Atelier – Découvrez votre propre comportement à risque en ligne

Objectifs

Explorez les actions effectuées en ligne qui peuvent compromettre votre sécurité ou votre vie privée.

Contexte/scénario

Internet est un environnement hostile et vous devez être vigilant pour vous assurer que vos données ne sont pas compromises. Les pirates sont créatifs et tenteront de nombreuses techniques différentes pour tromper les utilisateurs. Cet atelier vous aide à identifier un comportement à risque et fournit des conseils pour être plus en sécurité en ligne.

Partie 1 : Découvrir la politique des conditions de service

Répondez aux questions suivantes avec honnêteté et notez les points obtenus pour chaque réponse. Additionnez tous les points pour obtenir un score total et passez à la partie 2 pour une analyse de votre comportement en ligne.

a. Quel type d'informations partagez-vous avec les sites de réseaux sociaux ?

1) Tout ; j'ai recours aux réseaux sociaux pour rester en contact avec les amis et la famille. (3 points)
2) Les articles et les actualités que je trouve ou que je lis (2 points)
3) Ça dépend ; je filtre ce que je partage et avec qui je le partage. (1 point)
4) Rien ; je n'utilise pas les réseaux sociaux. (0 point)

b. Lorsque vous créez un nouveau compte dans un service en ligne, vous :

1) réutilisez le même mot de passe utilisé sur d'autres services pour le retenir plus facilement ; (3 points)
2) créez un mot de passe aussi facile que possible pour que vous puissiez vous en rappeler ; (3 points)
3) créez un mot de passe très complexe et vous le stockez dans un service de gestion de mot de passe ; (1 point)
4) créez un nouveau mot de passe similaire et non différent au mot de passe utilisé dans un autre service ; (1 point)
5) créez un tout nouveau mot de passe fiable. (0 point)

c. Lorsque vous recevez un courriel intégrant des liens vers d'autres sites :

1) vous ne cliquez pas sur le lien, puisque vous ne suivez jamais les liens envoyés par courriel ; (0 point)
2) vous cliquez sur les liens, puisque le serveur de messagerie a déjà analysé le courriel ; (3 points)
3) vous cliquez sur tous les liens si le courriel provient d'une personne que vous connaissez ; (2 points)
4) vous pointez votre souris sur les liens pour vérifier l'URL de destination avant de cliquer dessus. (1 point)

d. Une fenêtre contextuelle s'affiche lorsque vous visitez un site Web. Le message dit que votre ordinateur est vulnérable et que vous devez télécharger et installer un programme de diagnostic pour le sécuriser :

1) vous cliquez dessus, téléchargez et installez le programme pour sécuriser votre ordinateur ; (3 points)
2) vous inspectez les fenêtres contextuelles et pointez votre souris sur le lien pour vérifier sa validité ; (3 points)
3) vous ignorez le message, en veillant à ne pas cliquer dessus ou à télécharger le programme et vous fermez le site Web. (0 point)

e. Lorsque vous devez vous connecter au site Web de votre institution financière pour effectuer une tâche, vous :

   1) saisissez directement vos identifiants ; (3 points)

   2) vous vérifiez l'URL pour vous assurer que c'est bien votre institution avant d'entrer les renseignements ; (0 point)

   3) vous n'utilisez pas les services bancaires en ligne ou tout autre service financier en ligne ; (0 point)

f. vous avez lu des renseignements sur un programme et décidez de faire un essai. Vous faites des recherches sur Internet et découvrez la version d'essai d'un site inconnu, vous :

   1) téléchargez et installez rapidement le programme ; (3 points)

   2) recherchez des informations complémentaires sur le développeur du programme avant de le télécharger ; (1 point)

   3) ne téléchargez pas ou n'installez pas le programme. (0 point)

g. Vous trouvez un lecteur USB en allant au travail, vous :

   1) le prenez et le branchez sur votre ordinateur pour voir son contenu ; (3 points)

   2) le prenez et le branchez sur votre ordinateur pour le formater avant de le réutiliser ; (3 points)

   3) le prenez et le branchez sur votre ordinateur pour effectuer une analyse antivirus avant de le réutiliser pour vos fichiers (3 points)

   4) ne le prenez pas. (0 point)

h. Vous devez vous connecter à Internet et vous détectez une zone d'accès Wi-Fi libre. Vous :

   1) vous connectez au réseau et utilisez Internet ; (3 points)

   2) ne vous connectez pas au réseau et patientez jusqu'à ce que vous ayez accès à une connexion sécurisée ; (0 point)

   3) vous connectez au réseau et configurez un RPV vers un serveur sécurisé avant de transmettre des renseignements. (0 point)

Partie 2 : Analyser votre comportement en ligne

Le degré de sécurité de vos comportements en ligne diminue à mesure que votre score est élevé. L'objectif est un degré de sécurité de 100 % grâce à la considération de vos interactions en ligne. C'est très important étant donné qu'il ne suffit que d'une erreur pour compromettre votre ordinateur et vos données.

Additionnez les scores obtenus dans la partie 1. Enregistrez votre score.

0 : votre comportement en ligne est très sécurisé.

0 – 3 : votre comportement en ligne est légèrement sécurisé, mais vous devriez l'améliorer pour une sécurisation optimale.

3 – 17 : votre comportement en ligne est risqué et vous êtes très vulnérable à une compromission.

18 ou plus : votre comportement en ligne est très risqué et vous serez compromis.

Voici quelques conseils de sécurité en ligne essentiels.

a. Plus vous communiquez des renseignements sur les réseaux sociaux, plus vous donnez une occasion aux cybercriminels de vous connaître. Grâce à plus de connaissances, un cybercriminel peut mettre en œuvre une attaque plus ciblée. Par exemple, en communiquant aux autres que vous avez assisté à une course automobile, un cybercriminel peut mettre en œuvre un courriel malveillant venant d'une entreprise de billetterie responsable de l'événement de course. Puisque vous venez d'assister à l'événement, le courriel semble plus crédible.

b. Réutiliser les mots de passe est une mauvaise pratique. Si vous réutilisez un mot de passe dans un service sous le contrôle des pirates, ils peuvent réussir à se connecter en votre nom dans d'autres services.

c. Les courriers électroniques peuvent être aisément falsifiés pour paraître légitimes. Les courriers électroniques contiennent souvent des liens vers des sites ou malware. En règle générale, ne cliquez pas sur les liens intégrés reçus par courriel.

d. N'acceptez pas de logiciel non demandé, surtout venant d'une page Web. Il est invraisemblable que la page Web dispose d'une mise à jour logicielle légitime à vous proposer. Il est hautement recommandé de fermer le navigateur Web et d'utiliser les outils de système d'exploitation pour rechercher des mises à jour.

e. Les pages Web malveillantes peuvent facilement falsifier les sites Web d'une banque ou d'une institution financière. Avant de cliquer sur les liens ou de fournir des renseignements, revérifiez l'URL pour garantir que la page Web est authentique.

f. Lorsque vous exécutez un programme sur votre ordinateur, vous lui fournissez un contrôle considérable. Réfléchissez bien avant de permettre l'exécution d'un programme. Effectuez une recherche pour vérifier que la garantie et la légitimité de l'entreprise ou de l'individu auteur du programme. De même, ne téléchargez que les programmes venant des sites Web officiels de l'entreprise ou de l'individu.

g. Les clés USB comprennent un petit contrôleur qui permet une communication aux ordinateurs. Il est possible d'infecter ce contrôleur et de le commander pour installer un logiciel malveillant sur l'ordinateur hôte. Étant donné que le malware est hébergé directement sur le contrôleur USB, et non dans la zone des données, aucune opération de formatage ou d'analyse d'antivirus ne détectera le malware.

h. Les pirates déploieront souvent des zones d'accès Wi-Fi factices pour tromper les utilisateurs. Étant donné que le cybercriminel a accès à tous les renseignements échangés par l'entremise de la zone d'accès compromise, les utilisateurs connectés à cette zone d'accès sont vulnérables. N'utilisez jamais de zones d'accès Wi-Fi inconnus sans un cryptage de votre trafic par l'entremise d'un RPV. Ne communiquez aucune donnée sensible, comme les numéros de carte de crédit, lors de l'utilisation d'un réseau inconnu (filaire ou sans fil).

Remarques générales

Après l'analyse de votre comportement en ligne, quels changements souhaitez-vous faire pour votre protection en ligne ?