Club informatique Mont-Bruno

Présentations du 16 novembre 2018 et du 13 mars 2019
Présentateur : Michel Gagné

Contenu de la présentation

- Définition et exemples de transactions électroniques
- Historique de l'évolution des transactions commerciales
- Démonstration de connexion à un site sensible
- Les règles de sécurité pour les transactions électroniques

Définition et exemples de transactions électroniques

Définition : une transaction électronique est un échange (ou une portion d'un échange) impliquant l'utilisation d'un ordinateur et d'un lien de télécommunications.

Exemples de transactions électroniques

- Utilisation de cartes de crédit (comme Visa ou MasterCard)
- Utilisation de cartes de débit (comme AccèsD)
- Réception de relevés de compte par courrier électronique
- Paiements préautorisés pour des factures récurrentes

Historique de l'évolution des transactions commerciales

1. Le troc
2. L'utilisation d'objets petits et précieux (exemples : coquillages, sel)
3. L'utilisation de pièces de métal précieux
4. L'utilisation de papier-monnaie.
5. L'utilisation de chèques
6. L'utilisation de cartes de crédit
7. L'utilisation de transactions électroniques
8. L'utilisation de porte-monnaie électronique
9. …
10. La disparition du papier-monnaie, des chèques et des succursales bancaires

Démonstration de connexion à un site sensible

Exercice 1 : comment accéder, de façon sécuritaire, à un compte sur AccèsD.

1. Accédez au site AccèsD avec les actions suivantes :
   1.1. cliquez sur la barre d'adresses (c'est la barre à droite de ← → ↻ ⌂);
   1.2. écrivez **desjardins.com**
   1.3. frappez sur la touche **Entrée**;

1.4. vérifiez que vous êtes bien sur le site de Desjardins en vous assurant que **desjardins.com** apparaît à gauche de la première barre oblique simple;
1.5. en haut à droite de la page, cliquez sur le bouton **Se connecter**;
1.6. dans le menu qui est apparu, dans la section **AccèsD**, cliquez sur le bouton **Entrer**.

2. Accédez à votre compte avec les actions suivantes :
2.1. à droite d'**Identifiant**, écrivez les 12 derniers chiffres de votre numéro de carte;
2.2. ne cliquez pas sur **Mémoriser**;
2.3. cliquez sur le bouton **Entrer**;
2.4. si une fenêtre affichant **Valider l'identité** apparaît, faites comme suit
2.4.1. répondez à la question de vérification de votre identité,
2.4.2. cliquez sur le bouton **Valider**;
2.5. sur la page affichant **S'authentifier**, faites comme suit
2.5.1. lisez la phrase secrète et regardez l'image secrète,
2.5.2. si la phrase ou l'image ne sont pas celles que vous avez préalablement enregistrées, n'allez pas plus loin, car vous êtes sur un site pirate; au besoin, demandez de l'aide (vous pouvez rejoindre un conseiller AccèsD au 514-224-7737),
2.5.3. deuxième vérification : vérifiez que vous êtes bien sur le site de Desjardins en vous assurant que **desjardins.com** apparaît à gauche de la première barre oblique simple; si vous ne voyez pas **desjardins.com**, n'allez pas plus loin sur ce site, car vous êtes sur un site pirate; au besoin, demandez de l'aide (vous pouvez rejoindre un conseiller AccèsD au 514-224-7737),
2.5.4. si les deux vérifications précédentes n'ont révélé aucune anomalie, faites comme suit
2.5.4.1. cliquez dans le rectangle à droite de **Mot de passe**,
2.5.4.2. écrivez votre mot de passe,
2.5.4.3. cliquez sur le bouton **Valider**.

Exercice 2 : comment quitter le site d'AccèsD en toute sécurité.

1. En haut à droite de la page, cliquez sur le bouton **Se déconnecter**.

Les règles de sécurité pour les transactions électroniques

1. Faites du commerce uniquement avec des compagnies de confiance :
1.1. des compagnies que vous connaissez et qui ont bonne réputation (Bell, Microsoft, Amazon, Canadian Tire, Archambault, Renaud-Bray, etc.);
1.2. des compagnies qui vous ont été recommandées par des personnes bien informées (les instructeurs du club informatique sont probablement des personnes bien informées; votre voisin ou votre beau-frère ne sont peut-être pas des personnes bien informées en ce qui a trait au commerce électronique);
1.3. ne faites pas affaire avec une personne ou une entreprise qui vous offre ses services sur votre navigateur Web, sur Skype, par téléphone ou par la poste, même si la personne prétend qu'elle est un employé d'une compagnie en laquelle vous avez confiance.

2. **Assurez-vous que vous êtes vraiment sur le site de la compagnie visée :**
   - 2.1. **entrez vous-même l'adresse du site sur la barre d'adresse;**
   - 2.2. **n'accédez pas à un site à partir d'un favori; si vous le faites, vérifiez minutieusement l'adresse apparaissant sur la barre d'adresse;**
   - 2.3. **n'accédez pas à un site à partir d'une recherche Google; si vous le faites, vérifiez minutieusement l'adresse apparaissant sur la barre d'adresse;**
   - 2.4. **n'accédez pas à un site à partir d'un lien affiché sur un autre site;**
   - 2.5. **n'accédez jamais à un site à partir d'un lien affiché dans un message électronique, incluant un message venant d'une personne que vous connaissez ou du site auquel vous voulez accéder;**
   - 2.6. **lorsque vous accédez à un site sur lequel vous avez enregistré un code d'identification (par exemple, l'image secrète et la phrase secrète sur le site AccèsD), assurez-vous que le site affiche le code d'identification;**
   - 2.7. **avant d'entrer votre mot de passe, vérifiez le nom du domaine du site (ce sont les deux mots à gauche de la première barre oblique simple).**

3. **Transmettez des informations confidentielles (numéro de carte de crédit, NIP, mot de passe, etc.) seulement sur des liens sécurisés :**
   - 3.1. **l'adresse de la barre d'adresse commence alors par https;**
   - 3.2. **un petit cadenas apparaît sur la barre d'adresse;**
   - 3.3. **ne transmettez jamais un numéro de carte de crédit par courrier électronique même si l'adresse du service de courrier contient https.**

4. **Faites du commerce électronique uniquement à partir d'un ordinateur propre, c'est-à-dire un ordinateur que vous contrôlez, qui est muni de logiciels supportés, non piratés et à jour et qui est muni d'un antivirus à jour. Cela vous assure qu'il n'y a pas d'enregistreurs de frappes (*key loggers*) ou d'espions sur l'ordinateur. Ne faites pas de transactions électroniques à partir de l'ordinateur d'un ami ou d'un ordinateur public dans une bibliothèque, un café Internet, un hôtel ou un autre établissement.**

5. L'exécution des transactions électroniques exige toute votre attention. On ne fait pas de transactions électroniques après un souper bien arrosé!

6. Si, en situation d'urgence, vous utilisez un ordinateur autre que le vôtre pour faire du commerce électronique, suivez les règles suivantes :
   - 6.1. écrivez des caractères aléatoires dans d'autres champs lorsque vous écrivez des informations confidentielles, cela mettra probablement en échec les enregistreurs de frappes et les espions qui pourraient se trouver dans l'ordinateur;
   - 6.2. assurez-vous que personne ne peut voir ce que vous écrivez au clavier.

7. Lorsqu'un site de commerce électronique vous offre une façon de terminer votre session, utilisez toujours cette façon plutôt que de terminer la session en téléchargeant une autre page ou en fermant le navigateur.

8. Si quelque chose vous semble trop beau pour être vrai, arrêtez!
   Quand c'est trop beau pour être vrai, ce n'est pas vrai!!!!!

9. Comparez vos relevés de comptes bancaires et de cartes de crédit avec vos factures mensuellement.

10. Gérez vos mots de passe de façon responsable :
    - 10.1. choisissez des mots de passe qui ne sont pas faciles à deviner;
    - 10.2. utilisez des mots de passe différents pour le courrier électronique, le traitement des informations financières et le traitement des informations non financières;
    - 10.3. utilisez des mots de passe différents pour votre carte de crédit et votre carte de guichet;
    - 10.4. portez un soin particulier à protéger vos mots de passe reliés à des informations financières :
        - 10.4.1. ne donnez ces mots de passe à personne,
        - 10.4.2. ne conservez pas ces mots de passe dans votre portefeuille ou sur vous,
        - 10.4.3. n'écrivez pas ces mots de passe et surtout ne les conservez pas près de votre ordinateur;
    - 10.5. n'enregistrez pas vos mots de passe dans un fichier de votre ordinateur;
    - 10.6. ne vous envoyez pas vos mots de passe par courrier électronique dans le but de les avoir toujours sous la main;
    - 10.7. il est recommandé de changer ses mots de passe reliés à des activités financières chaque mois, mais cela peut entraîner des problèmes de mémorisation des mots de passe; pour réduire le problème de mémorisation, vous pouvez utiliser un code dans le mot de passe, par exemple, dans le mot de passe 86215, les troisième et quatrième chiffres peuvent être 20 + le rang du mois (21 pour janvier, 22 pour février, etc.).

    (Si malgré les mises en garde précédentes, vous écrivez vos mots de passe, utilisez un code pour les rendre difficiles à interpréter; par exemple, remplacez les 1 par des 7 et les 7 par des 1 ou encore inversez les trois derniers caractères.)

11. Enregistrez l'adresse de signalement d’hameçonnage de votre institution financière dans vos contacts (pour Desjardins, protection@desjardins.com) dès aujourd'hui et signalez à votre institution financière tous les messages d’hameçonnages que vous recevez.

12. Si vous êtes ou croyez être victime de fraude en ligne, au guichet automatique, sur votre carte de débit ou votre carte de crédit Visa Desjardins, composez l'un des numéros suivants :
    - Montréal et les environs : 514-397-8649;
    - Canada et États-Unis : 1-866-335-0338;
    - Autres pays : 514 397-4610 (à frais virés).