sites/default/files/fupload/16-fiches.pdf
Précédent