Sensibilisation à la sécurité du SI 1

(Attaques, Phishing, MELANI, Stop-Think-Connect...)

24heures

Des journaux belges et français ont été à nouveau paralysés

Des titres de la presse ré
nouveaux actes de **pirata**
présent consultables. Il n
professionnelles. Plus...

14.04.2015

- 07.05.2015 Cheval de Troie bancaire „Dyre": propagation massive
- 31.03.2015 Clients de PME suisses visés par des attaques de phishing sur mesure
- 02.02.2015 PME visées par un cheval de Troie bancaire

Des escrocs envoient des faux courriels au nom de l'Administration

Internet Une nouvelle vague de «phishing» déferle dans les boîtes mail helvétiques. Les escrocs demandent les coordonnées de cartes bancaires au nom de l'OFEN. Plus...

04.07.2014

Des clients de Migros visés par des escrocs à la carte-cadeau

Internet Utilisant la technique du «phishing», des escrocs ont tenté d'extorquer de l'argent à des clients de Migros en leur faisant miroiter une offre particulièrement attractive. Plus...

27.09.2013

Le phishing explose sur les téléphones mobiles

Sécurité 15 millions de SMS frauduleux sont envoyés chaque jour en Europe. La Suisse n'est pas épargnée, avertit l'opérateur Sunrise. Plus...

DREAMLAB TECHNOLOGIES

6 months compromised (apr-sep 2014).
56mio credit card leaked.
70mio customer personal data stolen.
10'000 lines of code to fix the breach.
85'000 new pin pad deployed.

La Sécurité, au cœur de notre quotidien

Alerte aux faux amis sur Facebook

Phishing Un appel à l'aide d'un ami sur Facebook, un coup de fil pour débloquer son téléphone et voilà 40 francs envolés: les auteurs d'arnaques via les réseaux sociaux redoublent d'audace dans leur manière de procéder. Plus...

Des hackers russes ont lu les mails d'Obama

Cyberattaque Des hackers sont entrés dans le système informatique non classé secret de la Maison-Blanche et ont eu accès aux e-mails du président. Plus...

Swissquote a été victime mercredi d'une attaque par deni de service. D'autres banques suisses auraient été touchées.

Les Suisses se font plus souvent piéger que les autres sur le net

Pouriels Les internautes suisses se font plus souvent piéger que les autres par les pirates de comptes email. Plus...

30.04.2015

Cet e-mail vient-il vraimen
3,1 milliards de dollars

Wanna

Un bug dans iOS12 m

Phish

Le groupe Pathé a été victime d'une fraude pour plus de 19,2 millions d'euros

Monde
Publié samedi à 16:10 (10.11.2018)

Les nouvelles armes du Pentagone sont truffées de vulnérabilités

Sécurité - Mauvais mots de passe, déficit de chiffrement, nombreuses failles non corrigées... Les dernières armes pilotées par l'informatique développées par le ministère américain de la Défense sont vulnérables.

https://actu.epfl.ch/news/massive-phishing-targeting-epfl-users/

EPFL | PAR PUBLIC | PAR FACULTÉ | EPFL EN BREF

EPFL > News

NEWS IT SECURITY

EPFL ENAC SB STI IC SV CDM CDH All

Share:

Massive phishing targeting EPFL users

***19.11.18* - A large scale phishing campaign using stolen EPFL credentials has been launched against the School this morning.**

More than 17'000 email addresses have been targeted. The attackers set up a lookalike EPFL webmail login page and sent the fraudulent link through valid email addresses, which misled a large number of unsuspecting users. We have thus taken additional security measures to contain this incident.

Most of the time, a phishing email can be spotted because of unusual sender addresses, or web links poorly imitating official institutions. The task becomes harder when you know the sender! Always keep in mind that you can never be sure of a sender's true identity.

If you are concerned about an email, we kindly advise you not to click on any attachment or web link, and send it to 1234@epfl.ch for analysis.

ent gratuitement un service de

uvelle attaque sur ses

cident de phishing datant de
identifié comme étant à l'origine
er piratage et du vol de données

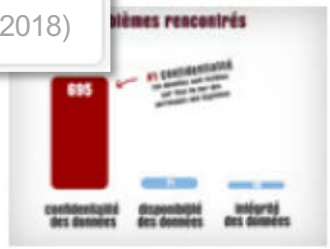
nbre 2018 par Catalin Cimpanu

découverte dans libssh, une

dont 46 avec un taux de gravité de 9,8+

n'était pas le plus gros patch d'Oracle. La palme revenait

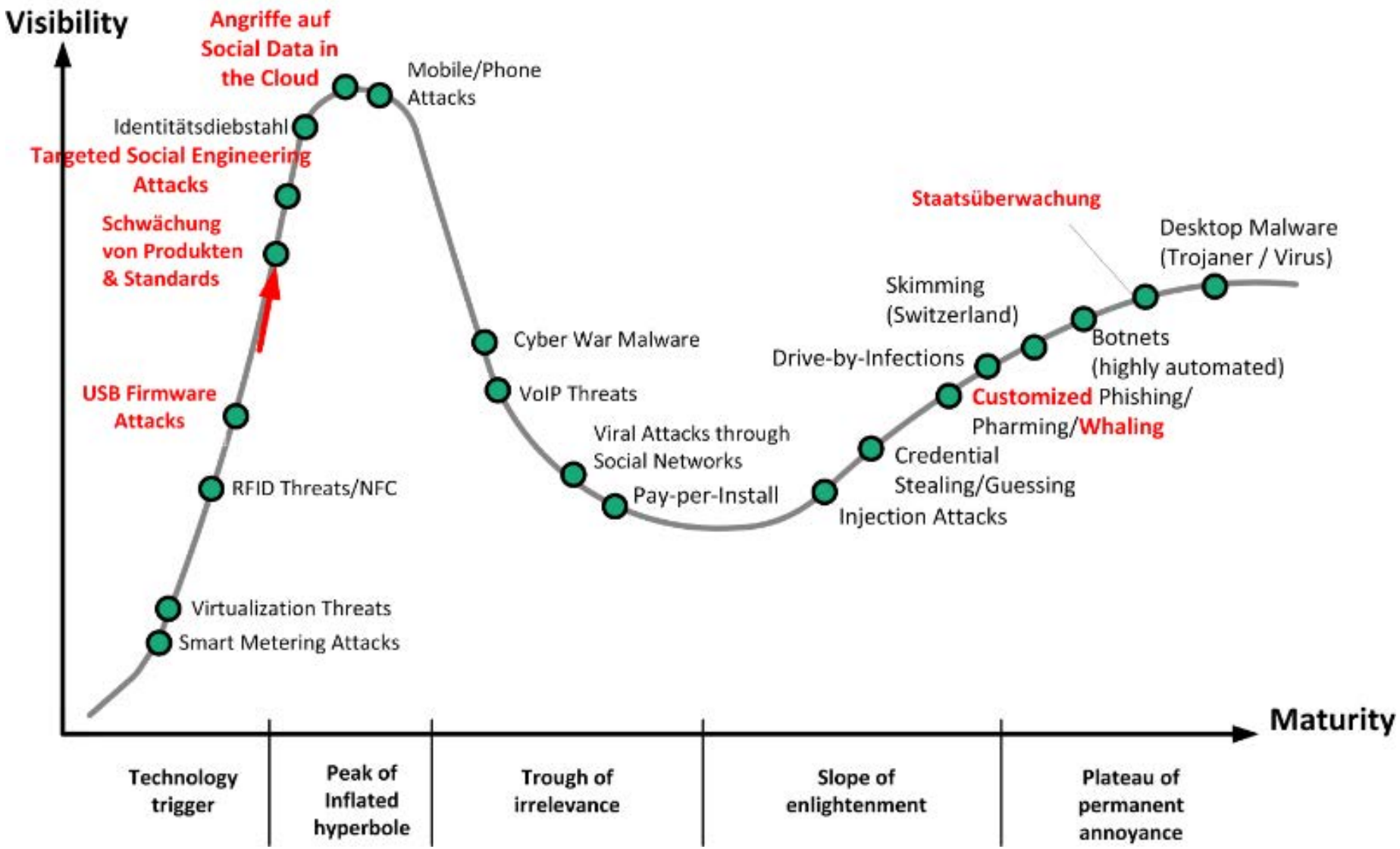
ions de données personnelles : la Cnil a reçu 742 notifications en 4 mois



Sécurité - La Cnil fait un premier bilan du RGPD et annonce avoir reçu 742 notifications pour des violations de données. Le secteur de l'hôtellerie est particulièrement touché, mais surtout "surreprésenté", avec 185 notifications. La première cause est externe et prend la forme d'actes de malveillance.

Mercredi 17 Octobre 2018 par Christophe Auffray

Des problèmes de sécurité… incessants



AdNovum's Information Security Hype Cycle as of March 2015
(Based on Gartner's Hype Cycle for Information Security)
http://www.adnovum.ch/en/wissen/focus/knowhow/adnovum_security_update_2015.html

Administration fédérale > DFF / DDPS > UPIC / SRC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

Les attaques de virus ou de vers tels que "Blaster" et "Slammer" ont causé la panne de millions d'ordinateurs à travers le monde. Tout système peut être victime de telles attaques, en particulier s'il est connecté à l'Internet:

- Les virus, vers, chevaux de Troie ainsi que les logiciels espions et les témoins de connexion (*cookies*) peuvent entraîner une perte irrémédiable de données ou représenter une intrusion grave dans la sphère privée. Les secrets d'affaires, les adresses de partenaires commerciaux, les numéros de téléphones portables de parents et amis, la correspondance avec la caisse d'assurance-maladie ou le médecin traitant, etc., risquent ainsi d'être détruits ou, pire encore, d'être copiés à votre insu.

- Les hameçonnages (*phishing*) et les numéroteurs (*dialers*) peuvent entraîner des achats non autorisés et facturés sur votre carte de crédit ou causer des frais de téléphone pour plusieurs centaines de francs. Il est souvent difficile de convaincre sa banque ou l'opérateur de téléphonie que les transactions effectuées étaient illicites.

- Les canulars (*hoaxes*) et les pourriels (*spam*) ne sont souvent que des incidents fâcheux causant une perte de temps (à cause du tri manuel); ils peuvent parfois aussi avoir des conséquences fâcheuses si l'on suit leurs indications ou si l'on accepte l'offre qu'ils contiennent.

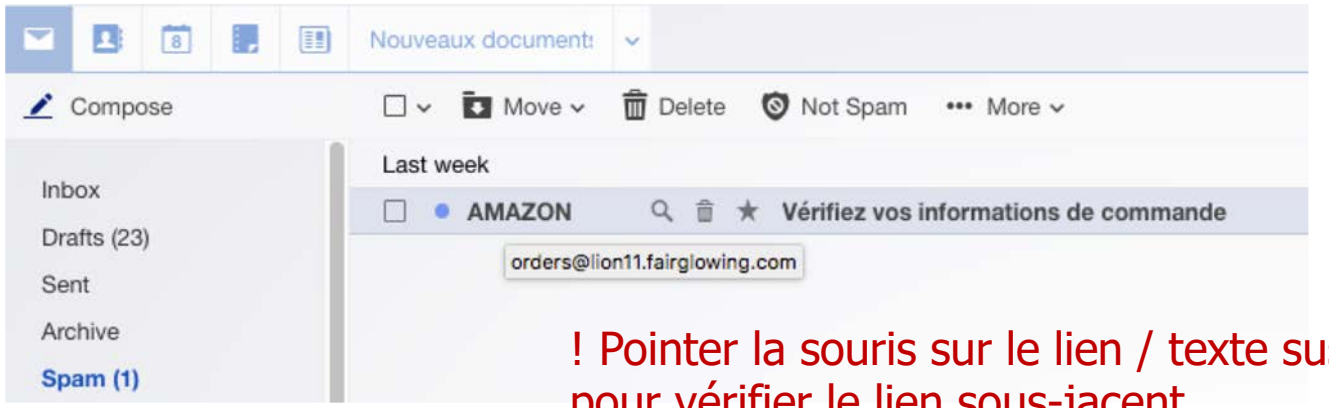
http://www.melani.admin.ch/index.html?lang=fr

Quelques recommandations… pour éviter le *Phishing*

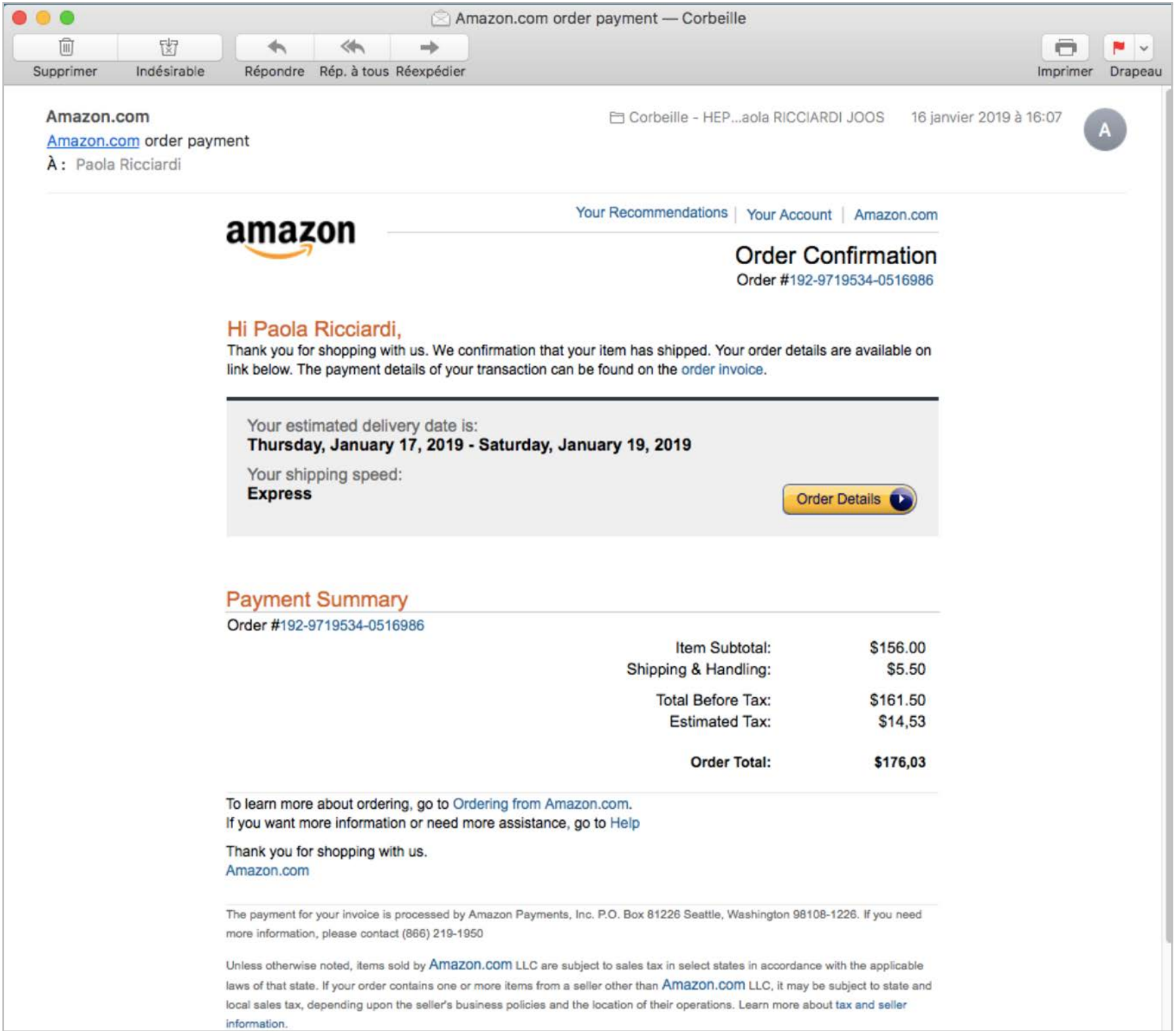
APWG Unifying the Global Response to Cybercrime

- Méfiez-vous de tout e-mail ou de communication avec des demandes d'informations financières, sensibles ou personnelles.
- Évitez de cliquer sur les liens. Au lieu de cela, aller sur le site en tapant l'adresse web directement dans votre navigateur ou en recherchant dans un moteur de recherche.
- Ne pas envoyer d'informations financières, sensibles ou personnelles par e-mail, et éviter de remplir des formulaires dans les e-mails qui vous demandent vos informations.
- Utilisez un site web sécurisé (https:// et l'icône « cadenas » https://) lors de la présentation de carte de crédit ou d'autres informations sensibles en ligne.

http://www.antiphishing.org/resources/overview/avoid-phishing-scams



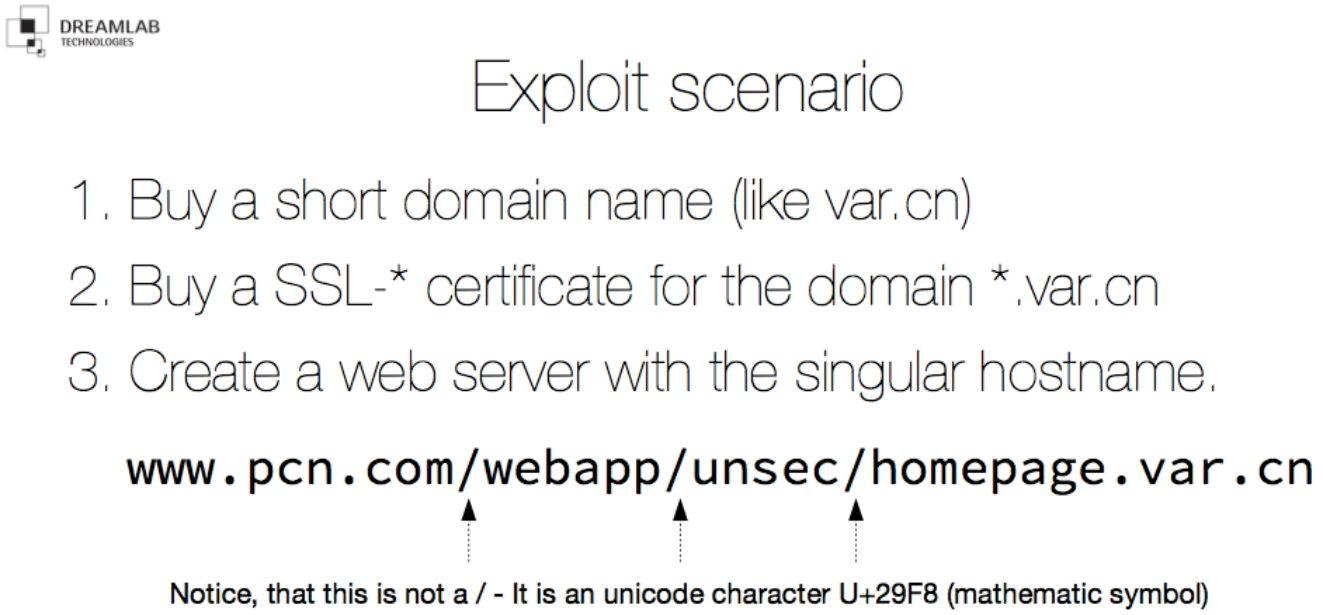
! Pointer la souris sur le lien / texte suspicieux pour vérifier le lien sous-jacent


Amazon.com order payment — Corbeille
Supprimer
Indésirable
Répondre
Rép. à tous
Réexpédier
Imprimer
Drapeau
Amazon.com
Amazon.com order payment
À : Paola Ricciardi
Corbeille - HEP...aola RICCIARDI JOOS
16 janvier 2019 à 16:07
A
amazon
Your Recommendations | Your Account | Amazon.com
Order Confirmation
Order #192-9719534-0516986
Hi Paola Ricciardi,
Thank you for shopping with us. We confirmation that your item has shipped. Your order details are available on link below. The payment details of your transaction can be found on the order invoice.
Your estimated delivery date is:
Thursday, January 17, 2019 - Saturday, January 19, 2019
Your shipping speed:
Express
Order Details
Payment Summary
Order #192-9719534-0516986
Item Subtotal: $156.00
Shipping & Handling: $5.50
Total Before Tax: $161.50
Estimated Tax: $14,53
Order Total: $176,03
To learn more about ordering, go to Ordering from Amazon.com.
If you want more information or need more assistance, go to Help
Thank you for shopping with us.
Amazon.com
The payment for your invoice is processed by Amazon Payments, Inc. P.O. Box 81226 Seattle, Washington 98108-1226. If you need more information, please contact (866) 219-1950
Unless otherwise noted, items sold by Amazon.com LLC are subject to sales tax in select states in accordance with the applicable laws of that state. If your order contains one or more items from a seller other than Amazon.com LLC, it may be subject to state and local sales tax, depending upon the seller's business policies and the location of their operations. Learn more about tax and seller information.

Client Mail: menu >
Présentation > Message > Contenu brut

Return-Path: <diego.miranda@lge.mx>
X-Spam-Status: No, hits=0.0 required=2.3
tests=TOTAL_SCORE: 0.000
X-Spam-Level:
Received: from hepl.ch ([195.176.194.153])
by webmail.hepl.ch with ESMTPS
(using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256 bits))
for paola.ricciardi-joos@hepl.ch;
Wed, 16 Jan 2019 16:07:57 +0100
Received: from server.logrand.net ([162.214.19.85])
by hepl.ch stage1 with esmtp
(Exim MailCleaner)
id 1gjmmt-0008NN-Qn
for <paola.ricciardi-joos@hepl.ch>
from <diego.miranda@lge.mx>; Wed, 16 Jan 2019 16:07:28 +0100
X-MailCleaner-SPF: pass
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=lge.mx;
s=default; h=Content-Type:MIME-Version:Subject:Message-
ID:To:From:Date:Sender
:Reply-To:Cc:Content-Transfer-Encoding:Content-ID:Content-Description:
Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc:Resent-
Message-ID:
In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:List-Subscribe:
List-Post:List-Owner:List-Archive;
bh=rwEZlxXswtb0ue+J8HZdvutglUb8IZ2nxN6kDLbUg0o=;
b=f8fNqWC/6BCUX3Aa9u2R1xAEm+
K98q8AKamDpYuuZXJlw93bJ7EkawmknAOBP50J+KMtOz5u1twbQurqhyRy
W30XL5fMf4ZLGRFqWai
3t94fr1ZiIWAI03EWKrplFgaBcfbVGupTIkgqMzqAVUJzjc1NXLf59O6y31LgMF
mr/P0MOn4WFu11
NdAc/IhZLvCjYb+sS1oWXhdTndoAqElzQ/Fv3KwiYemYD8UN+Bb/32I85mt/D
ZMlMsWWRB/okfv4q
ujq24Z9Jza/rysGlvGWwwobivAsLRMIuy/eVC1IdhHDachfcSUFZFSBcwEQAH
p0w4CflABmvBWF9C
MFTky4PA==;
Received: from host-181-177-181-91.supernet.com.bo
([181.177.181.91]:62638 helo=10.4.45.119)
by server.logrand.net with esmtpsa (TLSv1.2:ECDHE-RSA-AES256-GCM-
SHA384:256)
(Exim 4.91)
(envelope-from <diego.miranda@lge.mx>)
id 1gjn2e-0000X0-Qa
for paola.ricciardi-joos@hepl.ch; Wed, 16 Jan 2019 09:23:45 -0600
Date: Wed, 16 Jan 2019 11:09:42 -0400
From: Amazon.com <auto-confirm@amazon.com> <diego.miranda@lge.mx>
To: paola.ricciardi-joos@hepl.ch
Message-ID: <9411184983930419769.DC98F593D515B179@hepl.ch>
Subject: Amazon.com order payment
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----
=_Part_23865_1280071544.374072465410949532"
X-AntiAbuse: This header was added to track abuse, please include it with any
abuse report
X-AntiAbuse: Primary Hostname - server.logrand.net
X-AntiAbuse: Original Domain - hepl.ch
X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12]
X-AntiAbuse: Sender Address Domain - lge.mx
X-Get-Message-Sender-Via: server.logrand.net:
authenticated_id: diego.miranda@lge.mx
X-Authenticated-Sender: server.logrand.net: diego.miranda@lge.mx
X-Source:
X-Source-Args:
X-Source-Dir:
Authentication-Results: localhost; dmarc=skipped
X-Newsl: is not newsletter (0.0/5.0)
X-NiceBayes: is not spam (0%)
X-Spamc: is not spam (score=3.4, required=5.0)
X-MailCleaner-Information: Please contact mailcleaner@hepl.ch for more
information
X-MailCleaner-ID: 1gjmmu-0008OT-9m
X-MailCleaner: Found to be clean
X-MailCleaner-SpamCheck: not spam, Newsl (score=0.0, required=5.0,),
Spamc (score=3.4, required=5.0, FSL_HELO_BARE_IP_2 0.0,
T_REMOTE_IMAGE 0.0, DKIM_ADSP_ALL 0.8, MIME_HTML_ONLY 0.0,
BAYES_00 0.0, DKIM_SIGNED 0.6, MC_DBLE_ADR 2.0, T_DKIM_INVALID
0.0,
HTML_MESSAGE 0.0)
X-MailCleaner-ReportURL: https://va7549.mailcleaner.net/rs.php

Attention au certificat et à l'URL même avec le HTTPS



Source: Eb-Qual, Information security day, 2015-03-10
[2_Les attaques DNS_eb-Qual Security Day_March2015.pdf]

Ex. Piratage possible de BCV-net:

Page de login pour accéder au e-payment BCV-net:

https://www.bcv.ch/bcvd-login/authenticateAction.do

Page piratée pour accéder au e-payment BCV-net:

https://www.bcv.ch/bcvd-login/authenticateAction.do.var.cn

Quelques recommandations… de sécurité

- [MELANI] Règles de comportement:
  http://www.melani.admin.ch/themen/00166/00172/index.html?lang=fr
- [MELANI] E-banking « en toute sécurité » :
  http://www.melani.admin.ch/dienstleistungen/00132/00148/index.html?lang=fr
- Swiss governmental CERT: http://www.govcert.ch

Mais aussi:

- [ANSSI] Agence nationale pour la sécurité des SI:
  http://www.ssi.gouv.fr/administration/bonnes-pratiques/
- CERT-FR (Computer Emergency Response Team):
  http://www.cert.ssi.gouv.fr/
- Apprenez à naviguer en sécurité sur internet (cours en ligne):
  http://openclassrooms.com/courses/apprenez-a-naviguer-en-securite-sur-internet

Conservez votre ordinateur propre et à jour
Protégez vos informations personnelles
Soyez prudent lorsque vous êtes en ligne
Soyez attentif sur le Web
Soyez un bon internaute

http://www.stopthinkconnect.org/tips-and-advice/french-canadian-tips-and-advice/

STOP | THINK | CONNECT™

Centrale d'enregistrement et d'analyse pour la sûreté de l'information
MELANI

Conservez votre ordinateur propre et à jour

Actualisez votre logiciel de sécurité
Automatisez les mises à jour des logiciels
Protégez tous les périphériques connectés à Internet
Clé et lecteur USB

Protégez vos informations personnelles

Sécurisez vos comptes
Créez des mots de passe complexes et forts
Un mot de passe distinct pour chaque compte
Soyez maître de votre présence en ligne

Soyez prudent lorsque vous êtes en ligne

En cas de doute, supprimez le message reçu
Méfiez-vous des points d'accès Wi-Fi
Protégez vos finances

Soyez attentif sur le Web

Soyez à jour. Restez au fait des nouvelles méthodes de sécurité en ligne.
Réfléchissez avant d'agir
Effectuez des sauvegardes

Soyez un bon internaute

Plus de sécurité pour vous et donc pour les autres
Ne publiez pas d'informations sur les autres s'ils n'en publient pas sur vous.
Aidez les autorités à lutter contre la criminalité en ligne

http://www.stopthinkconnect.org/tips-and-advice/french-canadian-tips-and-advice/

Règles de comportement

En dehors des mesures techniques (p. ex. pare-feu personnel, mises à jour des logiciels, programme antivirus, etc.) destinées à améliorer la sécurité d'un ordinateur, c'est avant tout le comportement de chaque utilisateur qui s'avère d'une importance décisive. Le comportement adéquat comprend:

>> Choisir un bon mot de passe,
>> Etre prudent en utilisant le courrier électronique,
>> Etre prudent naviguant sur le Web,
>> Configurer correctement le système et le navigateur,
>> Etre prudent en utilisant les réseaux poste à poste et en participant aux bourses d'échange.

http://www.melani.admin.ch/themen/00166/00172/index.html?lang=fr

Guide d'hygiène informatique (1/2)

Connaître le SI et ses utilisateurs:

1 - Disposer d'une cartographie précise de l'installation informatique et la maintenir à jour.
2 - Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour.
3 - Rédiger et appliquer des procédures d'arrivée et de départ des utilisateurs (personnel, stagiaires...).

Maîtriser le réseau:

4 - Limiter le nombre d'accès Internet de l'entreprise au strict nécessaire.
5 - Interdire la connexion d'équipements personnels au système d'information de l'organisme.

Mettre à niveau les logiciels:

6 - Connaître les modalités de mises à jour de l'ensemble des composants logiciels utilisés et se tenir informé des vulnérabilités de ces composants et des mises à jour nécessaires.
7 - Définir une politique de mise à jour et l'appliquer strictement.

Authentifier l'utilisateur:

8 - Identifier nommément chaque personne ayant accès au système.
9 - Définir des règles de choix et de dimensionnement des mots de passe.
10 - Mettre en place des moyens techniques permettant de faire respecter les règles relatives à l'authentification.
11 - Ne pas conserver les mots de passe en clair dans des fichiers sur les systèmes informatiques.
12 - Renouveler systématiquement les éléments d'authentification par défaut (mots de passe, certificats) sur les équipements (commutateurs réseau, routeurs, serveurs, imprimantes).
13 - Privilégier lorsque c'est possible une authentification forte par carte à puce.

Sécuriser les équipements et terminaux:

14 - Mettre en place un niveau de sécurité homogène sur l'ensemble du parc informatique.
15 - Interdire techniquement la connexion des supports amovibles sauf si cela est strictement nécessaire ; désactiver l'exécution des autoruns depuis de tels supports.
16 - Utiliser un outil de gestion de parc informatique permettant de déployer des politiques de sécurité et les mises à jour sur les équipements.
17- Gérer les terminaux nomades selon une politique de sécurité au moins aussi stricte que celle des postes fixes.
18 - Interdire dans tous les cas où cela est possible les connexions à distance sur les postes clients.
19 - Chiffrer les données sensibles, en particulier sur les postes nomades et les supports potentiellement perdables.

Sécuriser l'intérieur du réseau:

20 - Auditer ou faire auditer fréquemment la configuration de l'annuaire central (Active Directory en environnement Windows ou annuaire LDAP par exemple).
21 - Mettre en place des réseaux cloisonnés. Pour les postes ou les serveurs contenant des informations importantes pour la vie de l'entreprise, créer un sous- réseau protégé par une passerelle d'interconnexion spécifique.

http://www.ssi.gouv.fr/administration/bonnes-pratiques/

Guide d'hygiène informatique (2/2)

22 - Éviter l'usage d'infrastructures sans fil (Wifi). Si l'usage de ces technologies ne peut être évité, cloisonner le réseau d'accès Wifi du reste du système d'information.
23 - Utiliser systématiquement des applications et des protocoles sécurisés.

Protéger le réseau interne de l'internet:

24 - Sécuriser les passerelles d'interconnexion avec Internet.
25 - Vérifier qu'aucun équipement du réseau ne comporte d'interface d'administration accessible depuis l'Internet.

Surveiller les systèmes:

26 - Définir concrètement les objectifs de la supervision des systèmes et des réseaux.
27 - Définir les modalités d'analyse des événements journalisés.

Sécuriser l'administration du réseau:

28 - Interdire tout accès à Internet depuis les comptes d'administration.
29 - Utiliser un réseau dédié à l'administration des équipements ou au moins un réseau logiquement séparé du réseau des utilisateurs.
30 - Ne pas donner aux utilisateurs de privilèges d'administration. Ne faire aucune exception.
31 - N'autoriser l'accès à distance au réseau d'entreprise, y compris pour l'administration du réseau, que depuis des postes de l'entreprise qui mettent en œuvre des mécanismes d'authentification forte et protégeant l'intégrité et la confidentialité des échanges à l'aide de moyens robustes.

Contrôler l'accès aux locaux et à la sécurité physique:

32 - Utiliser impérativement des mécanismes robustes de contrôle d'accès aux locaux.
33 - Protéger rigoureusement les clés permettant l'accès aux locaux et les codes d'alarme.
34 - Ne pas laisser de prises d'accès au réseau interne accessibles dans les endroits ouverts au public.
35 - Définir les règles d'utilisation des imprimantes et des photocopieuses.

Organiser la réaction en cas d'incident:

36 - Disposer d'un plan de reprise et de continuité d'activité informatique, même sommaire, tenu régulièrement à jour décrivant comment sauvegarder les données essentielles de l'entreprise.
37 - Mettre en place une chaîne d'alerte et de réaction connue de tous les intervenants.
38 - Ne jamais se contenter de traiter l'infection d'une machine sans tenter de savoir comment le code malveillant a pu s'installer sur la machine, s'il a pu se propager ailleurs dans le réseau et quelles informations ont été manipulées.

Sensibiliser:

39 - Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires.

Faire auditer la sécurité:

40 - Faire réaliser des audits de sécurité périodiques (au minimum tous les ans). Chaque audit doit être associé à un plan d'action dont la mise en œuvre est suivie au plus haut niveau.

http://www.ssi.gouv.fr/administration/bonnes-pratiques/

Quizz

- La Loterie romande fait un tirage au sort pour distribuer une cagnotte. Vous avez reçu un mail « gagnant » vous demandant de vous connecter sur votre compte e-banking pour recevoir votre gain.
  a) Chouette, vous démissionnez de la HEP et cliquez sur le lien pour accéder à votre compte e-banking pour recevoir l'argent
  b) Chouette, vous cliquez sur le lien pour accéder à votre compte e-banking pour recevoir l'argent
  c) Vous appelez la Loterie romande pour les détails, ou vous ignorez le message
- Votre banque vous informe par email qu'une transaction suspecte a eu lieu sur votre compte et vous demande de cliquer sur un lien pour accéder à votre compte e-banking et vérifier la transaction.
  a) Vous cliquez sur le lien pour accéder à votre compte et vérifier la transaction
  b) Vous allez sur le site web de votre e-banking pour accéder à votre compte pour vérifier la transaction
  c) Vous appelez votre conseillère / banque, ou ignorez le message
- Vous trouvez une clé USB dans le couloir, avec une description « Documents confidentiels ».
  a) Vous branchez la clé USB sur votre ordinateur pour lorgner sur les dossiers / documents confidentiels
  b) Vous êtes honnête: vous branchez la clé USB sur votre ordinateur pour savoir à qui appartient la clé USB afin de la lui remettre
  c) Vous remettez la clé à la Réception ou au Support informatique
- Vous êtes collaborateur de la HEP. Vous recevez un appel (« Bonjour ici le Support informatique ») pour vous demander votre login + mot de passe pour corriger un problème sur votre poste.
  a) Vous vous dîtes « Ah, ils sont non seulement sympas, mais en plus prévoyants ces gens du Support » et vous donnez les infos demandées.
  b) Vous vous renseignez sur l'appelant-e, et si c'est bien une personne de la liste du Pôle Support, vous donnez les infos demandées.
  c) Vous raccrochez au nez…
- Vous recevez un mail de Apple ou Dropbox indiquant que votre compte a été piraté (ou expiré) et qu'il vous faut changer le mot de passe en cliquant sur le lien suivant.
  a) Pour des raisons de sécurité, vous allez de suite changer votre mot de passe en cliquant sur le lien communiqué
  b) Vous vous renseignez sur qui a envoyé le mail
- Un fournisseur vous envoie un fichier (ZIP) contenant des factures non payées.
  a) Pour éviter des contentieux, vous double-cliquez sur le ZIP pour vérifier les factures
  b) Vous vous renseignez sur qui a envoyé le mail
- Vous recevez un appel de la Cheffe du DJFC ou chef-de de la DGES ou chef-fe xyz vous demandant de faire un virement urgent car…

Mais toujours les mêmes techniques d'attaque initiale...

1. Unpatched vulnerabilities	➔ Patch/Fix rapide vs Régression
2. Security misconfigurations	➔ Quantité de paramètres, Hardening vs Rapidité, confort, utilisabilité
3. Weak, leaked, stolen passwords	➔ Mot de passe simple à retenir... mais difficile à pirater
4. Social engineering	➔ Comportement responsable... d'où la campagne de sensibilisation
5. Insider threat	➔ Surveillance vs Protection de la sphère privée

Source: Tim Rains, AWS, Regional Leader, Security & Compliance for EMEA

Recommandations de MELANI et ANSSI

MELANI
(Centrale d'enregistrement et d'analyse pour la sûreté de l'information)

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

Travaillez selon le principe du droit d'accès minimal (least privilege).
Il convient de n'octroyer aux collaborateurs que les droits d'accès dont ils ont besoin pour accomplir les tâches leur étant confiées. Les collaborateurs ne devraient pas jouir par défaut de droits d'administrateur.

ANSSI
(Agence nationale pour la sécurité du système d'information)

http://www.ssi.gouv.fr/administration/bonnes-pratiques/

Guide d'hygiène informatique:

Règle 30: ***Ne pas donner aux utilisateurs de privilèges d'administration. Ne faire aucune exception.***
De nombreux utilisateurs, y compris au sommet des hiérarchies, sont tentés de demander à leur service informatique de pouvoir disposer de privilèges plus importants sur leurs machines (pouvoir installer des logiciels, pouvoir connecter des équipements personnels, etc.). De tels usages sont cependant excessivement dangereux et sont susceptibles de mettre en danger le réseau dans son ensemble.

Recommandations relatives à l'administration sécurisée des systèmes d'information:

Règle 9: *Les droits d'administration des postes doivent être strictement réservés aux personnes en charge de leur configuration et uniquement utilisés pour des tâches qui s'y rapportent.*
Règle 8: *Tous les administrateurs ne doivent pas disposer des droits d'administration sur leur poste de travail. Il conviendra d'attribuer ces droits uniquement aux administrateurs en charge de l'administration des postes.*

Autres recommandations et références

- Sensibilisation:
  - Campagne de phishing, présentation sur des thèmes spécifiques
  - Module de sensibilisation de la DSI de l'Etat de Vaud: https://www.esusi.vd.ch

- ThinkData (http://www.thinkdata.ch):
  - Sensibilisation à la protection des données et à la transparence dans le cadre organisationnel.
- Privatim (http://www.privatim.ch/fr/):
  - Association des commissaires suisses à la protection des données
- CLUSIS (http://www.clusis.ch):
  - Association suisse de la sécurité de l'information

- Normes: ISO 27001, ISO 27002
- Référentiel: ISACA COBIT (http://www.isaca.org/cobit/)

Sensibilisation à la sécurité du SI:

La sécurité, c'est l'affaire de tous !

Merci pour votre coopération.