LBE Ordinateurs et Internet - Programme 9

Auteur: Richard Lough
Rédaction: Maja Dreyer
Traduction: Yann Durand

Personnages: Beatrice (fille adolescente), John (garçon adolescent), Internet (voix off mécanique), expert (homme adulte)
Clips (English) à synchroniser: Daniel Gichuki (Homme environ 35 ans)
1 voix supplémentaire: 1 présentateur pour annonce et désannonce

Générique LbE

Annonce :

Narrateur :

Bonjour et bienvenue dans la série Learning by Ear de la Deutsche Welle consacrée aux ordinateurs et à l’Internet. Dans cette neuvième et dernière partie Béatrice et John vont explorer le monde obscur de la criminalité sur le web. Chaque jour dans l’Internet des fraudeurs sont occupés à subtiliser des données d’indentification pour extorquer aux internautes des millions d’Euros. Mais pourquoi l’Internet a-t-il autant de succès auprès des criminels ? Restez avec nous et vous aurez la réponse…

SFX_Internet_connexion

1.Internet: Bonjour Béatrice, Bonjour John

2. John/Beatrice: Salut l’web.

3. Internet: Je me demande si vous avez déjà assisté à un braquage de banque.

[SFX_sirène de police]

4. John: Tu veux dire des gens armés qui volent des sacs pleins de billets ?

5. Beatrice: Jamais.

6. Internet: Ça ne me surprend pas. Du moins ça ne m’aurait pas étonné avant que l’Internet n’entre dans votre vie.

7. John: PARDON?

8. Internet: Maintenant que vous surfez sur le Web et que vous possédez un compte E-mail, les chances sont grandes que vous ayez été ciblés par des braqueurs de banque sous forme de fraudeurs online.

9. Beatrice/John: QUOI !?!

10. Internet: Vous savez il est très difficile de me contrôler. C’est donc aux utilisateurs comme vous de se protéger eux-mêmes.

11. Beatrice: Mais comment est-ce qu’on peut faire?

12. Internet: Vous allez entendre plus d’information à ce sujet dans la deuxième partie de l’émission. Vous savez les fraudeurs ont volé des centaines de millions de dollars et causé des milliards de dommages.

13. John: Et comment s’y prennent-ils ces criminels?

14. Internet: Ils ont plusieurs façons d’opérer. En fin de compte ce qu’ils veulent c’est votre argent. Et ils n’ont besoin que de pousser l’internaute à divulguer sont nom d’utilisateur et son mot de passe.

17. John: Mais comment ? Je veux dire… Jamais je ne révélerais mes données personnelles !

18. Internet Ils utilisent différent moyens. Par exemple : ils lancent ce qu’ils appellent un logiciel espion.

SFX_James_Bond_Anthem – if we can use it…

19. John: Ça paraît très sournois …

20. Internet: Ça l’est. C’est un programme qui peut être envoyé à quelqu’un pour acquérir des informations confidentielles comme le numéro de compte bancaire, des mots de passe etc…

21. Beatrice: C’est ça qu’ils appellent un scam 419 ?

22. Internet: Non pas du tout ! Les 419 sont peut-être le meilleur exemple de fraude en ligne qui vient de l’Afrique. Ça a commencé au Nigéria au début des années 1980. Et là vous pouvez voir mon point faible : L’augmentation massive des utilisateurs d’E-Mail a rendu le coût d’envoi de Scam très bon marché.

23. John: D’où vient le numéro 419 ?

24. Internet: Il fait référence à l’article du code pénal nigérian qui concerne la fraude.

SFX_Typing

25. Internet: Voilà un scam que j’ai récupéré dans la corbeille d’un internaute récemment. Lisez-le

26. John: **(lit)** “Cher monsieur, j’ai le privilège de solliciter votre aide pour transférer la somme de 47 millions de dollars sur votre compte.”

27. Beatrice: **(lit)** “La somme citée résulte d’un contrat surfacturé. Elle se trouve actuellement sur un compte de la Banque centrale du Nigéria, La Banque Apex.”

28. John: **(lit)** “ Si vous jugez cette proposition acceptable, nous aurions besoin de vos coordonnées bancaires, nom et numéro de compte ainsi que votre adresse. ”

29. Beatrice: [rit] Et les gens s’y laisse vraiment prendre ?

30. Internet: Hélas oui, ils tombent dans le panneau.

31. Beatrice: Bon, qu’est que nous devrions faire si nous recevions une telle lettre ?

32. Internet: Il vous faut immédiatement l’effacer

[**SFX_Recycle_Bin Transfert dans la corbeille]**.

Il existe aussi des sites Internet sur lesquels on peut signaler de tels cas de fraude.

33. Beatrice Tous les crimes sur l’Internet sont centrés sur l’argent ?

34. Internet: Non hélas ce n’est vrai. On peut trouver des gens qui m’utilisent pour poster des photos pornographiques illégales montrant des enfants…

35. John Et j’ai un ami qui a été contacté par un étranger dans un forum online.

36. Internet C’est un autre domaine où vous devez être très méfiant. Quand vous chatter sur le Net, vous n’avez aucune idée de l’identité de la personne avec laquelle vous parlez. Elle peut avoir l’air d’un charmant jeune homme.

37. Beatrice: Mais en réalité c’est un délinquant sexuel.

38. Internet: Exactement, on ne sait jamais. Alors quand vous m’utiliser souvenez-vous de ne jamais baisser la garde.

39. John: Merci de tes bons conseils Web.

Transition:

Narrateur :

Pour clore cette première partie. Un bref résumé : ne donnez pas de détails que j'aimais vous ne dévoileriez en présence d'un étranger. Dans le second volet de cette émission nous allons apprendre d'un expert en informatique quelques instruments pour protéger ses données personnelles et se préserver des escroqueries.

Music – Full up for 0:10 then fade under Intro_9.2

Narrateur :

Après avoir abordé le monde de la fraude sur l'Internet. John et Beatrice s'intéressent aux moyens à mettre en œuvre pour protéger les informations privées face aux abus frauduleux. Notre expert maison est là pour les renseigner.

SFX_IAT_Gichuki_RoomTone

1. Beatrice Je suis ici à l'institut des hautes technologie de Nairobi pour parler avec Daniel Gichuki, l'un des enseignants de l'établissement. Je veux en apprendre plus sur la façon de se protéger de la fraude en ligne. Daniel, lorsque l'on surfe sur le Web. Est-ce qu'on laisse des traces ?

Clip: 9.2_Gichuki_1a

Grâce à certains navigateurs on est en mesure de relever les informations auxquelles on a eu accès.

2. Beatrice: Vraiment ? et comment ?

Clip: 9.2_Gichuki_1b

Par exemple on dispose d’une fonction installée sur la plupart des navigateurs et qu’on appelle cookies. Lorsque tu t’es rendu sur un site, tu y a laissé des informations telles que ton nom d’utilisateur, ton code d’entrée… peut-être que tu as ouvert une page particulière où tu a enregistré tes coordonnées personnelles. … Ton adresse ou se genre de chose. Les cookies permettent, s’il s’agit de sites que tu visite souvent, de ne pas avoir à redonner ses informations.

3. Beatrice: Bon, ça a l’air Ok. Ces cookies sont sûrement sécurisés, non ?

Clip: 9.2_Gichuki_3

Ils sont vulnérables. En fait avec des cookies activés, il est possible que quelqu’un s’y connecte et utilise les informations contre toi.

SFX: Beep sound (Bip introduisant chaque intervention de l’expert)

4. Expert: Bonjour Beatrice, ici l’expert depuis le studio. Sais-tu que quoique tu fasses avec ton ordinateur, il est possible reconstituer exactement ce que tu as effectué en ligne ? Ils peuvent constater quels site tu as consulté, quels documents tu as ouvert, quels films tu as téléchargés. Ils peuvent même accéder aux données confidentielles que tu as fournies tout au long de tes recherches.

5. Beatrice: Ça a l’air alarmant ! Mais parfois on est obligé de donner ses coordonnées quand on est en ligne, même si on ne veut pas les dévoiler aux autres. Daniel, les navigateurs peuvent-ils faire quelque chose pour régler ce problème ?

Clip: 9.2_Gichuki_4

Ce que différents sites ont essayé de faire, c’est d’instaurer des pages sécurisées. C’est-à-dire que les informations qui s’y trouvent sont cryptées avec une sorte de code. Il n’est donc pas facile pour quelqu’un de lire ses informations et de les comprendre.

6. Beatrice: Et y a-t-il autre chose que les internautes puissent faire pour se protéger ? Est-ce qu'il existe par exemple un moyen d'empêcher que des pirates se connectent à ton ordinateur ?

Clip: 9.2_Gichuki_4

Il y a les pare-feux. Il est possible d'en installer un. Et aujourd'hui la plupart des systèmes d'exploitation disposent automatiquement d'un pare-feu pour filtrer les informations qui entrent et qui sortent.

SFX: Beep sound (Bip expert)

7. Expert: Beatrice permet moi d'intervenir pour expliquer plus en détails.

8. Beatrice: Bien sûr !

9. Expert: Le pare-feu est la première ligne de défense concernant la protection des informations confidentielles. Un pare-feu est un programme qui fonctionne comme une barrière. Elle maintient les forces destructrices loin de tes biens. C'est pour cela qu'on l'appelle pare-feu. Sa fonction est la même qu'un pare-feu réel qui empêche un incendie de se propager d'un endroit à un autre.

11. Beatrice: Ok….

12. Expert Toute information qui atteint le pare-feu est examinée. Celles qui ne correspondent pas aux critères spécifiques de sécurité sont bloquées.

13. Beatrice: Bien… Daniel en installant un pare-feu, peut-on être certain que nos données sont protégées ?

Clip: 9.2_Gichuki_6

Je pense qu'on ne peut pas être sûr à 100 % parce c'est basé sur un cycle. On peut s'équiper d'un pare-feu très puissant et se sentir tout à fait à l'abri et puis quelqu'un arrive avec un nouveau logiciel espion ou d'autres programmes louches.

SFX_ IAT_ Gicuki_RoomTone (Atmo bureau Gichuki)

Désannonce

Narrateur :

Voilà c'est fini pour aujourd'hui Et nous nous quittons non sans avoir résumé le contenu de cette émission : N'oubliez pas qu'à chaque fois que vous êtes en ligne vous êtes exposés aux regards indiscrets. Assurez-vous que les sites dont l'accès nécessite vos données personnelles sont sécurisés et installez un pare-feu.
Si vous souhaitez réécoutez cette émission ou l'ensemble du programme Learning by Ear ou encore en parlez à vos amis, rendez-vous sur www.dw-world.de/lbe. Merci de attention et à Bientôt.