Chapitre 3 : Protection des données et confidentialité

Ce chapitre est axé sur vos périphériques personnels et sur vos données personnelles. Il comprend des conseils pour la protection de vos périphériques, pour la création de mots de passe fiables et pour l’utilisation sécurisée des réseaux sans fil. Il parle également de la sécurisation de vos données.

Vos données en ligne valent de l’argent pour les cybercriminels. Ce chapitre couvre brièvement les techniques d’authentification pour vous aider à sécuriser vos données. Il couvre également des méthodes de renforcement de la sécurité de vos données en ligne avec des conseils sur les bonnes et mauvaises pratiques en ligne.

# Protéger vos périphériques informatiques

Vos périphériques informatiques stockent vos données et représentent le portail de votre vie en ligne. Voici une liste finale des étapes à suivre pour protéger vos périphériques informatiques d’une intrusion :

* **Activez toujours le pare-feu** : que ce soit un pare-feu logiciel ou un pare-feu matériel sur un routeur, il doit être activé et mis à jour pour empêcher l’accès des pirates à vos données personnelles ou d’entreprise. Cliquez sur [Windows 7 et 8.1](http://windows.microsoft.com/en-us/windows/turn-windows-firewall-on-off) ou [Windows 10](http://windows.microsoft.com/en-us/windows-10/turn-windows-firewall-on-or-off) pour activer le pare-feu de la version respective de Windows. Cliquez [ici](https://support.apple.com/en-us/HT201642) pour activer le pare-feu pour les périphériques Mac OS X.
* **Utilisez un antivirus et un anti-logiciel espion** : les programmes malveillants, comme les virus, les chevaux de Troie, les vers, les rançongiciels et les logiciels espions s’installent sans autorisation sur vos périphériques informatiques, afin d’obtenir l’accès à votre ordinateur et à vos données. Les virus peuvent détruire vos données, ralentir votre ordinateur ou prendre son contrôle. Les virus peuvent prendre le contrôle de votre ordinateur grâce notamment à la possibilité des expéditeurs de pourriels de diffuser des e-mails à partir de votre compte. Le logiciel espion peut surveiller vos activités en ligne, collecter vos informations personnelles ou produire des publicités contextuelles indésirables sur votre navigateur Web lorsque vous êtes en ligne. La bonne règle consiste à ne télécharger que les logiciels venant de sites Web sécurisés afin d’éviter si possible l’intrusion du logiciel espion. Le logiciel antivirus est conçu pour analyser votre ordinateur et les e-mails reçus afin de détecter les virus et de les supprimer. Parfois, le logiciel antivirus inclut également un anti-logiciel espion. Maintenez votre logiciel à jour pour protéger votre ordinateur des derniers programmes malveillants.
* **Gérez votre système d’exploitation et votre navigateur Web** : les pirates s’efforcent toujours de tirer profit des vulnérabilités de vos systèmes d’exploitation et de vos navigateurs Web. Pour protéger votre ordinateur et vos données, configurez les paramètres de sécurité de votre ordinateur et de votre navigateur Web à un niveau moyen ou supérieur. Mettez à jour le système d’exploitation de votre ordinateur, notamment vos navigateurs Web et téléchargez et installez régulièrement les derniers correctifs de logiciel et les mises à jour de sécurité des fournisseurs.
* **Protégez tous vos périphériques** : vos périphériques informatiques, que ce soient des PC, des ordinateurs portables, des tablettes ou des smartphones, doivent être protégés par un mot de passe pour empêcher tout accès non autorisé. Les informations stockées doivent être chiffrées, surtout les données sensibles et confidentielles. Pour les terminaux mobiles, ne stockez que les informations nécessaires, au cas où ces périphériques seraient volés ou perdus lorsque vous sortez. Si l’un de vos périphériques est compromis, les cybercriminels peuvent avoir accès à toutes vos données par l’intermédiaire de votre fournisseur de service en nuage, comme iCloud ou Google Drive.

Les appareils connectés à l’IoT représentent un risque plus considérable par rapport aux périphériques informatiques. Si les postes de travail, les ordinateurs portables et les plate-formes mobiles reçoivent fréquemment des mises à jour logicielles, la plupart des appareils connectés à l’IoT exécutent encore leur micrologiciel d’origine. Si des vulnérabilités sont trouvées dans le micrologiciel, il est certain que le périphérique reste vulnérable. Pour empirer le problème, les appareils connectés à l’IoT sont souvent conçus pour une connexion domestique et nécessite un accès Internet. Pour accéder à Internet, la plupart des fabricants d’appareils connectés à l’IoT dépendent du réseau local du client. Résultat : les appareils connectés à l’IoT sont certains d’être compromis et dans ce cas, ils permettent l’accès au réseau local et aux données du client. La meilleure façon d’éviter ce scénario est une connexion réseau isolée des appareils connectés à l’IoT et de la partager uniquement avec d’autres appareils connectés à l’IoT.

Cliquez [ici](https://www.shodan.io/) pour visiter Shodan, un scanner d’appareils connectés à l’IoT basé sur le Web.

# Utiliser les réseaux sans fil en toute sécurité

Les réseaux sans fil permettent aux périphériques à accès Wi-Fi, comme les ordinateurs portables et les tablettes, de se connecter au réseau grâce à l’identificateur de réseau, connu sous le nom d’identificateur SSID (Secure Set Identifier). Pour empêcher l’accès des intrus à votre réseau sans fil domestique, l’identificateur SSID préfiguré et le mot de passe par défaut de l’interface administrative du navigateur Web doivent être changés. Les pirates connaissent ce type d’informations d’accès par défaut. Le routeur sans fil peut également être configuré de façon à ne pas diffuser le SSID, ce qui constitue un obstacle supplémentaire à la découverte du réseau. Toutefois, cette approche est loin d'être suffisante pour un réseau sans fil. De plus, vous devez crypter votre communication sans fil en activant la sécurité sans fil et la fonctionnalité de chiffrement WPA2 du routeur sans fil. Même avec la fonctionnalité de chiffrement WPA2, le réseau sans fil reste vulnérable.

En octobre 2017, une faille de sécurité a été détectée dans le protocole WPA2, permettant à un intrus de contourner le chiffrement entre le routeur sans fil et le client sans fil, et ainsi d'accéder au trafic réseau et de le manipuler. Cette vulnérabilité peut être exploitée par la méthode KRACK (**K**ey **R**einstallation **A**tta**ck**s). Elle affecte tous les réseaux Wi-Fi modernes protégés. Pour bloquer le hacker, l'utilisateur doit mettre à jour tous les produits impactés : les routeurs sans fil et tous les appareils sans fil, tels que les ordinateurs portables et les terminaux mobiles, dès la publication des mises à jour de sécurité. Pour corriger cette vulnérabilité, il suffit de brancher votre ordinateur portable ou tout autre appareil équipé d'une carte réseau filaire. En outre, vous pouvez également utiliser un service VPN fiable pour empêcher tout accès non autorisé à vos données lorsque vous utilisez le réseau sans fil.

Cliquez [ici](https://www.krackattacks.com/) pour en savoir plus sur la méthode KRACK.

Lorsque vous sortez, une zone d’accès Wi-Fi public vous permet d’accéder à vos informations en ligne et de naviguer sur Internet. Cependant, il est recommandé de ne pas accéder ou envoyer d’informations personnelles sensibles sur un réseau sans fil public. Vérifiez si votre ordinateur est configuré pour le partage de fichiers et de médias et s’il nécessite une authentification des utilisateurs avec un chiffrement. Pour empêcher l’interception de vos informations par un tiers (ou « écoute illicite ») en cas d’utilisation d’un réseau sans fil public, utilisez des tunnels et services VPN chiffrés. Le service VPN vous fournit un accès à Internet sécurisé, avec une connexion chiffrée entre votre ordinateur et le serveur VPN du fournisseur de service VPN. Grâce au tunnel VPN chiffré, même si la transmission des données est interceptée, elle est non déchiffrable.

Cliquez [ici](https://www.fcc.gov/consumers/guides/protecting-your-wireless-network) pour en savoir plus sur les mesures de protection lors de l’utilisation des réseaux sans fil.

De nombreux terminaux mobiles, comme les smartphones et les tablettes, intègrent le protocole sans fil Bluetooth. Cette fonctionnalité permet aux périphériques à accès Bluetooth de se connecter à un autre périphérique et de partager des informations. Malheureusement, la technologie Bluetooth peut être exploitée par les pirates pour une écoute illicite de certains périphériques, pour configurer des contrôles d’accès à distance, pour distribuer des programmes malveillants et pour décharger les batteries. Pour éviter ces problèmes, désactivez le Bluetooth lorsque vous ne l’utilisez pas.

Utiliser des mots de passe uniques pour chaque compte en ligne

Vous avez probablement plusieurs comptes en ligne, et chacun doit avoir un mot de passe unique. Il y en a beaucoup à se rappeler. Cependant, si vous n'utilisez pas de mots de passe fiables et uniques, vous et vos données serez vulnérables face aux cybercriminels. Utiliser le même mot de passe pour tous vos comptes en ligne revient à utiliser la même clé pour toutes vos portes ; si un hacker parvient à découvrir votre mot de passe, il aura accès à tout ce que vous possédez. Si les cybercriminels ont eu votre mot de passe par hameçonnage par exemple, ils essaieront d’accéder à vos autres comptes en ligne. Si vous n’utilisez qu’un seul mot de passe pour tous les comptes, ils accéderont à ces derniers, voleront ou supprimeront toutes vos données, ou décideront d’emprunter votre identité.

Nous avons tous de nombreux comptes en ligne qui nécessitent des mots de passe ; il y en a trop à mémoriser. La solution pour éviter de réutiliser les mots de passe ou d’utiliser des mots de passe trop simples consiste à utiliser un gestionnaire de mots de passe. Un gestionnaire de mots de passe stocke et chiffre tous les mots de passe uniques et complexes. Le gestionnaire peut vous permettre de vous connecter automatiquement à vos comptes en ligne. Vous devez seulement vous rappeler de votre mot de passe principal pour accéder au gestionnaire de mots de passe et pour gérer tous vos comptes et vos mots de passe.

**Conseils pour choisir un bon mot de passe**:

* N’utilisez pas des mots et des noms du dictionnaire, peu importe la langue.
* N’utilisez pas les fautes d’orthographe des mots du dictionnaire.
* N’utilisez pas des noms d’ordinateur ou des noms de compte.
* Si possible, utilisez des caractères spéciaux, comme ! @ # $ % ^ & \* ( )
* Votre mot de passe doit comporter au moins 10 caractères

Utiliser une phrase secrète et non un mot de passe

Pour empêcher un accès physique non autorisé à vos périphériques informatiques, utilisez des phrases secrètes et non des mots de passe. Il est plus simple de créer une longue phrase secrète plutôt qu'un mot de passe, puisqu'elle est généralement constituée d'une phrase et non d'un mot. Les phrases secrètes plus longues sont moins vulnérables aux attaques de force brute ou de dictionnaire. Elles peuvent aussi être plus simples à mémoriser, surtout s'il vous est fréquemment demandé de modifier votre mot de passe. Voici quelques conseils pour choisir de bons mots de passe et de bonnes phrases secrètes :

**Conseils pour choisir une bonne phrase de passe :**

* Choisissez une phrase significative
* Ajoutez des caractères spéciaux, comme ! @ # $ % ^ & \* ( )
* Plus c’est long, mieux c’est.
* Évitez les phrases courantes ou célèbres, par exemple, des textes d’une chanson populaire.

Le NIST (National Institute for Standards and Technology), une agence gouvernementale américaine, a publié récemment ses nouvelles exigences relatives aux mots de passe. Les standards NIST sont destinés aux administrations, mais ils peuvent aussi s'appliquer à d'autres domaines. Ces nouvelles instructions visent à améliorer l'expérience des utilisateurs et à transmettre la responsabilité de la vérification de l'identité des utilisateurs aux fournisseurs d'accès.

**Résumé des nouvelles instructions :**

* Composé de 8 à 64 caractères
* Ne pas choisir un mot de passe courant ou facile à deviner comme abc123
* Aucune règle de sécurité comme utiliser une combinaison de lettres majuscules, de lettres minuscules et de chiffres
* Améliorer la précision de la saisie en affichant le mot de passe au moment de la saisie
* Tous les caractères d'impression et les espaces sont autorisés
* Pas d'indice
* Aucun délai d'expiration du mot de passe (périodique ou arbitraire)
* Aucun processus d'authentification basée sur une question (question secrète, question sur des données marketing, question sur l'historique des transactions)

Cliquez [ici](https://pages.nist.gov/800-63-3/) pour en savoir plus sur les nouvelles exigences du NIST sur les mots de passe.

Même si l’accès à vos ordinateurs et à vos périphériques réseau sont sécurisés, il est également important de protéger et de sécuriser vos données.

# Chiffrer vos données

Vos données doivent toujours être chiffrées. Vous pensez ne pas avoir de secrets, ni de choses à cacher, alors pourquoi utiliser le chiffrement, dites-vous ? Peut-être pensez-vous que vos données ne sont importantes pour personne. Vous vous trompez certainement.

Êtes-vous prêt à montrer toutes vos photos et tous vos documents à des étrangers ? Êtes-vous prêt à partager avec vos amis les informations financières stockées sur votre ordinateur ? Souhaitez-vous fournir les mots de passe de votre e-mail et de vos comptes au public ?

Cela peut empirer si l’application malveillante infecte votre ordinateur ou votre terminal mobile et vole des informations potentiellement utiles, comme les numéros de compte, les mots de passe et d’autres documents officiels. Ce type d’informations peut mener à l’usurpation d’identité, à la fraude ou à une demande de rançon. Les cybercriminels peuvent décider de simplement chiffrer vos données pour les rendre inutilisables jusqu’à ce que vous payez la rançon.

Qu’est-ce que le chiffrement ? Le chiffrement est un processus de conversion des informations en un format non accessible en lecture pour une partie non autorisée. Seule une personne fiable et autorisée, dotée du code secret ou du mot de passe peut déchiffrer les données et accéder à leur format original. Le chiffrement proprement dit n’empêche pas l’interception des données par un tiers. Le chiffrement ne peut qu’empêcher une personne non autorisée à visionner ou à accéder au contenu.

Des programmes sont utilisés pour chiffrer des fichiers, des dossiers et même des disques entiers.

Le système EFS (Encrypting File System) de Windows permet de chiffrer les données. Cette fonction est directement liée à un compte d'utilisateur. Seul l'utilisateur ayant chiffré les données pourra à nouveau y accéder. Pour chiffrer des données à l'aide du système EFS dans toutes les versions de Windows, procédez comme suit :

**Étape 1.** Sélectionnez un ou plusieurs fichiers ou dossiers.

**Étape 2**. Cliquez avec le bouton droit sur **>Propriétés** des données sélectionnées.

**Étape 3**. Cliquez sur **Avancé**.

**Étape 4**. Cochez la case **Chiffrer le contenu pour sécuriser les données**.

**Étape 5**. Les fichiers et dossiers ayant été chiffrés avec le système EFS sont affichés en vert (voir ci-contre).

# Sauvegarder vos données

Votre disque dur peut tomber en panne. Votre ordinateur portable peut être perdu. Votre smartphone peut être volé. Vous avez peut-être supprimé la version originale d’un document important. Avoir une sauvegarde permet d’empêcher la perte de données irremplaçables, comme les photos de famille. Pour bien sauvegarder les données, vous aurez besoin d’une mémoire supplémentaire pour vos données, dans laquelle vous devez les copier régulièrement et automatiquement.

La mémoire supplémentaire pour vos fichiers sauvegardés peut être votre réseau domestique, une mémoire secondaire ou le cloud. Grâce au stockage local de la sauvegarde des données, vous avez le contrôle total de ces dernières. Vous pouvez décider de copier vos données dans un périphérique de stockage (stockage en réseau NAS), dans un simple disque dur externe ou vous pouvez également ne sélectionner que quelques dossiers importants pour les sauvegarder sur des clés USB, sur des CD/DVD ou même sur des bandes. Dans ce cas, vous en êtes le propriétaire et vous êtes totalement responsable du coût et de la maintenance du périphérique de stockage. Si vous souscrivez à un service de stockage du cloud, le coût dépend du total d’espace de stockage nécessaire. Grâce à un service de stockage du cloud comme Amazon Web Services (AWS), vous avez accès à vos données de sauvegarde, tant que vous avez accès à votre compte. Lorsque vous souscrivez à des services de stockage en ligne, vous devez être plus sélectif concernant les données à sauvegarder, en raison du coût de stockage et des transferts continus de données en ligne. L’un des avantages du stockage de la sauvegarde sur un autre site est que cela offre une sécurité en cas d’incendie, de vol ou de catastrophes autres que la panne du périphérique de stockage.

# Supprimer définitivement vos données

Lorsque vous déplacez un fichier dans la corbeille et le supprimez définitivement, le fichier n'est accessible qu'à partir du système d'exploitation. Toute personne possédant les bons outils de recherche peut encore récupérer le fichier en raison de l'empreinte magnétique sur le disque dur.

Afin de supprimer les données pour qu’elles ne soient plus récupérables, ces dernières doivent être remplacées par une suite de uns (1) et de zéros (0). Pour empêcher la récupération des fichiers supprimés, vous devez utiliser des outils spécialement conçus à cette fin. Le programme SDelete de Microsoft (pour Vista et les versions ultérieures) est réputé avoir la capacité de définitivement supprimer les fichiers sensibles. Les programmes Shred (pour Linux) et Secure Empty Trash (pour Mac OSX) sont quelques-uns des outils qui sont réputés fournir le même service.

La seule manière de certifier que les données ou les fichiers ne sont pas récupérables consiste à détruire physiquement le disque dur ou le périphérique de stockage. Penser que leurs fichiers étaient inaccessibles et irrécupérables a été la perte de plusieurs cybercriminels.

Outre le fait de stocker les données sur vos disques durs locaux, vos données peuvent également être stockées en ligne. Ces copies devront également être supprimées. Prenez un moment pour considérer l’emplacement où vous enregistrez vos données. Où vos données sont-elles sauvegardées ? Sont-elles chiffrées ? Lorsque vous devez supprimer vos données ou vous débarrasser d’un disque dur ou d’un ordinateur, demandez-vous si vous avez protégé les données pour que des personnes malveillantes n’y aient pas accès.

# Authentification à deux facteurs

Les services en ligne populaires, comme Google, Facebook, Twitter, LinkedIn, Apple et Microsoft, utilisent une authentification à deux facteurs pour renforcer la sécurité des connexions aux comptes. Outre le nom d’utilisateur et le mot de passe, ou le modèle ou le numéro d’identification personnelle (PIN), l’authentification à deux facteurs nécessite un second jeton, comme :

* **Un objet physique** (une carte de crédit, une carte ATM, un téléphone ou un porte-clé) ;
* **Un balayage biométrique** (une empreinte digitale ou palmaire et une reconnaissance vocale ou faciale).

Même avec une authentification à deux facteurs, les pirates peuvent toujours obtenir l’accès à vos comptes en ligne, notamment par le biais d’attaques d’hameçonnage, de programmes malveillants et de piratage psychologique.

Allez [ici](https://twofactorauth.org/) pour découvrir si les sites Web que vous visitez utilisent une authentification à deux facteurs.

# OAuth 2.0

OAuth (Open Authorization) est un protocole ouvert normalisé qui permet à l’utilisateur final identifié d’accéder à des applications tierces sans exposer le mot de passe utilisateur. OAuth sert d’intermédiaire dans l’autorisation d’accès des utilisateurs finaux à des applications tierces. Supposons par exemple que vous souhaitiez accéder à une application XYZ et que vous n’avez pas de compte utilisateur pour accéder à cette application Web. Cependant, XYZ fournit une option qui vous permet de vous connecter grâce à des informations d’identification d’un site Web de réseaux sociaux ABC. Vous accédez donc au site Web grâce à la connexion pour les réseaux sociaux.

Pour que cela fonctionne, l’application « XYZ » doit être enregistrée dans « ABC » et être une application approuvée. Lorsque vous accédez à XYZ, vous utilisez vos informations d’identification pour ABC. XYZ nécessite ensuite un jeton d’accès d’ABC en votre nom. Vous avez maintenant accès à XYZ. XYZ ne possède aucune information d’identification de l’utilisateur et l’interaction est totalement fluide pour ce dernier. Utiliser des jetons secrets empêche une application malveillante d’accéder à vos informations et à vos données.

# Ne partagez pas trop d’informations sur les réseaux sociaux

Si vous souhaitez maintenir votre confidentialité sur les réseaux sociaux, partagez le moins d’informations possible. Vous ne devez pas partager d’informations comme votre date de naissance, adresse e-mail ou votre numéro de téléphone sur votre profil. Les personnes qui doivent connaître vos informations personnelles les connaissent probablement déjà. Ne remplissez pas entièrement votre profil de réseaux sociaux, ne fournissez que le minimum d’informations nécessaire. De plus, vérifiez vos paramètres de réseaux sociaux pour permettre uniquement à vos connaissances de voir vos activités ou d’interagir dans vos discussions.

Plus vous partagez d’informations personnelles en ligne, plus il est facile pour une personne de créer un profil en votre nom pour en tirer profit hors connexion.

Avez-vous oublié le nom d’utilisateur et le mot de passe d’un compte en ligne ? Les questions de sécurité comme « quel est le nom de jeune fille de votre mère ? » ou « dans quelle ville êtes-vous né ? » sont supposées sécuriser votre compte contre l’accès d’intrus. Cependant, toute personne souhaitant accéder à vos comptes peut rechercher les réponses sur Internet. Vous pouvez répondre de façon erronée à ces questions, tant que vous pouvez vous rappeler des réponses incorrectes. Si vous avez des difficultés à vous les rappeler, vous pouvez utiliser un gestionnaire de mots de passe pour les gérer à votre place.

# Confidentialité des e-mails et sur navigateur Web

Chaque jour, des millions de messages électroniques sont utilisés pour communiquer entre amis ou pour le travail. L’e-mail est un outil pratique pour communiquer rapidement. Envoyer un e-mail revient à envoyer un message grâce à une carte postale. Le message par carte postale est transmis au vu et au su de toute personne y ayant accès, tout comme le message électronique qui est transmis en texte brut. Ces communications sont également transférées sur plusieurs serveurs lors de l’acheminement vers la destination. Même si vous supprimez vos messages électroniques, ils peuvent être archivés sur les serveurs de messagerie pour une durée déterminée.

Toute personne ayant accès à votre ordinateur ou à votre routeur peut voir les sites Web que vous avez visité grâce à l’historique de navigation Web, au cache et éventuellement aux fichiers journaux. Ce problème peut être minimisé en activant le mode de navigation privée sur le navigateur Web. La plupart des navigateurs Web populaires ont leur propre dénomination du mode de navigation privée :

* **Microsoft Internet Explorer** : InPrivate
* **Google Chrome** : navigation privée
* **Mozilla Firefox** : onglet privé / fenêtre privée
* **Safari** : privé (navigation privée)

Grâce à l’activation du mode de navigation privée, les cookies sont désactivés et les fichiers Internet temporaires et l’historique de navigation sont supprimés à la fermeture de la fenêtre ou du programme.

Activer le mode privé pour l’historique de votre navigation Internet peut empêcher des tiers de collecter des informations sur votre activité en ligne pour vous inciter à acheter des choses par le biais de publicités ciblées. Même si la navigation privée est activée et les cookies désactivés, les entreprises développent différentes méthodes pour retracer les utilisateurs afin de collecter des informations et de faire un suivi du comportement de l’utilisateur. Par exemple, les périphériques intermédiaires, comme les routeurs, peuvent contenir des informations sur l’historique de navigation Web d’un utilisateur.

Au final, il est de votre responsabilité de protéger vos données, votre identité et vos périphériques informatiques. Lorsque vous envoyez un e-mail, devez-vous inclure vos dossiers médicaux ? La dernière fois que vous avez navigué sur Internet, votre transmission était-elle sécurisée ? Il suffit de quelques précautions simples pour vous éviter des problèmes dans le futur.

# Conclusion

Ce chapitre a été axé sur vos périphériques personnels et sur vos données personnelles. Il donnait des conseils pour protéger vos périphériques, pour créer des mots de passe fiables et pour utiliser les réseaux sans fil en toute sécurité. Il a abordé les sauvegardes de données, le stockage de données et la suppression définitive de vos données.

Les techniques d’authentification abordées dans ce chapitre visent à vous permettre de sécuriser vos données. La facilité du partage excessif d'informations sur les réseaux sociaux et les mesures à prendre pour éviter les risques de sécurité ont été brièvement abordées.

Si vous souhaitez découvrir plus en détail les concepts de ce chapitre, référez-vous à la page des [ressources et activités supplémentaires](https://contenthub.netacad.com/legacy/I2CS/2.1/fr/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) dans les Ressources des étudiants.