#GE_cybersecurite

Matériel de prévention à la cyber sécurité
Mode d'emploi

Définissez un point de contact unique pour les alertes

Choisissez une personne qui a des affinités avec la cyber sécurité (ressources humaines, informatique, marketing…) qui sera le relai de votre campagne.
Précisez:

- Un numéro de téléphone
- Une adresse e-mail unique de référence.

Procédez simplement

Utilisez le canal de communication habituel et préféré de vos collaborateurs

Adaptez le matériel à votre culture d'entreprise

Le matériel à disposition constitue une proposition de base de travail. Il est prévu pour être adapté pour un plus fort impact au sein de votre organisation.
Astuce :

- Gagnez du temps: utilisez la version une présentation trois thèmes lors d'une unique séance de 1h voire 1h30 maximum
- Simplifiez les actions: Envoyez l'e-mail aux collaborateurs avec en même temps la campagne sur le phishing

Définissez un agenda et un planning clair

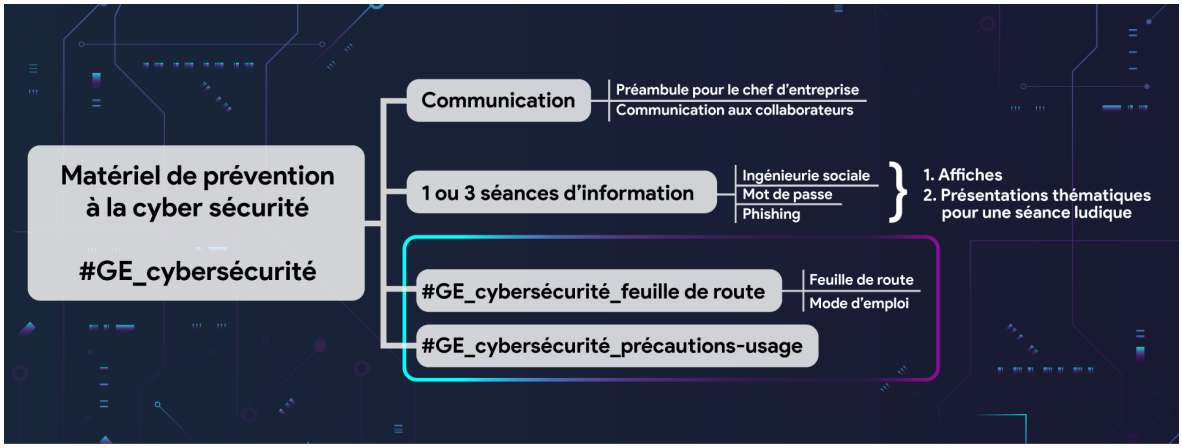
En annexe des documents une feuille de route est à votre disposition pour guider les interventions dans le temps.

Lancer votre campagne de sensibilisation Ouvrez le dialogue

1. Une communication de la direction aux employés (à télécharger un exemple d'email)
2. Campagne avec affiches (à télécharger)
3. Présentations à utiliser lors de vos séances (à télécharger)

Ce matériel va sensibiliser vos collaborateurs aux enjeux et aux risques liés à la cybercriminalité. Pour la réussite de votre communication, leur engagement est nécessaire. Aussi il est important de récolter les témoignages et les idées des collaborateurs.

Cybersécurité: passons à l'action !



Cher(e)s collègues,

Un matin comme les autres dans une entreprise genevoise, Laurence arrive au bureau, allume son ordinateur, ouvre ses emails et clique machinalement sur un message…

La collaboratrice de cette PME genevoise en a fait la malheureuse expérience du hold-up moderne! En 2 clics, en ouvrant une pièce jointe malveillante. Son ordinateur a agi comme une porte d'entrée pour les cyber-criminels et tous les fichiers de l'entreprise ont été chiffrés (sauvegardes incluses). Tout se déroule très vite : demande rançon de 5 bitcoins, pertes de données importantes, plaintes des clients. Un coût de CHF100'000.- pour ce cas réel.

Cela n'arrive qu'aux autres ?
Les cyber criminels sont de plus en plus ingénieux, alors communiquons et apprenons ensemble à repérer ces arnaques qui peuvent coûter très cher!

Nous vous invitons à une séance d'échange et de discussion sur 3 types de cyber-attaques les plus redoutables et mais aussi les plus courantes :

Vous connaissez sûrement ce type d'arnaque sur internet? Vous avez des exemples ?
Engageons le dialogue ensemble et réfléchissons pour :

- Déceler les attaques et repérer la piraterie sur internet
- Acquérir les bons réflexes
- Prévenir et apprendre à (ré)agir le plus rapidement possible

Engageons-nous et agissons pour protéger notre organisation. La cyber criminalité n'est pas une fatalité. Participez à la campagne interne qui aura lieu prochainement avec des affiches dans nos lieux communs et une invitation à une séance interne pour débattre du sujet.

La cyber sécurité est l'affaire de tous ! Je compte sur votre engagement.

Meilleures salutations,

Signature

Précautions d'usage

Le contenu des documents du matériel de prévention – cybersécurité :

- Ne prétend ni être exhaustif, ni précis, ni même suffisamment actualisé pour permettre de prendre une décision dans le domaine juridique ou technique en matière de sécurité.
- Ne peut se substituer aux conseils d'un spécialiste.
- Ne doit pas être considéré comme un ensemble de conseils – qu'ils soient d'ordre juridique ou technique – applicables à une situation concrète.
- Est exclusivement de caractère général et ne tient compte d'aucune spécificité propre à toute situation concrète.
- Ne permet en soi ni de déterminer le niveau de la protection souhaitable, ni d'assurer un niveau de protection donné.

Le matériel de prévention en matière de cybersécurité a été constitué par l'Etat de Genève.
L'Etat de Genève décline toute responsabilité concernant l'application du contenu de ce matériel.

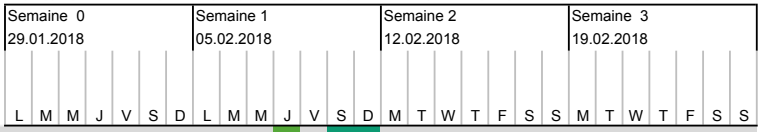
Le matériel de prévention est inspiré et constitué de l'agrégation de multiples sources et ne saurait être exhaustif.

Feuille de route - Campagne de Cybersécurité

[Nom de l'entreprise]
[Logo]

Responsable du projet :
Date de début du projet: 10.02.2018
Date du jour : 08.03.2018

N°	Activité	Responsable	Début	Fin	Durée (jours)	% réalisé	Effort estimé (jours)	Jours consommés	Jours restants
1	**Lancement**	[NOM]	10.02.2018	11.02.2018	2		0		
1.1	Diffusion e-mail teasing	[NOM]	10.02.2018	11.02.2018	2	0%	0	0	2
2	**Mot de Passe fort**	[NOM]	17.02.2018	21.02.2018	5		3		
2.1	Diffusion e-mail	[NOM]	17.02.2018	17.02.2018	1	0%	0	0	1
2.2	Campagne d'affichage	[NOM]	17.02.2018	21.02.2018	5	0%	3	0	5
2.3	Présentation	[NOM]	19.02.2018	19.02.2018	1	0%	1	0	1
3	**Hammeçonnage**	[NOM]	24.02.2018	28.02.2018	5		3		
3.1	Diffusion e-mail	[NOM]	24.02.2018	24.02.2018	1	0%	0	0	1
3.2	Campagne d'affichage	[NOM]	24.02.2018	28.02.2018	5	0%	3	0	5
3.3	Présentation	[NOM]	26.02.2018	26.02.2018	1	0%	1	0	1
4	**Ingénierie sociale**	[NOM]	03.03.2018	07.03.2018	5		3		
4.1	Diffusion e-mail	[NOM]	03.03.2018	03.03.2018	1	0%	0	0	1
4.2	Campagne d'affichage	[NOM]	03.03.2018	07.03.2018	5	0%	3	0	5
4.3	Présentation	[NOM]	05.03.2018	05.03.2018	1	0%	1	0	1



PHISHING : NE MORDEZ PAS À L'HAMEÇON

Le phishing est une arnaque par email utilisée par des cyber criminels pour vous soutirer des informations personnelles

SOYEZ ATTENTIFS AUX STRATAGÈMES SUIVANTS:

- On vous met sous pression en prétendant une urgence immédiate.
- On vous fait miroiter une récompense pour vous pousser à cliquer sur le lien.
- On usurpe l'adresse mail d'un supérieur hiérarchique pour solliciter un virement.
- On vous demande des informations confidentielles ou votre mot de passe.
- On utilise une orthographe et une grammaire douteuses.
- On veut vous faire cliquer sur un lien qui ressemble à celui d'un site web fiable:

www.ge.etat.ch ou www.3tat.ge.ch au lieu de www.ge.ch
www.twiter.com au lieu de www.twitter.com / www.linkdin.com

TRUCS ET ASTUCES:
Si vous passez votre souris au-dessus du lien l'adresse réelle devrait apparaître.

REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

INGÉNIERIE SOCIALE & RÉSEAUX SOCIAUX

Ces attaques exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles pour permettre d'obtenir quelque chose de la personne ciblée (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.).

DÉJOUEZ LES PIÈGES !

C'est une attaque ciblée

- Pour dérober des informations confidentielles.
- Pour introduire des logiciels malveillants.

43% des piratages
=
ingénierie sociale
(Verizon Data Breach Investigations 2016)

QUEL COMPORTEMENT ADOPTER ?

- Soyez discret.
- Challengez votre interlocuteur.
- Soyez vigilant à toute demande inhabituelle.
- Confirmez l'information par un autre canal de communication.
- Vérifiez les liens reçus : passez votre souris dessus avant de cliquer

Activez votre **BON SENS** contre les cyber criminels

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

LE BON MOT DE PASSE

Votre mot de passe un moyen facile, efficace et indispensable pour empêcher les utilisateurs non autorisés d'accéder à vos appareils.

- Au moins 12 caractères.
- Lettres capitales
- Minuscules / majuscules
- Conserver les espaces de frappe (entre les mots)
- Nombres, symboles ***`! "? $?% ^ & * ()_ - + = {[]]:; @ '~ # | \ <,>.? /***

- Votre identifiant ou votre nom d'utilisateur
- Votre nom, le nom de votre ami, le nom de votre famille ou un nom commun
- Un mot du dictionnaire
- Comme vos mots de passe précédents
- Votre date de naissance
- Un modèle de clavier, tel que qwerty, asdfghjkl ou 12345678

3 TECHNIQUES

1. Une ***PHRASE DE PASSE*** plutôt qu'un mot de passe : *J'aime Genève@SWISS.ch*

2. La méthode **phonétique** : « J'ai acheté 5 cd pour cent francs cet après-midi » deviendra ght5CD%F7am

3. La méthode des **premières lettres** : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

Les 2 mots de passe les plus utilisés en 2017

« 123456 »
« password »

REPUBLIQUE ET CANTON DE GENEVE

POST TENEBRAS LUX

PHISHING : NE MORDEZ PAS À L'HAMEÇON

Le phishing est une arnaque par email utilisée par des cyber criminels pour vous soutirer des informations personnelles

SOYEZ ATTENTIFS AUX STRATAGÈMES SUIVANTS:

- On vous met sous pression en prétendant une urgence immédiate.
- On vous fait miroiter une récompense pour vous pousser à cliquer sur le lien.
- On usurpe l'adresse mail d'un supérieur hiérarchique pour solliciter un virement.
- On vous demande des informations confidentielles ou votre mot de passe.
- On utilise une orthographe et une grammaire douteuses.
- On veut vous faire cliquer sur un lien qui ressemble à celui d'un site web fiable:

www.ge.etat.ch ou www.3tat.ge.ch au lieu de www.ge.ch
www.twiter.com au lieu de www.twitter.com / www.linkdin.com

TRUCS ET ASTUCES:
Si vous passez votre souris au-dessus du lien l'adresse réelle devrait apparaître.

REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

INGÉNIERIE SOCIALE & RÉSEAUX SOCIAUX

Ces attaques exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles pour permettre d'obtenir quelque chose de la personne ciblée (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.).

DÉJOUEZ LES PIÈGES !

C'est une attaque ciblée

- Pour dérober des informations confidentielles.
- Pour introduire des logiciels malveillants.

43% des piratages
=
ingénierie sociale
(Verizon Data Breach Investigations 2016)

QUEL COMPORTEMENT ADOPTER ?

- Soyez discret.
- Challengez votre interlocuteur.
- Soyez vigilant à toute demande inhabituelle.
- Confirmez l'information par un autre canal de communication.
- Vérifiez les liens reçus : passez votre souris dessus avant de cliquer

Activez votre **BON SENS** contre les cyber criminels

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

LE BON MOT DE PASSE

Votre mot de passe un moyen facile, efficace et indispensable pour empêcher les utilisateurs non autorisés d'accéder à vos appareils.

- Au moins 12 caractères.
- Lettres capitales
- Minuscules / majuscules
- Conserver les espaces de frappe (entre les mots)
- Nombres, symboles ***`! "? $?% ^ & * ()_ - + = {[]}:; @ '~ # / \ <,>.? /***

- Votre identifiant ou votre nom d'utilisateur
- Votre nom, le nom de votre ami, le nom de votre famille ou un nom commun
- Un mot du dictionnaire
- Comme vos mots de passe précédents
- Votre date de naissance
- Un modèle de clavier, tel que qwerty, asdfghjkl ou 12345678

3 TECHNIQUES

1. Une ***PHRASE DE PASSE*** plutôt qu'un mot de passe : *J'aime Genève@SWISS.ch*

2. La méthode **phonétique** : « J'ai acheté 5 cd pour cent francs cet après-midi » deviendra ght5CD%F7am

3. La méthode des **premières lettres** : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

Les 2 mots de passe les plus utilisés en 2017

« 123456 »
« password »

REPUBLIQUE ET CANTON DE GENEVE

POST TENEBRAS LUX

REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

Ingénierie sociale

Communiquez !

AGENDA

Propos : Sensibilisation à la cybersécurité

Action : Ingénierie sociale

5 astuces pour se protéger
Techniques de cybercriminels
Des cas pour ouvrir la discussion

Le terme d'« **ingénierie sociale** » (en anglais « *social engineering* ») désigne la manière de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part d’une personne par téléphone, courrier électronique, courrier traditionnel ou contact direct.

5 astuces pour se protéger

Astuce 1: Enregistrez vos sites de confiance.
Cela vous évitera de passer par des liens frauduleux.

Astuce 2 : Ne cédez pas à la peur.
Ne vous laissez pas intimider par les menaces.
Nombre de cybercriminels comptent sur l'élément de surprise pour vous amener à faire quelque chose à votre insu.
Repérez et ignorez purement et simplement les tactiques basées sur la peur.

5 astuces pour se protéger

Astuce 3 : Renseignez-vous sur l'identité de votre interlocuteur, demandez des informations précises : nom et prénom, société, numéro de téléphone.
Exigez des précisions sur les attentes de la personne.

Astuce 4 : Ne mentionnez pas sur internet de détails qui vous concernent, vous ou votre entreprise, et qui pourraient renseigner les cybercriminels.

Astuce 5 : Interrogez-vous sur la criticité des informations demandées.

La clé de la réussite

Pour éviter des attaques par ingénierie sociale :

→ communiquez en interne !

Techniques de cybercriminels

Les cybercriminels utilisent souvent des e-mails, des messageries instantanées ou des SMS pour diffuser les messages malveillants.

Ils persuaderont la victime de révéler des informations directement ou de réaliser une action comme :

- entrer dans un faux site Web (promotion saisonnière et exceptionnelle, etc…)
- cliquer sur un lien de téléchargement malveillant (s'annonçant comme représentant de Microsoft par exemple)
- transmettre des informations sensibles et confidentielles (arnaque au Président)

→ ce qui permet au criminel de poursuivre son plan malintentionné.

Techniques de cybercriminels

Cas pratique : l’arnaque au Président

La « fraude au **président** » est une escroquerie. Elle consiste pour des escrocs à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision sur un contrat, etc…

Le comportement à adopter

- Instaurez des **procédures de vérification sécurisées** pour les paiements internationaux.
- Utilisez de manière **prudente les réseaux sociaux** → ne divulguez pas trop d’informations.
- **Saisissez vous-même l'adresse du donneur d'ordre**, lorsqu'il s'agit d'effectuer un virement international.
- Accentuez la vigilance sur les **périodes de vacances, les jours fériés.**
- Contactez directement le donneur d’ordre afin de vérifier qu’il est bien à l’origine de la demande.
- Sensibilisez régulièrement les employés des services comptable, trésorerie, secrétariat, standard, etc.
- En cas d'attaque, alertez immédiatement votre hiérarchie ainsi que les autorités.
- Un dépôt de plainte rapide, en apportant un maximum d'éléments, permet d'optimiser les chances de récupérer les fonds volés.
- **Demandez immédiatement à votre banque le retour des fonds** qui ont pu être envoyés.

Et maintenant, repérons les arnaques ensemble !

Des cas pour ouvrir la discussion

Cas 1 :

En se faisant passer pour un technicien (par ex. d'une compagnie téléphonique, d'une centrale électrique, etc.), une personne essaye d'obtenir l'accès à votre habitation ou au sein de votre entreprise.

Vous recevez un courriel vous demandant de cliquer sur un lien hypertexte vous invitant à ouvrir une session en saisissant votre identifiant et votre mot de passe, ou à révéler des informations personnelles.

Des cas pour ouvrir la discussion

Cas 2 :

Une personne vous appelle au téléphone dans le cadre d'un sondage et vous pose une série de questions, concernant par exemple vos revenus, les mesures de sécurité informatique adoptées, etc.).

Cas 3 :

Un escroc falsifie son adresse email et se fait passer pour une personne connue, et vous envoie par exemple un virus en pièce jointe.

Cas 4 :

Un pseudo-informaticien se présente sur votre lieu de travail, soi-disant pour effectuer des travaux d'entretien sur votre PC.

REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

Ingénierie sociale

Faites preuve de bon sens.
Contre les cybercriminels,
le meilleur rempart
c'est VOUS !

REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

Phishing

Ne mordez pas à l'hameçon

AGENDA

Propos : Sensibilisation à la cyber sécurité

Action : Phishing

Késako?

Le jeu des 4 erreurs

Face à la sophistication des cyberattaques
et des techniques utilisées par les cybercriminels,
les entreprises doivent agir sans attendre
pour contrer les tentatives d’intrusion.

Définition du hameçonnage

Le **hameçonnage**, ***phishing*** ou **filoutage** est la technique la plus courante parmi les cyberattaques liées à l'ingénierie sociale. Les fraudeurs tentent d'obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration, etc.) afin de lui soutirer des renseignements personnels :

→ mot de passe, numéro de carte de crédit, date de naissance, etc.

Les méthodes utilisées

- Pièce jointe infectée
- Lien vers un site malicieux
- Faux système de paiement

Identifiez les messages frauduleux à temps

Posez-vous les bonnes questions :

Le message contient-il un lien inhabituel ?

Le domaine de l'adresse email vous semble-t-il étrange ? ex. info@f0ldse.ch

Le message est-il inapproprié et inattendu ?

- Une livraison non prévue, message d’une banque dont vous n’êtes pas client
- Une invitation à télécharger un document ou à compléter des données confidentielles
- Le message contient des fautes d’orthographes, le langage vous surprend

Identifiez les messages frauduleux à temps

Ne tombez pas dans le piège :

Envoi de faux messages tellement **convaincants** que vous ouvrez la pièce attachée

Urgence ultime, il faut répondre de suite sous peine de…

Promesses d'une **importante récompense** si vous effectuez une action en fournissant vos données personnelles → c'est trop beau pour être vrai ! Il y a de fortes chances que ce soit faux, non?!

Identifiez les messages frauduleux à temps

L’adresse web ressemble à celle d’un site légitime, mais elle est subtilement différente :

www.ge.etat.ch ou www.3tat.ge.ch au lieu de www.ge.ch

www.twiter.com au lieu de www.twitter.com

www.linkdin.com au lieu de www.linkedin.com

Et maintenant, passez à l'action!

Le jeu des 4 erreurs

Comment ne pas se faire piéger?

Da: UBS [mailto:info@sumaciudadana.org]
Inviato: domenica, 4. ottobre 2015 16:29
A: [redacted]
Oggetto: [C5C2] MasterCard Issue

PHISHING

Ma BanQue

Sehr geehrter Kunde / Sehr geehrte Kundin,

Unsere Sicherheitsabteilung hat ungewöhnliche Aktivitäten in Verbindung mit ihrerer Kreditkarte festgestellt. Laut unseren Geschäftbedingungen, sowie um sicher zu gehen das Ihre Karte nicht von unberechtigten Dritten verwendet wurde, haben wir Ihren Zugriff zu ihrem Kundenkonto eingeschränkt.

Um Ihr Kundenkonto wieder zu aktivieren, klicken Sie bitte hier.

Wir nahmen Ihre Sicherheit sehr ernst, weswegen wir stehts bemüht sind unsere Betrugserkennung auf dem aktuellsten Stand zu halten, und Ihrre Kundendetails mit einem sicheren Verifikationsprozess zu überprüfen.

Vielen Dank für Ihr Verständnis.

Cher client,

Nous nous adressons à vous avec un message que notre département de la sécurité a identifié une certaine activité inhabituelle de votre carte de crédit. Conformément à nos Conditions générales de l'Accord et afin d'assurer la sécurité de votre carte à l'égard de fraude, l'accès à votre compte a été limité.

S'il vous plaît, cliquez ici pour confirmer votre compte dès que possible.

Nous avons une approche approfondie a la question de votre sécurité en ligne, donc nous utilisons des systèmes modernes d'avertissement pour détecter toute activité suspecte et vérifiez vos données.

Merci pour votre aide.

Gentile cliente,

Il nostro sistema di sicurezza ha trovato attività sospetta con la sua carta, per protegere il suo conto lo abbiamo limitato temporaneamente, secondo le nostre condizioni d'utilizzo in questo momento abbiamo bisogno del suo intervento.

Clicca qui per sbloccare il suo conto

L'online banking non è solo semplice e pratico, ma anche sicuro. Aiutateci a garantirvi la massima sicurezza possibile, semplicemente osservando alcune importanti regole di comportamento.

Cordiali Saluti.

Comment ne pas se faire piéger?

1

Est-ce que je connais cette personne?
Son email ne correspond pas pas une adresse de Ma Banque ?

Da: UBS [mailto:info@sumaciudadana.org]
Inviato: domenica, 4. ottobre 2015 16:29
A: [redacted]
Oggetto: [C5C2] MasterCard Issue

PHISHING

Ma BanQue

Sehr geehrter Kunde / Sehr geehrte Kundin,

Unsere Sicherheitsabteilung hat ungewöhnliche Aktivitäten in Verbindung mit ihrerer Kreditkarte festgestellt. Laut unseren Geschäftbedingungen, sowie um sicher zu gehen das Ihre Karte nicht von unberechtigten Dritten verwendet wurde, haben wir Ihren Zugriff zu ihrem Kundenkonto eingeschränkt.

Um Ihr Kundenkonto wieder zu aktivieren, klicken Sie bitte hier.

Wir nehmen Ihre Sicherheit sehr ernst, weswegen wir stehts bemüht sind unsere Betrugserkennung auf dem aktuellsten Stand zu halten, und Ihrre Kundendetails mit einem sicheren Verifikationsprozess zu überprüfen.

Vielen Dank für Ihr Verständnis.

Cher client,

Nous nous adressons à vous avec un message que notre département de la sécurité a identifié une certaine activité inhabituelle de votre carte de crédit. Conformément à nos Conditions générales de l'Accord et afin d'assurer la sécurité de votre carte à l'égard de fraude, l'accès à votre compte a été limité.

S'il vous plaît, cliquez ici pour confirmer votre compte dès que possible.

Nous avons une approche approfondie a la question de votre sécurité en ligne, donc nous utilisons des systèmes modernes d'avertissement pour détecter toute activité suspecte et vérifiez vos données.

Merci pour votre aide.

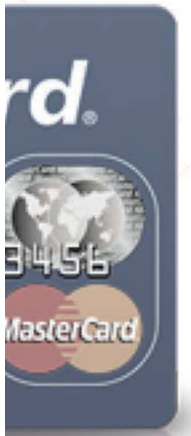
Gentile cliente,

Il nostro sistema di sicurezza ha trovato attività sospetta con la sua carta, per protegere il suo conto lo abbiamo limitato temporaneamente, secondo le nostre condizioni d'utilizzo in questo momento abbiamo bisogno del suo intervento.

Clicca qui per sbloccare il suo conto

L'online banking non è solo semplice e pratico, ma anche sicuro. Aiutateci a garantirvi la massima sicurezza possibile, semplicemente osservando alcune importanti regole di comportamento.

Cordiali Saluti.



Comment ne pas se faire piéger?

1

Est-ce que je connais cette personne?
Son email ne correspond pas pas une adresse Ma Banque ?

2

Un email <u>non</u> nominatif provenant de Ma Banque ?

Da: UBS [mailto:info@sumaciudadana.org]
Inviato: domenica, 4. ottobre 2015 16:29
A: [redacted]
Oggetto: [C5C2] MasterCard Issue

PHISHING

Ma BanQue

Sehr geehrter Kunde / Sehr geehrte Kundin,

Unsere Sicherheitsabteilung hat ungewöhnliche Aktivitäten in Verbindung mit ihrerer Kreditkarte festgestellt. Laut unseren Geschäftbedingungen, sowie um sicher zu gehen das Ihre Karte nicht von unberechtigten Dritten verwendet wurde, haben wir Ihren Zugriff zu ihrem Kundenkonto eingeschränkt.

Um Ihr Kundenkonto wieder zu aktivieren, klicken Sie bitte hier.

Wir nehmen Ihre Sicherheit sehr ernst, weswegen wir stehts bemüht sind unsere Betrugserkennung auf dem aktuellsten Stand zu halten, und Ihrre Kundendetäls mit einem sicheren Verifikationsprozess zu überprüfen.

Vielen Dank für Ihr Verständnis.

Cher client,

Nous nous adressons à vous avec un message que notre département de la sécurité a identifié une certaine activité inhabituelle de votre carte de crédit. Conformément à nos Conditions générales de l'Accord et afin d'assurer la sécurité de votre carte à l'égard de fraude, l'accès à votre compte a été limité.

S'il vous plaît, cliquez ici pour confirmer votre compte dès que possible.

Nous avons une approche approfondie a la question de votre sécurité en ligne, donc nous utilisons des systèmes modernes d'avertissement pour détecter toute activité suspecte et vérifiez vos données.

Merci pour votre aide.

Gentile cliente,

Il nostro sistema di sicurezza ha trovato attività sospetta con la sua carta, per protegere il suo conto lo abbiamo limitato temporaneamente, secondo le nostre condizioni d'utilizzo in questo momento abbiamo bisogno del suo intervento.

Clicca qui per sbloccare il suo conto

L'online banking non è solo semplice e pratico, ma anche sicuro. Aiutateci a garantirvi la massima sicurezza possibile, semplicemente osservando alcune importanti regole di comportamento.

Cordiali Saluti.

Comment ne pas se faire piéger?

1

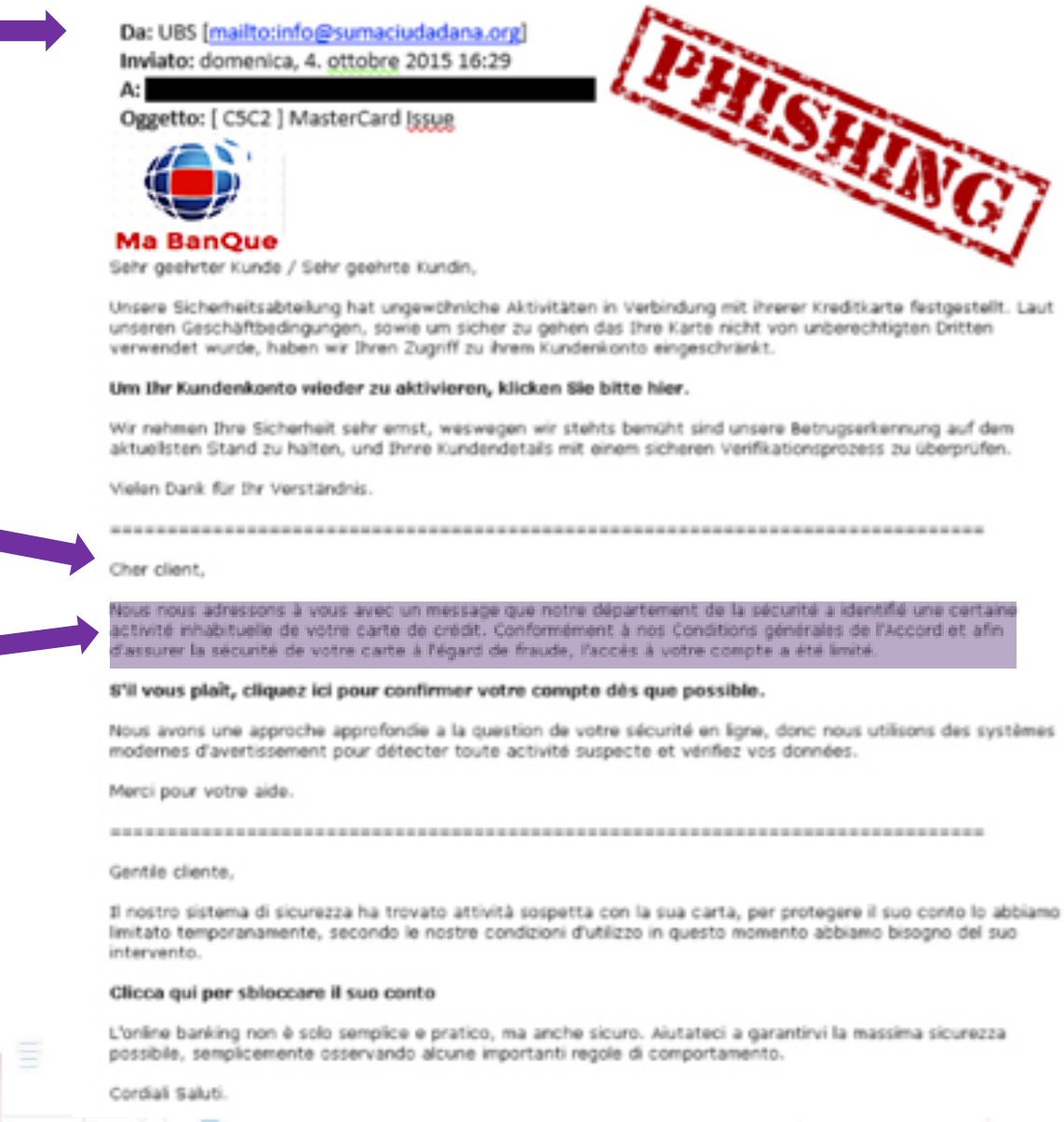
Est-ce que je connais cette personne?
Son email ne correspond pas pas une adresse de Ma Banque?

2

Un email non nominatif provenant de ma banque ?

3

Pourquoi mon compte a été bloqué plutôt que la transaction?



Da: UBS [mailto:info@sumaciudadana.org]
Inviato: domenica, 4. ottobre 2015 16:29
A: [redacted]
Oggetto: [C5C2] MasterCard Issue

PHISHING

Ma BanQue

Sehr geehrter Kunde / Sehr geehrte Kundin,

Unsere Sicherheitsabteilung hat ungewöhnliche Aktivitäten in Verbindung mit ihrerer Kreditkarte festgestellt. Laut unseren Geschäftbedingungen, sowie um sicher zu gehen das Ihre Karte nicht von unberechtigten Dritten verwendet wurde, haben wir Ihren Zugriff zu ihrem Kundenkonto eingeschränkt.

Um Ihr Kundenkonto wieder zu aktivieren, klicken Sie bitte hier.

Wir nehmen Ihre Sicherheit sehr ernst, weswegen wir stehts bemüht sind unsere Betrugserkennung auf dem aktuellsten Stand zu halten, und Ihrre Kundendetails mit einem sicheren Verifikationsprozess zu überprüfen.

Vielen Dank für Ihr Verständnis.

Cher client,

Nous nous adressons à vous avec un message que notre département de la sécurité a identifié une certaine activité inhabituelle de votre carte de crédit. Conformément à nos Conditions générales de l'Accord et afin d'assurer la sécurité de votre carte à l'égard de fraude, l'accès à votre compte a été limité.

S'il vous plaît, cliquez ici pour confirmer votre compte dès que possible.

Nous avons une approche approfondie a la question de votre sécurité en ligne, donc nous utilisons des systèmes modernes d'avertissement pour détecter toute activité suspecte et vérifiez vos données.

Merci pour votre aide.

Gentile cliente,

Il nostro sistema di sicurezza ha trovato attività sospetta con la sua carta, per protegere il suo conto lo abbiamo limitato temporaneamente, secondo le nostre condizioni d'utilizzo in questo momento abbiamo bisogno del suo intervento.

Clicca qui per sbloccare il suo conto

L'online banking non è solo semplice e pratico, ma anche sicuro. Aiutateci a garantirvi la massima sicurezza possibile, semplicemente osservando alcune importanti regole di comportamento.

Cordiali Saluti.

Comment ne pas se faire piéger?

1

Est-ce que je connais cette personne?
Son email ne correspond pas pas une adresse Ma Banque ?

2

Un email non nominatif provenant de ma banque ?

3

Pourquoi mon compte a été bloqué plutôt que la transaction?

4

Bizarre ce lien….

Da: UBS [mailto:info@sumaciudadana.org]
Inviato: domenica, 4. ottobre 2015 16:29
A: [redacted]
Oggetto: [C5C2] MasterCard Issue

PHISHING

Ma BanQue

Sehr geehrter Kunde / Sehr geehrte Kundin,

Unsere Sicherheitsabteilung hat ungewöhnliche Aktivitäten in Verbindung mit ihrerer Kreditkarte festgestellt. Laut unseren Geschäftbedingungen, sowie um sicher zu gehen das Ihre Karte nicht von unberechtigten Dritten verwendet wurde, haben wir Ihren Zugriff zu ihrem Kundenkonto eingeschränkt.

Um Ihr Kundenkonto wieder zu aktivieren, klicken Sie bitte hier.

Wir nehmen Ihre Sicherheit sehr ernst, weswegen wir stehts bemüht sind unsere Betrugserkennung auf dem aktuellsten Stand zu halten, und Ihrre Kundendetails mit einem sicheren Verifikationsprozess zu überprüfen.

Vielen Dank für Ihr Verständnis.

Cher client,

Nous nous adressons à vous avec un message que notre département de la sécurité a identifié une certaine activité inhabituelle de votre carte de crédit. Conformément à nos Conditions générales de l'Accord et afin d'assurer la sécurité de votre carte à l'égard de fraude, l'accès à votre compte a été limité.

S'il vous plaît, cliquez ici pour confirmer votre compte dès que possible.

Nous avons une approche approfondie a la question de votre sécurité en ligne, donc nous utilisons des systèmes modernes d'avertissement pour détecter toute activité suspecte et vérifiez vos données.

Merci pour votre aide.

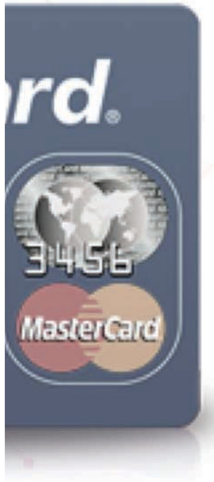
Gentile cliente,

Il nostro sistema di sicurezza ha trovato attività sospetta con la sua carta, per protegere il suo conto lo abbiamo limitato temporaneamente, secondo le nostre condizioni d'utilizzo in questo momento abbiamo bisogno del suo intervento.

Clicca qui per sbloccare il suo conto

L'online banking non è solo semplice e pratico, ma anche sicuro. Aiutateci a garantirvi la massima sicurezza possibile, semplicemente osservando alcune importanti regole di comportamento.

Cordiali Saluti.



Comment ne pas se faire piéger?

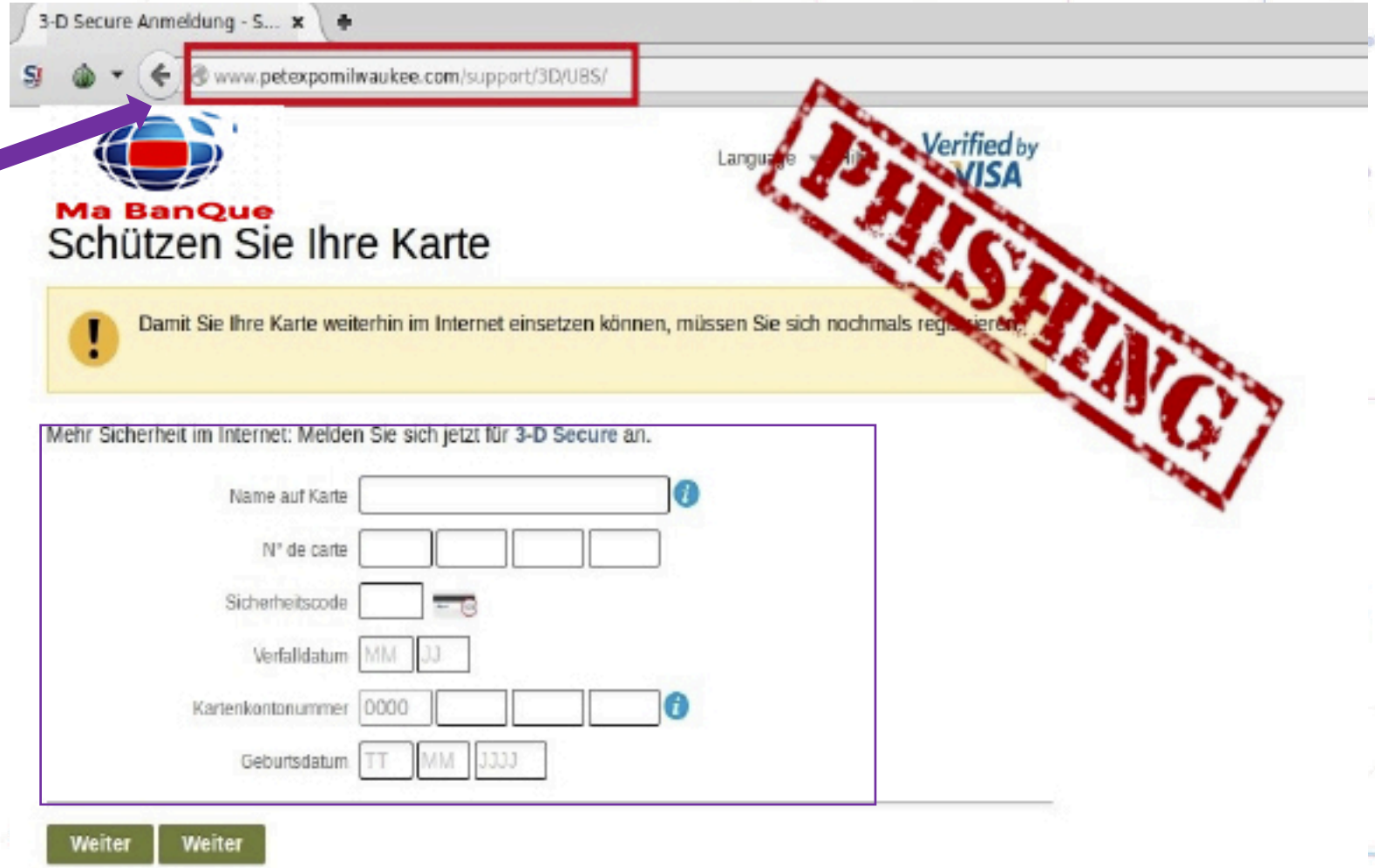
1

Encore une URL étrange

2

Il est demandé d'inscrire nos informations bancaire pour confirmer notre identité?

Une question secrète devrait suffire….



Comment ne pas se faire piéger?

Avec l'aimable accord de Swisscom
pour la prévention en cyber sécurité

Von: Swisscom [mailto:sme.contactcenter@bill.swisscom.com]
Gesendet: Mittwoch, 15. Februar 2017 12:31
An:
Betreff: Rechnungskopie

swisscom

Sehr geehrte Kundin, sehr geehrter Kunde
Vielen Dank fur Ihren Auftrag.
Hiermit erhalten Sie die gewunschten Unterlagen.

CHF 863.43 (zahlbar bis 24.01.2017) Rechnung einsehen ›

Betroffene Rechnung(en): Januar 2017

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

Angaben zur papierlosen Bezahlung

Post-Konto:	01-38395-9
Zugunsten von:	Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern
Referenznummer:	788608635814519370390643231
Codierzeile:	010000549394>788608635814519370390643231+ 010218415>

Falls Sie Ihre Zahlung aus dem **Ausland** tatigen, verwenden Sie bitte folgende Uberweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A.
Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Mochten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich fur die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer Webseite.
Freundliche Grusse
Ihr Swisscom Team

Comment ne pas se faire piéger?

Avec l'aimable accord de Swisscom
pour la prévention en cyber sécurité

1

**Bizarre ce mail…
swisscom.com?**

Von: Swisscom [mailto:sme.contactcenter@bill.swisscom.com]
Gesendet: [illegible]5. Februar 2017 12:31
An: [illegible]
Betreff: Rechnungskopie

swisscom

Sehr geehrte Kundin, sehr geehrter Kunde
Vielen Dank fur Ihren Auftrag.
Hiermit erhalten Sie die gewunschten Unterlagen.

CHF 863.43 (zahlbar bis 24.01.2017) Rechnung einsehen >

Betroffene Rechnung(en): Januar 2017

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

Angaben zur papierlosen Bezahlung

Post-Konto:	01-38395-9
Zugunsten von:	Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern
Referenznummer:	788608635814519370390643231
Codierzeile:	0100000549394>788608635814519370390643231+ 010218415>

Falls Sie Ihre Zahlung aus dem **Ausland** tatigen, verwenden Sie bitte folgende Uberweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A.
Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Mochten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich fur die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer Webseite.
Freundliche Grusse
Ihr Swisscom Team

Comment ne pas se faire piéger?

Avec l'aimable accord de Swisscom
pour la prévention en cyber sécurité

1

Bizarre ce mail…
swisscom.com?

2

email non nominatif?

Von: Swisscom [mailto:sme.contactcenter@bill.swisscom.com]
Gesendet: Mittwoch, 15. Februar 2017 12:31
An:
Betreff: Rechnungskopie

swisscom

Sehr geehrte Kundin, sehr geehrter Kunde
Vielen Dank fur Ihren Auftrag.
Hiermit erhalten Sie die gewunschten Unterlagen.

CHF 863.43 (zahlbar bis 24.01.2017) Rechnung einsehen

Betroffene Rechnung(en): Januar 2017

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

Angaben zur papierlosen Bezahlung

Post-Konto:	01-38395-9
Zugunsten von:	Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern
Referenznummer:	788608635814519370390643231
Codierzeile:	0100000549394>788608635814519370390643231+ 010218415>

Falls Sie Ihre Zahlung aus dem **Ausland** tatigen, verwenden Sie bitte folgende Uberweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A.
Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Mochten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich fur die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer Webseite.
Freundliche Grusse
Ihr Swisscom Team

Comment ne pas se faire piéger?

Avec l'aimable accord de Swisscom
pour la prévention en cyber sécurité

1

Bizarre ce mail… swisscom.com?

2

email non nominatif?

3

Un montant qui n'est pas exact?

Von: Swisscom [mailto:sme.contactcenter@bill.swisscom.com]
Gesen Mittwoch, 15. Februar 2017 12:31
An:
Betreff: Rechnungskopie

swisscom

Sehr geehrte Kundin, sehr geehrter Kunde
Vielen Dank fur Ihren Auftrag.
Hiermit erhalten Sie die gewunschten Unterlagen.

CHF 863.43 (zahlbar bis 24.01.2017) Rechnung einsehen >

Betroffene Rechnung(en): Januar 2017

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

Angaben zur papierlosen Bezahlung

Post-Konto:	01-38395-9
Zugunsten von:	Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern
Referenznummer:	788608635814519370390643231
Codierzeile:	0100000549394>788608635814519370390643231+ 010218415>

Falls Sie Ihre Zahlung aus dem **Ausland** tatigen, verwenden Sie bitte folgende Uberweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A.
Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Mochten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich fur die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer Webseite.
Freundliche Grusse
Ihr Swisscom Team

Comment ne pas se faire piéger?

Avec l'aimable accord de Swisscom
pour la prévention en cyber sécurité

1

Bizarre ce mail… swisscom.com?

2

email non nominatif?

3

Un montant qui n'est pas exact?

4

Un lien dans un email…?

Von: Swisscom [mailto:sme.contactcenter@bill.swisscom.com]
Gesend Mittwoch, 15. Februar 2017 12:31
An:
Betreff: Rechnungskopie

swisscom

Sehr geehrte Kundin, sehr geehrter Kunde
Vielen Dank fur Ihren Auftrag.
Hiermit erhalten Sie die gewunschten Unterlagen.

CHF 863.43 (zahlbar bis 24.01.2017) Rechnung einsehen >

Betroffene Rechnung(en): Januar 2017

Alles Wissenswerte rund um d[illegible]hema Rechnung, Verbindungen & aktuelle Kosten finden [illegible] Ihrem personlichen Kundencenter.

Ang[illegible]en zur papierlosen Bezahlung

Post-Konto:	01-38395-9
Zugunsten von:	Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern
Referenznummer:	788608635814519370390643231
Codierzeile:	0100000549394>788608635814519370390643231+ 010218415>

Falls Sie Ihre Zahlung aus dem **Ausland** tatigen, verwenden Sie bitte folgende Uberweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A.
Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Mochten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich fur die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer Webseite.
Freundliche Grusse
Ihr Swisscom Team

REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

Phishing

Soyez prudent et vigilant…
Contre les cybercriminels,
le meilleur rempart
c’est VOUS !

REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

Mots de passe

Apprenez à composer

AGENDA

Propos : Sensibilisation à la cyber sécurité

Action : Mots de passe

5 astuces pour déjouer les tactiques des cybercriminels

Les techniques pour retenir ses mots de passe

Vos mots de passe sont des moyens faciles, efficaces et indispensables pour empêcher les utilisateurs non autorisés d'accéder à vos appareils.

Alors utilisez-les !

5 astuces

Astuce 1: Assurez-vous d'activer la protection par mot de passe

Astuce 2 : Changez tous les mots de passe par défaut

L'une des erreurs les plus courantes est de ne pas modifier les mots de passe par défaut des fabricants pour les smartphones, ordinateurs portables et autres types d'équipements.

Les bonnes pratiques : 5 astuces

Astuce 3 : Évitez d'utiliser des mots de passe prévisibles

Test : assurez-vous que quelqu'un qui vous connaît bien ne peut pas **deviner votre mot de passe en 20 tentatives**.

Astuce 4 : Utilisez l'authentification à deux facteurs pour les comptes 'importants'
Cela peut être un code envoyé à votre smartphone (ou un code généré à partir du lecteur de carte d'une banque) que vous devez entrer en plus de votre mot de passe.

5 astuces

Astuce 5 : Faites face à la «surcharge de mot de passe»

Envisagez d'utiliser des **gestionnaires de mots de passe**, qui sont des outils permettant de créer et de stocker pour vous des mots de passe auxquels vous accédez via un mot de passe «maître».

Puisque le mot de passe principal protège tous vos autres mots de passe, **assurez-vous qu'il soit robuste.**

Déjouez les tactiques des cybercriminels

1. Utilisez un mot de passe suffisamment long

La capacité des hackers à pirater un mot de passe dépend d'abord de sa longueur.

Les logiciels qu'ils utilisent testent automatiquement toutes les combinaisons possibles. Chaque caractère supplémentaire augmente considérablement le temps nécessaire à « craquer » un mot de passe.

Une chaîne de 8 à 12 caractères est un bon compromis entre sécurité et facilité de mémorisation.

Déjouez les tactiques des cybercriminels

2. Privilégiez un mot de passe utilisant une diversité de caractères

Les logiciels des pirates sont programmés pour tester
tous les mots du dictionnaire // une grande quantité de prénoms // toutes les dates du calendrier

Le bon mot de passe :
au moins 12 caractères + lettres capitales + minuscules / majuscules +conserver les espaces de frappe + nombres, symboles `! "? $?% ^ & * () _ - + = {[}]:; @ '~ # | \ <,>.? /

3. Choisissez un mot de passe unique

Chaque site web/abonnement utilisé par l'internaute doit avoir une clef d'accès différente.

Et maintenant, passez à l'action!

Les techniques pour retenir les mots de passe

Comment construire un mot de passe robuste

15 minutes // 3 techniques

1. Une ***PHRASE DE PASSE*** plutôt qu'un mot de passe

J’aime Genève@SWISS.ch

J’aime Genève:) & son jet d’eau#1207

Conseils pour renforcer votre mot de passe

La robustesse de votre mot de passe peut être améliorée en appliquant les conseils suivants :

- ✓ Eviter de choisir un nombre compris entre 1950 et 2049
- ✓ Ajouter une ponctuation ou un caractère spécial (dollar, dièse, ...)
- ✓ Utiliser un émoticône pour remplacer le mot correspondant, comme remplacer le mot "sourire" par :-)

A vous de jouer, inventez votre phrase!

Comment construire un mot de passe robuste

2. La méthode phonétique

« J’ai acheté 5 cd pour cent francs cet après-midi » deviendra

ght5CD%F7am

A vous de jouer, inventez votre mot de passe!

Comment construire un mot de passe robuste

3. La méthode des premières lettres

La citation « un tien vaut mieux que deux tu l'auras » donnera

1tvmQ2tl'A.

La phrase de passe «J'aime Genève:) & son jet d'eau#1207» devient

JG:)&sjd'e120

Pour retrouver votre mot de passe :

- ✓ Mémoriser la phrase choisie avec les majuscules, les nombres et la ponctuation.
- ✓ Prendre les premières lettres de chaque mot, garder les nombres et la ponctuation.

A vous de jouer, inventez votre mot de passe!

REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

Mots de Passe

Soyez créatifs !
Contre les cybercriminels,
le meilleur rempart
c'est VOUS !