

**Votre
PME est-elle
en sécurité?**





Bienvenue

Sécurité informatique ★ ★ ★
un défi pour les garagistes

Les règles du jeu



Audio et vidéo

Le micro des participants est désactivé, ils doivent entendre les intervenants et voir les diapositives.



Questions et remarques

Il est possible de poser les questions à tout moment dans le chat. Les réponses sont fournies en continu.

**Le mythe:
sécurité informatique
= un défi pour les
PME**

trop cher

trop complexe

fastidieux

pas une priorité

aucun bénéfice direct

chronophage

évolution trop rapide

**L'UPSA s'engage à former ses membres
dans le domaine de la sécurité
informatique**



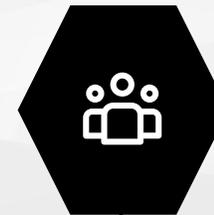
Cybermenace

Max Klaus,
Responsable adjoint cyber
sécurité opérative, NCSC



Environnement de travail moderne et sûr

Lydie Delon,
Spécialiste informatique,
Swisscom



Conclusion

Séance d'échange



Max Klaus

Responsable adjoint cyber sécurité
opérative, NCSC

NCSC

Centre national de cybersécurité :
mandat pour protéger les
infrastructures critiques en Suisse

Sécurité informatique – un défi pour les garagistes

Max Klaus

Chef suppléant cyber sécurité opérationnelle NCSC

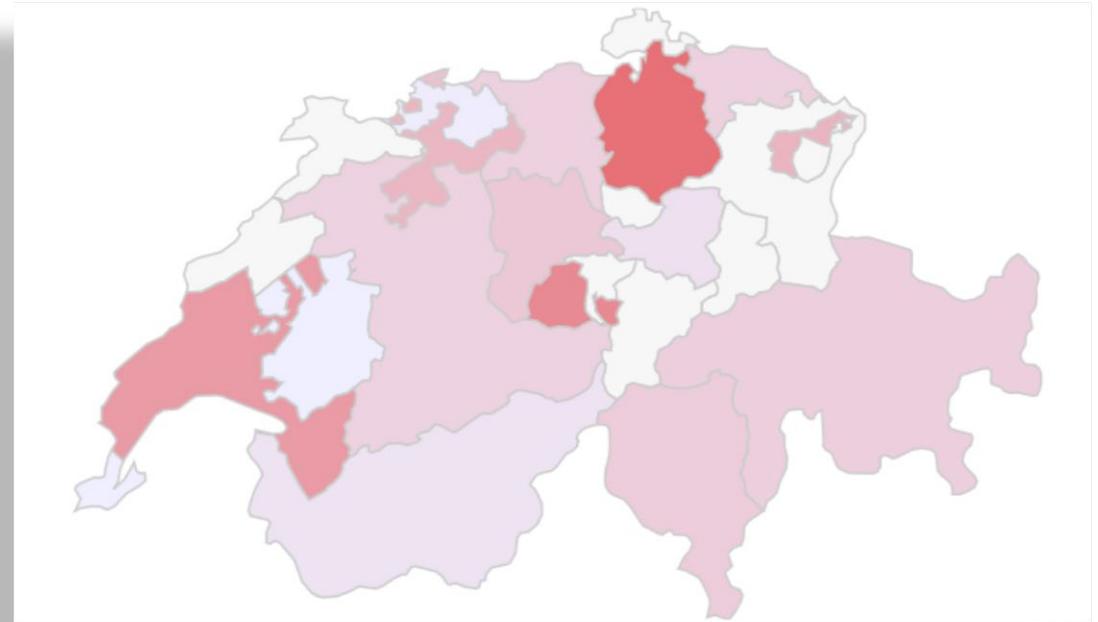
Contenus

- 1. Situation nationale et internationale**
2. Cyber attaques: deux exemples
3. Conclusions / recommandations

1. Situation nationale et internationale



Situation nationale et internationale



Quelle est la vulnérabilité des PME ?

LesEchos

À la une Idées Économie Politique Élections Monde Tech-Médias Entreprises Bourse Finance - Marchés Régions Patrimoine Le Mag W-E

orange

Cyberattaques : pas de pitié pour les PME ?

La crise a accéléré la transformation numérique des entreprises et notamment des PME. En quelques semaines, il est devenu vital pour nombre d'entrepreneurs, de commerçants, de restaurateurs, de libraires mais aussi de professions libérales de se lancer sur le web pour poursuivre leur activité. La conséquence: une exposition aux attaques des cyberpirates que les PME ne soupçonnaient pas en se lançant dans le grand bain du numérique. Et un fort besoin d'accompagnement pour répondre à ces menaces.

[Lire plus tard](#) [Orange Cyberdefense](#) [Partager](#) [Commenter](#)



Les PME sont plus vulnérables que les grandes entreprises !



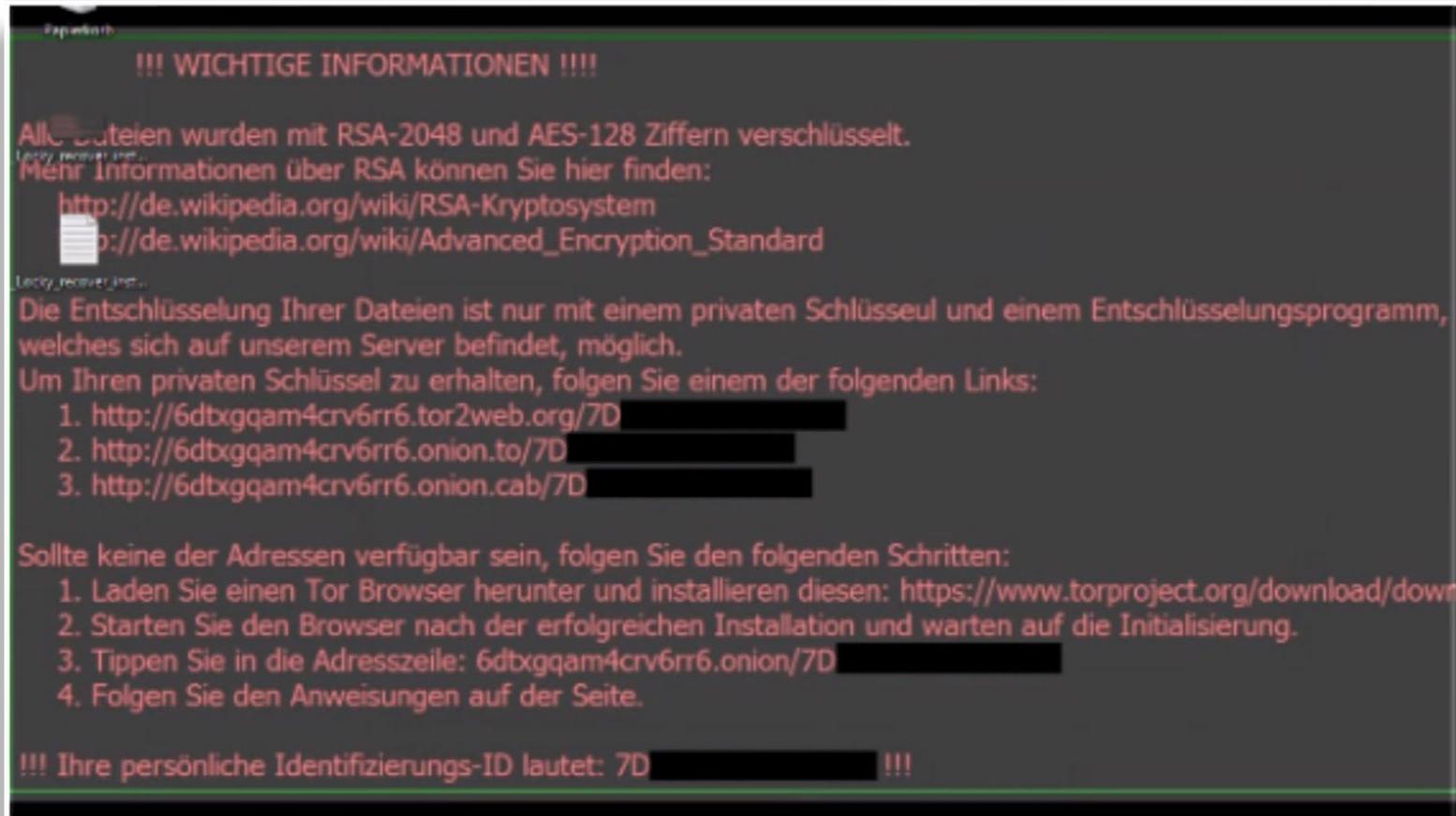
Figure 109. Top 20 threat actions (referencing the 2013 DBIR)

Quelle: Verizon Data Breach Report 2020 (<https://enterprise.verizon.com/resources/reports/dbir/2020/smb-data-breaches-deep-dive/>)

2. Cyber attaques: deux exemples



Rançonlogiciels



Rançonlogiciels : recommandations

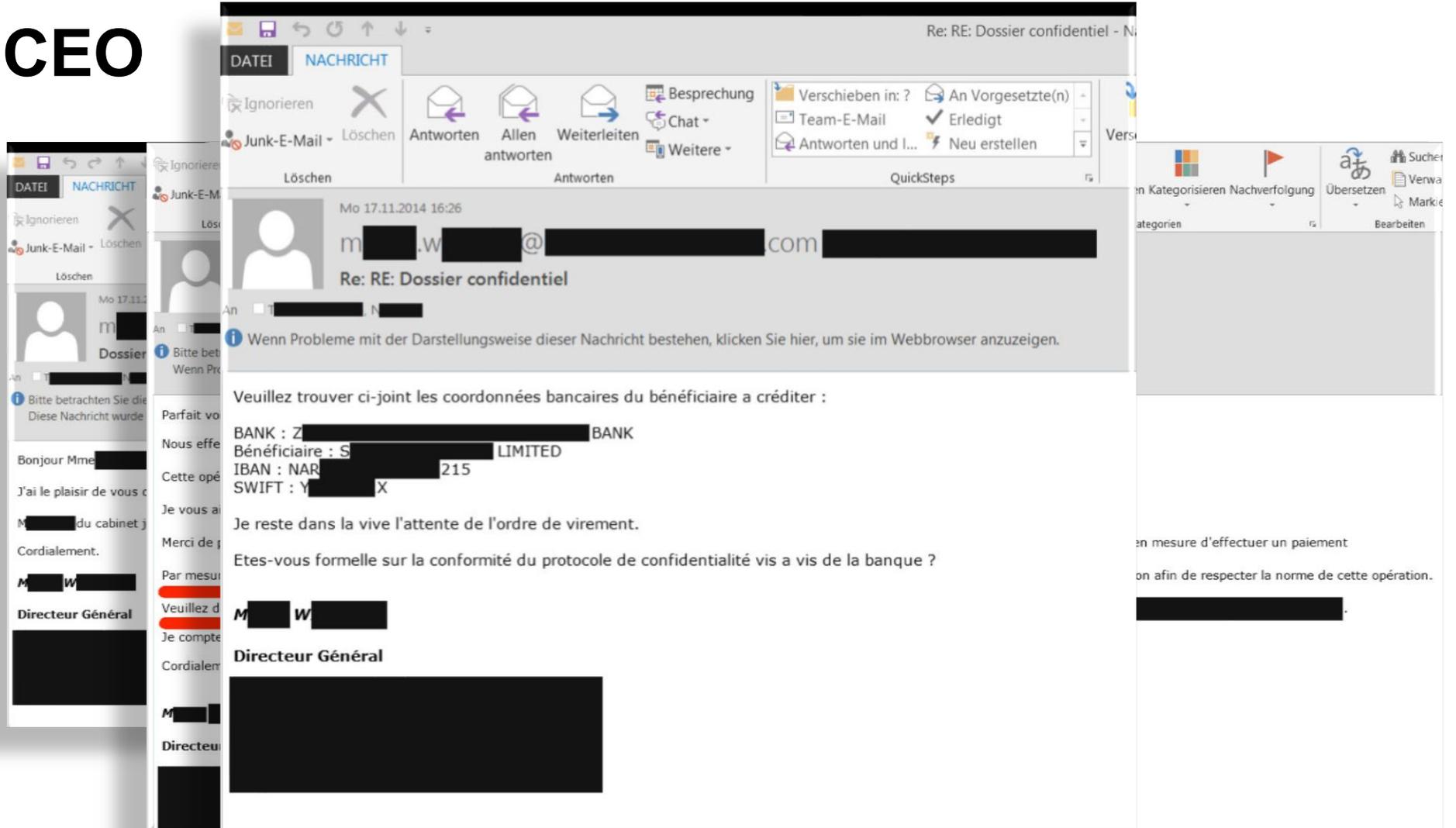


- Sauvegarde régulière des données.
- Déconnexion des disques durs externes du PC / réseau après la sauvegarde.
- Vérifiez sporadiquement la qualité des sauvegardes.
- S'entraîner à importer des sauvegardes pendant une minute de calme.
- Essayez de restaurer les données :
www.nomoreransom.org
- Ne payez pas de rançon !
- Informer le NCSC, si nécessaire déposer une plainte pénale contre des inconnus auprès de la police cantonale.

Fraude à CEO



Fraude à CEO



Re: RE: Dossier confidentiel - N

DATEI NACHRICHT

Ignorieren X

Junk-E-Mail - Löschen

Löschen

Antworten

Allen antworten

Weiterleiten

Besprechung

Chat

Weitere

Verschieben in: ?

An Vorgesetzte(n)

Team-E-Mail

Erledigt

Antworten und I...

Neu erstellen

QuickSteps

Mo 17.11.2014 16:26

m. [REDACTED].w [REDACTED]@ [REDACTED].com [REDACTED]

Re: RE: Dossier confidentiel

An [REDACTED]

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Bitte betrachten Sie die
Diese Nachricht wurde

Parfait vo

Nous effe

Cette opé

Je vous ai

Merci de p

Par mesur

Veillez d

Je compte

Cordialem

M [REDACTED]

Directeu

Veillez trouver ci-joint les coordonnées bancaires du bénéficiaire a créditer :

BANK : Z [REDACTED] BANK

Bénéficiaire : S [REDACTED] LIMITED

IBAN : NAR [REDACTED] 215

SWIFT : Y [REDACTED] X

Je reste dans la vive l'attente de l'ordre de virement.

Etes-vous formelle sur la conformité du protocole de confidentialité vis a vis de la banque ?

M [REDACTED] W [REDACTED]

Directeur Général

M [REDACTED]

Directeu

en mesure d'effectuer un paiement

on afin de respecter la norme de cette opération.

[REDACTED]

Fraude à CEO : recommandations



- Donner des instructions claires concernant les paiements.
- Ne pas transmettre d'informations internes.
- En cas de doute, vérifiez auprès de la direction de l'entreprise.
- Est-il absolument nécessaire de mentionner le nom des employés sur le site web de l'entreprise ?
- Informer le NCSC, si nécessaire déposer une plainte pénale contre des inconnus auprès de la police cantonale.

3. Conclusions / recommmandations



Conclusions

- Les PME sont plus vulnérables que les grandes entreprises
- Le bon sens comme « protection de base »
- Le NCSC sera heureux de vous soutenir en cas de besoin.

Recommandations: proactives

La première habituelle :

Mots de passe forts / changement régulier du mot de passe

Pare-feu (liste noire, etc.)

Mises à jour

Sauvegardes

...

Mais :

Les mesures techniques seules ne suffisent pas !

Envisagez des mesures organisationnelles telles que la gestion de la continuité des activités ou la communication de crise.

Recommandations: réactives

Soutien aux entreprises et aux particuliers :

Centre national de cybersécurité NCSC:

<https://www.report.ncsc.admin.ch/fr/>

Application de la loi :

Les particuliers : Police cantonale du lieu de résidence

Les entreprises : Police cantonale sur le lieu de travail

Merci pour votre attention



Max Klaus
Chef suppléant cybersécurité opérationnelle NCSC

Centre national pour la cybersécurité NCSC
Schwarztorstrasse 59
3003 Berne



Environnement de travail moderne et sûr

Lydie Delon, Swisscom

« **Bonjour** »

123456 1234

123456789

1234578 12345

11111 bonjour

motdepasse

soleil password

Quel mot de passe est-il sûr?



A CorrectChevalBatterieAgrafe

B Tr0ub4dour&3

Les programmes de piratage modernes peuvent identifier les mots connus («troubadour» dans cet exemple) en quelques secondes, même si des lettres ont été remplacées par des caractères spéciaux ou si des caractères supplémentaires ont été ajoutés.

A CorrectChevalBatterieAgrafe

B Tr0ub4dour&3

Mots de passe sûrs



Chaque compte en ligne doit avoir son **propre mot de passe**: les mots de passe constituent la clé d'accès à nos données!



Les mots de passe représentent la **mesure de sécurité la plus puissante** que les utilisateurs maîtrisent eux-mêmes.



Les mots de passe robustes sont: **uniques**

- comportent au moins **12 caractères**
- comportent des chiffres, des lettres majuscules et minuscules, des caractères spéciaux

Les collaborateurs constituent le principal risque en matière de sécurité

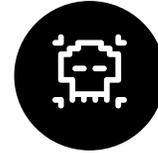
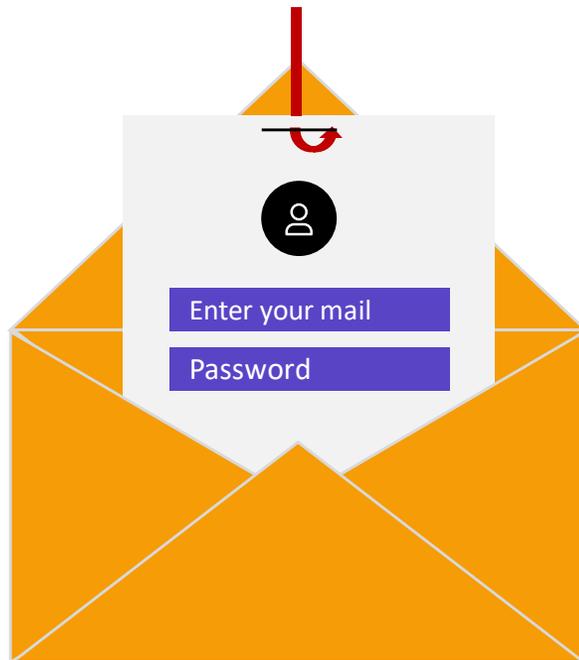


> 90%

de toutes les cyberattaques sont
dus à une erreur humaine

- Stratégies de sécurité
- Limiter les droits des utilisateurs
- Sensibiliser les collaborateurs,
utilisation des e-mails

Identification des e-mails de phishing



Adresse e-mail cryptée



Indication de données personnelles



Pièces jointes suspectes



Invitation à agir sur-le-champ



Le texte du lien et le lien ne correspondent pas



Fautes d'orthographe et langage simple



Adresse du destinataire falsifiée

Von: "homegate.ch" <info@homegate.ch>
Datum: 12. November 2020 um 12:06:23 MEZ
An: IhreAdresse@mail.ch
Betreff: SOFORTIGE ÜBERPRÜFUNG für Ihr Konto erforderlich
Antwort an: noreply@homegates.ch ← Incorrect reply address

↓ Mail with a similar layout to homegate.ch



Als Registrant bei der homegate.ch müssen Sie dem Registrierungsvertrag der homegate.ch zustimmen.

Bitte überprüfen Sie die E-Mail-Adresse des Registranten und stimmen Sie den Bedingungen unserer Registrierungsvereinbarung ausdrücklich zu.

Alle Konten müssen innerhalb des 12/11/2020 überprüft werden. Dies ist die Zeitspanne, in der Ihr Konto gesperrt wird, wenn keine Maßnahmen ergriffen werden.

Klicken Sie auf "Jetzt bestätigen", um Ihr Konto zu bestätigen und der Registrierungsvereinbarung zuzustimmen:

[Jetzt bestätigen](#)

Sie müssen diese E-Mail-Adresse bestätigen und der Registrierungsvereinbarung bis zum oben angegebenen Zeitraum zustimmen. Nach diesem Datum wird das mit diesem Registrierungskontakt verknüpfte Konto gesperrt, bis die E-Mail-Adresse überprüft und die Registrierungsvereinbarung bestätigt wurde.

Freundliche Grüße
Ihr homegate.ch-Team

Services Clients Netflix (info@blacksea-cbc.net)
To: you [Details](#) ▾

tr>

NETFLIX

⚠ Votre compte est suspendu.

Vos informations de paiement doivent être mises à jour

Bonjour,

Nous rencontrons des difficultés avec vos informations de facturation. Nous allons réessayer, mais il est possible que vous deviez mettre à jour vos détails de paiement.

[METTRE LE COMPTE A JOUR](#)

Besoin d'aide ? N'hésitez pas à consulter le [Centre d'aide](#) ou à [nous contacter](#).

L'équipe Netflix



Invitation à agir sur-le-champ

 LinkFire logo

Hi! Clients,

Your iCloud ID has been locked on Monday, January, 4 2021 for security reasons

If you do not respond within 12 hours of this email, your Apple account will be suspended and you will no longer be able to access

[VERIFY ACCOUNT](#)

We apologize for any inconvenience this may have caused you and appreciate your patience with our security measures

Best regards,
Apple Support



Lien apparemment fiable



mer. 15.02.2017 12:43

Swisscom <sme.contactcenter@bill.swisscom.com>

Rechnungskopie

L'expéditeur semble bien être de chez Swisscom

À ■ Thévenaz Dominique

Vous avez transféré ce message le 15.02.2017 13:07.

Cliquez ici pour télécharger des images. Pour protéger la confidentialité, Outlook a empêché le téléchargement automatique de certaines images dans ce message.



Le mail respecte très bien le design corporate de swisscom et imite à s'y méprendre une facture de Swisscom

Sehr geehrte Kundin, sehr geehrter Kunde

Vielen Dank für Ihren Auftrag.

Hiermit erhalten Sie die gewünschten Unterlagen.

Le montant n'est pas arrondi, alors que Swisscom arrondi toujours les montants

CHF 328.42 (zahlbar bis 23.01.2017)

Betroffene Rechnung(en): Januar 2017

https://u4748775.ct.sendgrid.net/wf/click?upn=r32gpj0k4b0ahco9jro2zplamngrej1fmedskmwgtmwmjrn-2fm6a0ghsphms9yfrdr3x1vxazdgartenl6na5-2f8m3-2fscdiar4vgjl-aaucubunsbncmvixrqkon7rfdqgpnlit919iknjqfj6cqosr83rlxb-2f1lw7pk2he5zl-2bvx54hpgwuehqldxaoogqkdjzcd-2bhb1sx0vhffvlb-2fhqgwtv-2bpz4a0bckrpppeg0s9msymeo43i4hsctpi9i3_aohlpqjiahgvbyhms-2b9ujbxe7qvsf1yolrca01dn1dviyezjx0m1vzlgxm9inm0vsvsozpepfizuclduth54vz4b245yc5louxurkmmey9fwgthbza-2bvhplcc6ra1y5pmlcecxwqzdtuv4ewvny9yrrkesvgiify1svmowvx5lakwiniq-2bpy6zlmhh2ob9p2o8jy7xaoezbnklp8vli6efowvktvbu3lnj-2b06i1xda-3d

Cliquez pour suivre le lien

[Rechnung einsehen >](#)

Le lien dirige vers un site douteux! Danger!



Alles Wissenswerte rund um das Thema Rechnung, Verbindungen & aktuelle Kosten finden Sie in Ihrem persönlichen Kundencenter.

Angaben zur papierlosen Bezahlung

Post-Konto: 01-89213-9

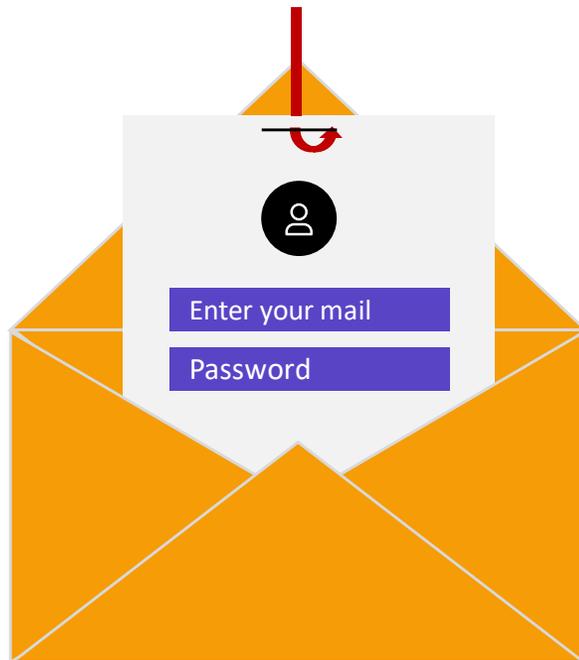
Zugunsten von: Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern

Referenznummer: 744833493827159939732733977

Codierzeile: 0100000455573>744833493827159939732733977+ 010206313>

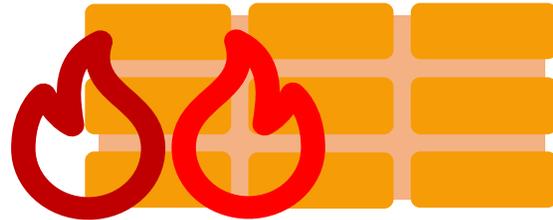
Falls Sie Ihre Zahlung aus dem Ausland tätigen, verwenden Sie bitte folgende Überweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZ80A.

E-mails de phishing: conseils et astuces

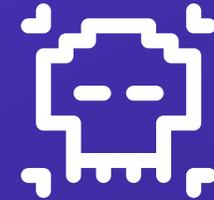


- Ne communiquez **jamais** votre **nom d'utilisateur**, **votre mot de passe** ou des informations détaillées concernant votre adresse par e-mail.
- Méfiez-vous des e-mails contenant des **fautes d'orthographe et de grammaire**.
- Ouvrez les **pièces jointes à un e-mail** uniquement si vous avez **confiance** en l'expéditeur et si vous les **attendiez**.
- Lien «[Cliquez ici](#)» dans un e-mail? Survolez-le avec le pointeur de la souris et découvrez la page vers laquelle il pointe vraiment.

Antivirus + pare-feu = protection totale?



**Nombre de nouveaux
programmes malveillants
chaque jour?**



350 000

**Quels systèmes d'exploitation
utilisez-vous?**



A Windows 7

B Windows 8

C Windows 10

Failles de sécurité à cause de mises à jour manquantes

- 
- **Mettre à jour** les systèmes d'exploitation, les programmes et les applications
 - **Gestion des correctifs et des mises à jour** du matériel et des applications



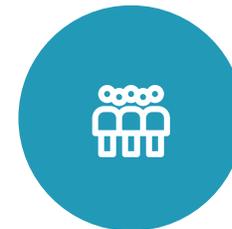
Sécurité du réseau au moyen de la segmentation



Données, processus
et systèmes critiques dans
des réseaux séparés



Séparer le réseau destiné
aux invités



Créer des groupes
d'utilisateurs

La mobilité, risque pour la sécurité



Protéger les
appareils

Un système de sauvegarde qui fonctionne peut sauver votre journée.



Séparer les sauvegardes du système



Plus les sauvegardes sont régulières, mieux c'est.

Checklist relative à la sécurité



Antivirus et
pare-feu



Sécurité du réseau



Systèmes
d'exploitation



Sauvegarde des
données



Sauvegardes



Collaborateurs



Mots de passe



Appareils mobiles



<https://ibarry.ch/>

Outils gratuits

Contrôles de sécurité

Nous vous présentons ci-après quelques outils gratuits qui vous aideront à estimer le niveau de sécurité informatique de vos appareils.

Pour toute question liée au support technique, adressez-vous au fabricant.

Fuite de données

Il arrive très régulièrement que des identifiants et des mots de passe donnant accès à des services en ligne soient volés ou espionnés au moyen de logiciels malveillants. Ces données sont souvent rendues publiques ce qui permet à n'importe qui de les voir. Vous pouvez vérifier à l'aide du site ci-dessous si vos données d'accès figurent dans une base de données piratées et, le cas échéant, savoir depuis quand.

Ce service est mis à disposition par [Have I Been Pwned](#) (en anglais).

Adresse e-mail

Vérifier

Vérification du réseau

La vérification du réseau a pour but :

d'établir si, au cours des derniers jours, l'adresse IP (identification sur internet) de l'accès internet utilisé a tenté une connexion avec un serveur infecté connu. Dans un tel cas, on peut craindre qu'un appareil connecté au réseau concerné ait été infecté.

de veiller à ce qu'aucun service présentant une éventuelle faille de sécurité ne puisse être atteint par le routeur (appareil donnant l'accès à Internet). Une faille de sécurité pourrait être utilisée par un pirate pour prendre le contrôle de l'appareil.

Commencer

Détecteur de logiciels malveillant

Hitman Pro s'utilise en complément d'un antivirus ordinaire. Il détecte et détruit les virus, chevaux de Troie et logiciels malveillants, mais n'est pas prévu pour une utilisation quotidienne. La version d'essai complète est valable 30 jours.

Hitman Pro est mis à disposition par [Sophos](#) (en anglais).

Download Hitman Pro x64

Vérification des logiciels

Les logiciels obsolètes présentent souvent des failles de sécurité qui peuvent être exploitées par les auteurs d'une attaque informatique. Grâce à l'outil de vérification des logiciels, vous pouvez contrôler que votre navigateur web est à jour. Vous avez également l'option d'installer un programme qui vérifie que le système d'exploitation et les logiciels installés sont à jour.

La vérification des logiciels est mise à disposition par [Qualys](#) (en anglais).

Vérification des versions

**Notre solution informatique pour votre garage ! Tout d'un seul tenant.
Nous trouvons votre partenaire personnel.
www.swisscom.ch/garage**



X



**Un solide réseau de
partenaires Swisscom dans
toute la Suisse**



**Notre solution informatique
pour votre garage**

[Vers le configurateur](#)

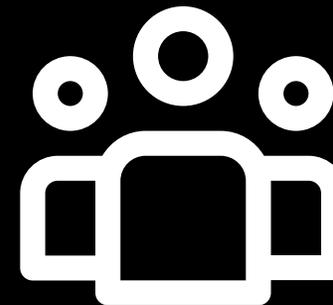
Composez maintenant votre offre individuelle et recevez une offre.

[Télécharger le pack info](#)

Obtenez des informations détaillées sur les TIC intelligentes pour l'industrie automobile.



« **Au revoir** »



Conclusion

Séance d'échange

La formation continue est la route qui nous permet de rouler vers notre avenir

L'offre de formations continues de l'UPSA est certifiée et de haute qualité. Profitez-en !
www.agvs-upsa.ch, Rubrique: Formation/UPSA Business Academy

**Garantissez la
sécurité de votre
informatique!**

