RestartVET

RESTART VET:

An innovative approach to support VET teachers/trainers through the digital transformation of VET education

Digital Safety and Security (French)

Co-funded by the Erasmus+ Programme of the European Union

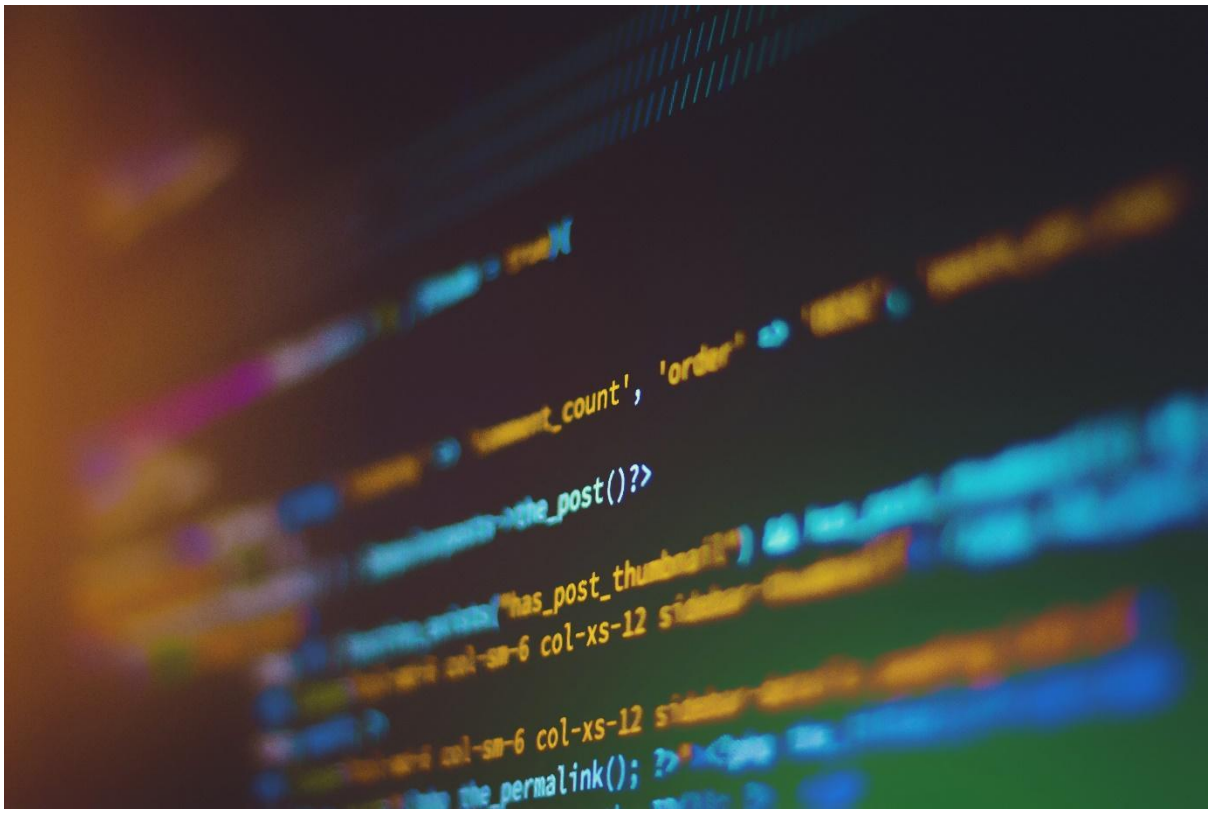
Sûreté et sécurité numériques

Introduction :

Certains des aspects les plus courants de notre vie quotidienne auraient ressemblé à de la science-fiction il y a seulement quelques décennies ! L'utilisation d'appareils mobiles pour la quasi-totalité de nos besoins technologiques, la vitesse et la portée d'Internet, la richesse des applications et des solutions informatiques, ont remodelé notre expérience quotidienne, le commerce, l'éducation, le divertissement, la recherche, et même nos vies interpersonnelles.

On estime qu'il y a actuellement 4,66 milliards d'utilisateurs actifs de l'internet dans le monde sur une population mondiale de 7,83 milliards d'habitants, ce qui signifie que 92,6 % des habitants de la planète ont accès au World Wide Web par le biais de divers appareils. En outre, 56,8 % de la population mondiale utilisent régulièrement des applications de médias sociaux dans leur vie personnelle et professionnelle.

Avec une telle portée de la technologie, il n'est pas étonnant qu'il y ait plusieurs risques impliqués qui peuvent avoir un impact négatif sur l'expérience et les menaces qui peuvent compromettre la sécurité des utilisateurs dans le monde numérique. Dans ce module, nous examinerons et présenterons les principaux aspects de la sûreté et de la sécurité numériques, tant pour l'utilisation générale des outils en ligne que pour l'aspect apprentissage/enseignement dans le secteur de l'EFP.



Objectifs d'apprentissage :

À la fin de ce module, vous :

● aurez une compréhension des risques liés à l'utilisation des outils numériques et en ligne.

● aurez une conscience accrue concernant la sûreté et la sécurité numériques.

● aurez acquis des compétences de base pour répondre à vos besoins en matière de sûreté et de sécurité numériques.

● aurez acquis des compétences qui vous permettront de maintenir une expérience d'apprentissage en ligne sûre et sécurisée pour vos apprenants.

● être habilité et motivé à préserver la sûreté et la sécurité numériques et à adopter les meilleures pratiques et solutions les plus récentes.

Conseils généraux au formateur :

Assurez-vous qu'il existe une compréhension commune des termes utilisés dans ce module afin de garantir une diffusion fluide du contenu ; il peut être utile de passer un peu de temps à faire la distinction entre différents mots et différents outils.

Demandez aux apprenants de réfléchir à leur propre utilisation des outils numériques et en ligne et à l'étendue de cette utilisation ; demandez-leur peut-être comment leur vie serait différente, plus difficile ou même meilleure si, pendant les 24 heures suivantes, il n'y avait pas d'Internet disponible.

Invitez les apprenants à partager leurs expériences ou leurs préoccupations concernant la sécurité et la sûreté numériques, notez ces questions et reliez-les au contenu du module si possible. Si certaines questions ne sont pas couvertes, essayez de proposer d'autres ressources extérieures.

1. Quels sont les principaux risques et menaces qui existent en ligne ?

Adware

Un adware est un logiciel indésirable conçu pour afficher des publicités sur votre écran, également appelées pop-ups.

Voici quelques signes révélateurs typiques de la présence de logiciels publicitaires sur votre système :

● Des publicités apparaissent à des endroits où elles ne devraient pas être.

● La page d'accueil de votre navigateur Web a mystérieusement changé sans votre permission.

● Des pages Web que vous visitez habituellement ne s'affichent pas correctement.

● Des liens de sites Web redirigent vers des sites différents de ceux auxquels vous vous attendiez.

● Votre navigateur web ralentit à vue d'œil.

● De nouvelles barres d'outils, extensions ou plugins envahissent soudainement votre navigateur.

● Votre ordinateur commence à installer automatiquement des applications logicielles indésirables.

Malvertising

Le malvertising - ou publicité malveillante - est une technique de cyberattaque qui consiste à injecter du code malveillant dans les publicités numériques. Difficiles à détecter tant par les internautes que par les éditeurs, ces publicités infectées sont généralement diffusées aux consommateurs par des réseaux publicitaires légitimes. Comme les publicités sont affichées

à tous les visiteurs d'un site web, pratiquement chaque visiteur de la page risque d'être infecté.

Phishing

Le phishing est une attaque généralement envoyée par courrier électronique qui incite les utilisateurs finaux à cliquer sur un lien ou une pièce jointe malveillante. Les attaquants peuvent utiliser le phishing pour s'implanter dans une organisation, souvent en distribuant des logiciels malveillants.

Hameçonnage par harponnage

Le spear phishing est une méthode de phishing qui cible des individus ou des groupes spécifiques au sein d'une organisation. Il s'agit d'une variante puissante du phishing, une tactique malveillante qui utilise les courriels, les médias sociaux, la messagerie instantanée et d'autres plates-formes pour amener les utilisateurs à divulguer des informations personnelles ou à effectuer des actions qui entraînent une compromission du réseau, une perte de données ou une perte financière. Une attaque typique de spear phishing comprend un e-mail et une pièce jointe. L'e-mail contient des informations spécifiques à la cible, notamment son nom et son rang au sein de l'entreprise. Cette tactique d'ingénierie sociale augmente les chances que la victime effectue toutes les actions nécessaires à l'infection, notamment l'ouverture de l'e-mail et de la pièce jointe incluse.

Cybersquattage (squattage de domaine)

Le cybersquattage est l'enregistrement et l'utilisation non autorisés de noms de domaines Internet identiques ou similaires à des marques commerciales, des marques de service, des noms de sociétés ou des noms de personnes, dans le but de créer une confusion, d'attirer malicieusement des utilisateurs ou de mener des escroqueries.

Spyware

Les logiciels espions sont des logiciels au comportement malveillant qui visent à recueillir des informations sur une personne ou une organisation et à les envoyer à une autre entité de manière à nuire à l'utilisateur.

Smishing

Les attaques par smishing utilisent le service de messages courts ou SMS, plus communément appelés messages texte.

Le smishing consiste à voler vos données personnelles en vous faisant passer pour un représentant de votre banque, à vous faire cliquer sur un lien dans le message texte pour vous connecter à la page Web de votre banque et vérifier un récent débit suspect, à vous demander d'appeler le numéro du service clientèle, commodément inclus dans le message texte, pour leur parler d'un récent débit suspect ou d'un compte compromis.

Les exemples ci-dessus ne représentent qu'une sélection limitée des menaces en ligne qui sévissent actuellement et qui visent des millions d'utilisateurs chaque jour. Il est conseillé aux utilisateurs de se tenir informés de l'évolution de la situation et des nouvelles menaces en

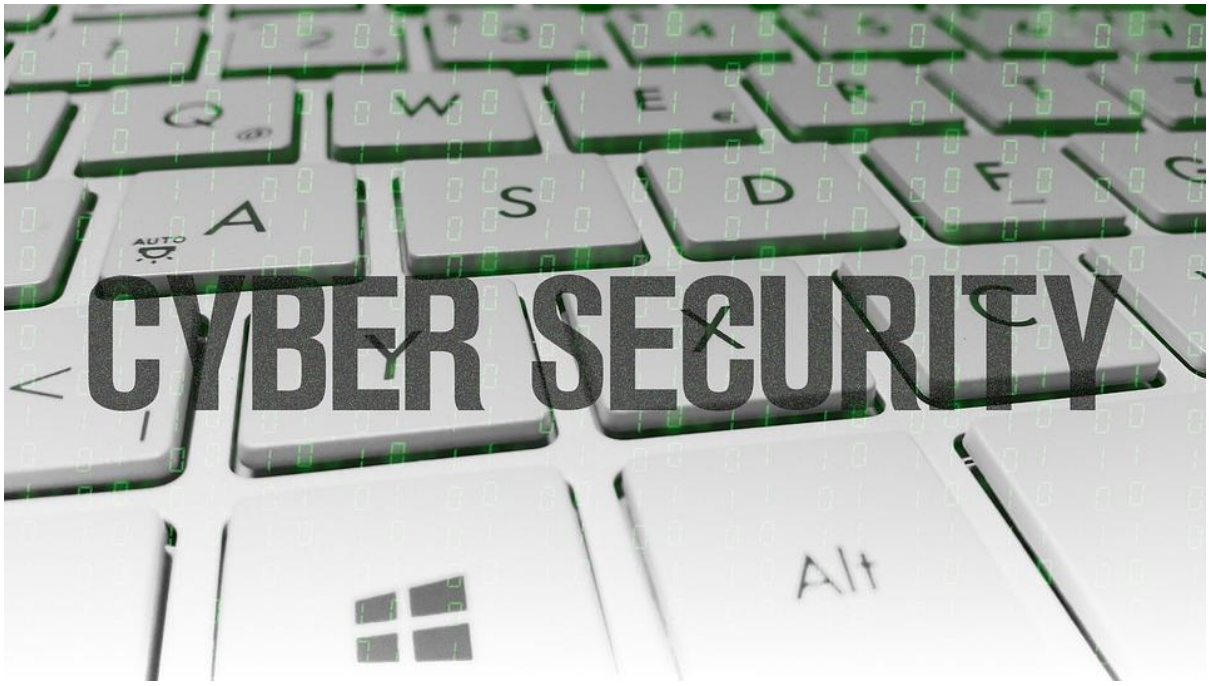
consultant régulièrement des sites Web tels que ceux mentionnés ci-dessous dans la rubrique "Autres ressources" :

Autres ressources

ENISA (europa.eu)

Risques de cybersécurité | NIST

Il est conseillé aux formateurs d'enrichir la liste des autres ressources avec du matériel dans leur propre langue et/ou du matériel pertinent pour le pays/la région. Une bonne source d'information peut également être trouvée dans les articles et publications en ligne des experts et chercheurs en cybersécurité.



1. Mesures de sûreté et de sécurité numériques

Créer des mots de passe et les rendre forts.

Un grand nombre d'utilisateurs n'utilisent pas la fonction mot de passe sur au moins un de leurs appareils connectés à Internet, le laissant ouvert à quiconque pourrait le prendre. Verrouillez tous vos appareils, y compris les ordinateurs, les tablettes et les smartphones, avec des mots de passe sécurisés. Cela empêchera les regards indiscrets d'entrer et ajoutera

une ligne de défense en cas de perte, d'égarement ou de vol de vos appareils. Un mot de passe fort comporte au moins 12 caractères. Les conseils pour un mot de passe fort comprennent l'utilisation d'un mélange de lettres minuscules et majuscules, de chiffres et de symboles, et l'évitement d'utiliser des informations personnelles facilement identifiables (nom du conjoint, nom de l'animal de compagnie, anniversaires, etc.) Un mot de passe faible serait quelque chose que n'importe qui pourrait facilement découvrir, comme le nom d'un animal de compagnie adoré "KittkyCat" ; un mot de passe fort pourrait ressembler à "1Kitty234Cat !!".

À quelle fréquence devez-vous changer les mots de passe ?

À moins que vous n'ayez connaissance d'une violation de mot de passe, il n'est pas nécessaire de changer régulièrement vos mots de passe si chacun d'eux est fort et unique. Cela est encore plus vrai si vous utilisez une authentification à deux facteurs.
Dans la mesure du possible, utilisez une forme d'authentification à deux facteurs afin qu'un mot de passe piraté ne compromette pas votre compte. La combinaison de l'authentification à deux facteurs et des mots de passe générés par une machine rend la plupart des comptes d'utilisateur pratiquement inviolables.

Qu'est-ce qu'un mot de passe unique ?

Un mot de passe unique est :

1. Jamais réutilisé. Une fois que vous utilisez un mot de passe, vous ne pouvez jamais l'utiliser pour un autre compte.
2. Suffisamment long. Un mot de passe fort comporte au moins 12 caractères. Les conseils pour un mot de passe fort incluent l'utilisation d'un mélange de lettres, de chiffres et de symboles.
3. Rien qui vous concerne. Cela signifie que vous n'utilisez pas le nom d'un enfant ou d'un animal de compagnie dans votre mot de passe, ni d'autres informations qui peuvent facilement remonter jusqu'à vous.

Étant donné que les utilisateurs utilisent aujourd'hui plusieurs applications et appareils, il peut être très tentant d'utiliser un seul mot de passe pour la majorité de vos appareils et applications. Aussi pratique soit-elle, cette pratique peut entraîner une grande vulnérabilité, car une seule attaque malveillante peut affecter la majorité de vos comptes et même compromettre les solutions de banque en ligne ou de stockage dans le cloud. Il est donc fortement conseillé d'utiliser des mots de passe uniques différents pour les différents appareils et applications et de faire preuve de prudence lorsque vous partagez ou tapez ces mots de passe sur des réseaux publics.

Comment fonctionne l'authentification à deux facteurs ?

Vous pouvez activer une authentification à deux facteurs dans les paramètres de votre compte de médias sociaux, de votre messagerie électronique ou d'autres profils. Les authentifications à deux facteurs se feront à l'aide de votre numéro de téléphone ou d'une application d'authentification sur votre smartphone. Après avoir activé l'authentification à deux facteurs, chaque fois que vous vous connecterez à votre compte à partir d'un nouvel appareil ou d'un nouveau navigateur, le code de sécurité sera envoyé à votre téléphone ou à votre application d'authentification. Vous devez saisir ce code et vous serez autorisé à vous connecter. Si un cybercriminel tente de se connecter à votre compte, il n'y parviendra pas s'il n'a pas accès à votre téléphone portable. Vous pourrez également remarquer une tentative de connexion à votre compte, car vous recevrez une notification avec un code. Ne partagez jamais ce code avec d'autres personnes ! Un attaquant essaierait de l'obtenir. Si vous avez reçu le code mais que vous n'avez pas tenté de vous connecter, supprimez le message de code et changez votre mot de passe dès que possible.

Paramètres de confidentialité dans les médias sociaux

Lorsque vous créez des messages sur les médias sociaux, vous pouvez choisir des paramètres de confidentialité. Par exemple, vous pouvez choisir le public qui verra votre message. Il peut s'agir uniquement des amis que vous avez ajoutés sur le réseau social, d'un message public pour tout le monde ou d'un message privé pour vous seul. Vous pouvez également spécifier ou non votre localisation. Assurez-vous que vos informations privées ne sont pas partagées. Par exemple, vos mots de passe, votre numéro de téléphone, votre adresse électronique, etc.

Règles de sécurité dans les médias sociaux, les messageries et les e-mails

Lorsque vous communiquez par l'intermédiaire des réseaux sociaux, des messageries et des e-mails, vous devez veiller à ne pas être victime de prétextes, de malvertising ou de différents types de phishing. Ne cliquez pas sur les liens qui vous sont envoyés par une personne inconnue. Soyez prudent : les cybercriminels peuvent se faire passer, par exemple, pour des employés de Facebook ou du service de sécurité d'Instagram. Ne faites pas confiance à ces messages, si vous les recevez par le biais d'un chat, d'un message ou d'une page Facebook ordinaire. Les messages de sécurité vous seront transmis par le biais de notifications ou seront disponibles dans les paramètres. Les employés des médias sociaux ne vous demanderont jamais votre mot de passe ou des informations privées.

Quelqu'un vous demande de l'argent ?

Si des amis ou des membres de votre famille vous demandent de les aider en cas d'urgence, appelez toujours pour leur parler personnellement afin de confirmer que le message provient bien d'eux. Sinon, ces messages peuvent provenir de cybercriminels. Ils peuvent créer un

profil identique à celui d'un membre de votre famille ou d'un ami, et tenter de vous soutirer de l'argent.

Sécurité des appareils

Utilisez un logiciel de sécurité. Installez sur vos appareils un logiciel de sécurité provenant d'une source fiable et tenez-le à jour. Il est préférable d'exécuter régulièrement le logiciel antivirus et anti-spyware. Méfiez-vous des mises à jour de sécurité provenant de publicités pop-up ou d'e-mails. Il peut s'agir de logiciels malveillants qui peuvent infecter votre ordinateur.

Utilisez la protection par défaut du pare-feu de votre ordinateur. Votre système d'exploitation (SE) possède probablement des paramètres de pare-feu par défaut qui protégeront votre ordinateur sans qu'il soit nécessaire de les ajuster. Si votre logiciel antivirus comprend une protection supplémentaire par pare-feu que vous pouvez régler séparément, envisagez de contacter un professionnel de l'informatique pour obtenir de l'aide afin de vous assurer que vous êtes bien protégé sans bloquer excessivement les sites et les programmes que vous utilisez régulièrement.

Déconnectez-vous. N'oubliez pas de vous déconnecter des applications et des sites Web lorsque vous avez fini de les utiliser. Les laisser ouverts sur votre écran d'ordinateur pourrait vous rendre vulnérable à des risques de sécurité et de confidentialité.

10 conseils pour assurer votre sécurité en ligne

1. Créez des mots de passe et faites en sorte qu'ils soient forts.

2. Sécurisez l'accès à vos comptes. Comme les mots de passe peuvent être volés, l'ajout d'une authentification en deux étapes aux comptes constitue une deuxième couche de protection. De nombreux services en ligne, y compris des apps et des sites Web, proposent des options gratuites qui pourraient vous aider à protéger vos informations et à vous assurer que c'est bien vous qui essayez d'accéder à votre compte - et pas seulement quelqu'un qui possède votre mot de passe.

3. Réfléchissez avant d'agir. Les courriels et les communications qui créent un sentiment d'urgence, comme un problème avec votre compte bancaire ou vos impôts, sont probablement une arnaque. Pensez à contacter directement l'entreprise par téléphone pour déterminer si le courriel est légitime ou non.

4. En cas de doute, jetez-le. C'est souvent en cliquant sur les liens contenus dans les courriels que les escrocs obtiennent des informations personnelles. Si un courriel vous semble inhabituel, même si vous connaissez la personne qui l'a envoyé, il est préférable de le supprimer. N'oubliez pas que les escrocs peuvent réquisitionner les adresses électroniques d'amis et vous envoyer des messages en se faisant passer pour eux. Activez les filtres anti-spam de votre compte de messagerie pour vous aider à filtrer les messages suspects.

5. Partagez avec précaution. Faites attention à ce que vous partagez publiquement sur les sites de médias sociaux comme Facebook. Réglez vos paramètres de confidentialité pour limiter les personnes qui peuvent voir vos informations. Évitez de partager votre emplacement.

6. Utilisez des logiciels de sécurité. Installez sur vos appareils des logiciels de sécurité provenant d'une source fiable et tenez-les à jour. Il est préférable d'exécuter régulièrement le logiciel antivirus et anti-spyware. Méfiez-vous des mises à jour de sécurité provenant de publicités pop-up ou d'e-mails. Il peut s'agir en fait de logiciels malveillants qui peuvent infecter votre ordinateur.

7. Réglez les paramètres de sécurité de votre navigateur. Vous recherchez probablement des actualités, des informations et des produits en utilisant un navigateur Internet tel que Firefox, Google Chrome, Internet Explorer et Safari. Réglez vos paramètres dans chacun de ces navigateurs pour définir vos options en vue d'une sécurité optimale. Ces menus se trouvent souvent dans le coin supérieur droit de votre navigateur. Pensez à effacer votre historique de navigation à la fin de votre session pour ne pas laisser de traces de données sensibles.

8. Utilisez la protection par défaut du pare-feu de votre ordinateur. Votre système d'exploitation (SE) possède probablement des paramètres de pare-feu par défaut qui protégeront votre ordinateur sans qu'il soit nécessaire de les ajuster. Si votre logiciel antivirus comprend une protection supplémentaire par pare-feu que vous pouvez régler séparément, envisagez de contacter un professionnel de l'informatique pour obtenir de l'aide afin de vous assurer que vous êtes bien protégé sans bloquer excessivement les sites et les programmes que vous utilisez régulièrement.

9. Déconnectez-vous. N'oubliez pas de vous déconnecter des applications et des sites Web lorsque vous avez fini de les utiliser. Les laisser ouverts sur votre écran d'ordinateur pourrait vous rendre vulnérable à des risques de sécurité et de confidentialité.

Envisagez une assistance. Si vous êtes préoccupé par la sécurité numérique, adressez-vous à un professionnel de confiance ou demandez de l'aide et des conseils au service informatique de votre entreprise.

AUTO-ÉVALUATION :

● Réfléchissez à vos habitudes et pratiques quotidiennes, pensez-vous que vous pourriez être vulnérable en termes de sécurité / sûreté numérique ?

● Sur les 10 conseils proposés, combien en appliquez-vous actuellement ?

● Quels sont les conseils ou les idées que vous prévoyez d'utiliser ?

● Quels sont les 3 conseils que vous donneriez aux apprenants en matière de sécurité / sûreté numérique ?