Reconnaître et se protéger des menaces informatiques

Prof. Sylvain Pasini

Responsable du pôle de compétences Y-Security, HEIG-VD

Seniors et technologies:
s'entraider pour s'approprier les outils digitaux
4 décembre 2024

Agenda

1. Introduction et contexte
2. Etat actuel de la menace
3. Modes opératoires des cybercriminels
4. Bonnes pratiques pour se protéger


2014
Photography by dougthomsen.tv
Engineering by Anton Georgiev


2014
Photography by dougthomsen.tv
Engineering by Anton Georgiev

https://thedigitaltransformation.org/industry-4-0-empowering-machines/


https://www.stratum-ics.com/solution.php

https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-b

Le « cyber » change la criminalité

Le « cyber » change la criminalité

- **Opportunités** en augmentation
  - Actions à travers la planète
  - Accessibilité des cibles

Le « cyber » change la criminalité

- **Opportunités** en augmentation
  - Actions à travers la planète
  - Accessibilité des cibles
- **Techniques** en évolution rapide
  - Outils accessibles (kits en libre accès sur Internet)
  - Données accessibles en masse (données personnelles, vols, fuites, etc.)
  - Attaques à grande échelle, automatisation, attaques en masses
  - Fracture technologique entre criminels et victimes

Le « cyber » change la criminalité

- **Opportunités** en augmentation
  - Actions à travers la planète
  - Accessibilité des cibles
- **Techniques** en évolution rapide
  - Outils accessibles (kits en libre accès sur Internet)
  - Données accessibles en masse (données personnelles, vols, fuites, etc.)
  - Attaques à grande échelle, automatisation, attaques en masses
  - Fracture technologique entre criminels et victimes
- **Avantages** des criminels
  - Blanchiment par crypto-monnaies
  - Anonymat total (réseau Internet / Tor)
  - Obstacles juridiques, enquêtes et poursuites internationales

Le « cyber » change la criminalité

- **Opportunités** en augmentation
  - Actions à travers la planète
  - Accessibilité des cibles
- **Techniques** en évolution rapide
  - Outils accessibles (kits en libre accès sur Internet)
  - Données accessibles en masse (données personnelles, vols, fuites, etc.)
  - Attaques à grande échelle, automatisation, attaques en masses
  - Fracture technologique entre criminels et victimes
- **Avantages** des criminels
  - Blanchiment par crypto-monnaies
  - Anonymat total (réseau Internet / Tor)
  - Obstacles juridiques, enquêtes et poursuites internationales
- Cercle vicieux :
  les **profits** colossaux permettent aux criminels de s'améliorer

Que relatent les chiffres ?

Vaud 2023

Nombre de plaintes « cyber » déposées

4’361

Préjudice total

CHF 26’724’228.-

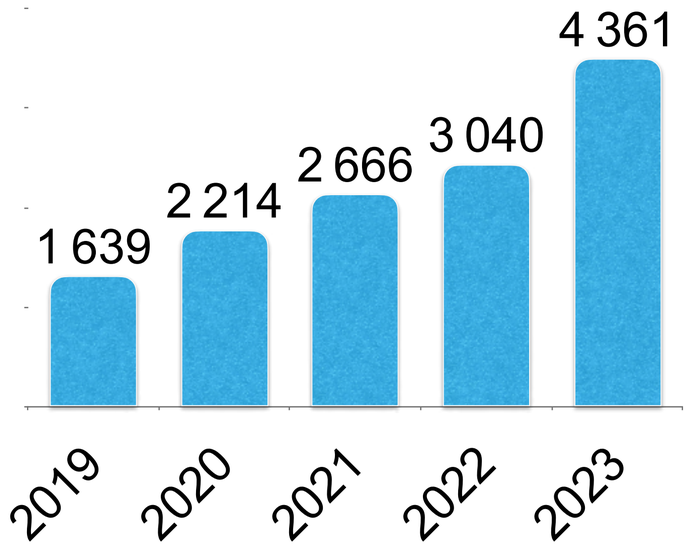
Source : Police Cantonale Vaudoise

Que relatent les chiffres ?

Vaud 2023

Nombre de plaintes « cyber » déposées

4’361



Préjudice total

CHF 26’724’228.-

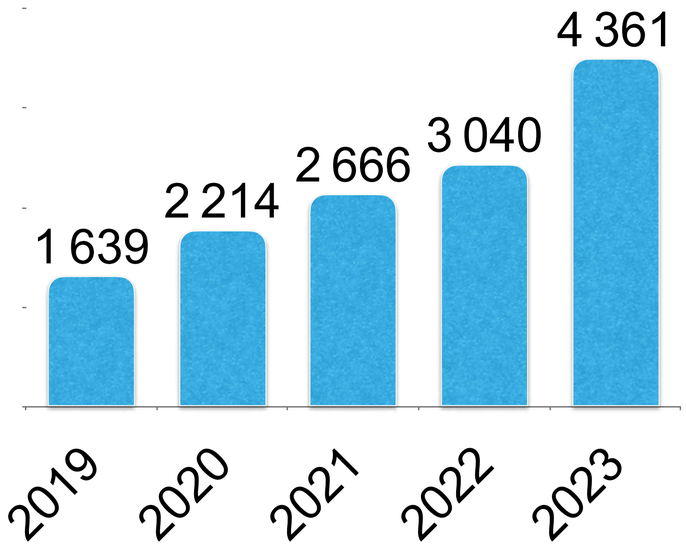
Source : Police Cantonale Vaudoise

Que relatent les chiffres ?

Vaud 2023

Nombre de plaintes « cyber » déposées

4’361

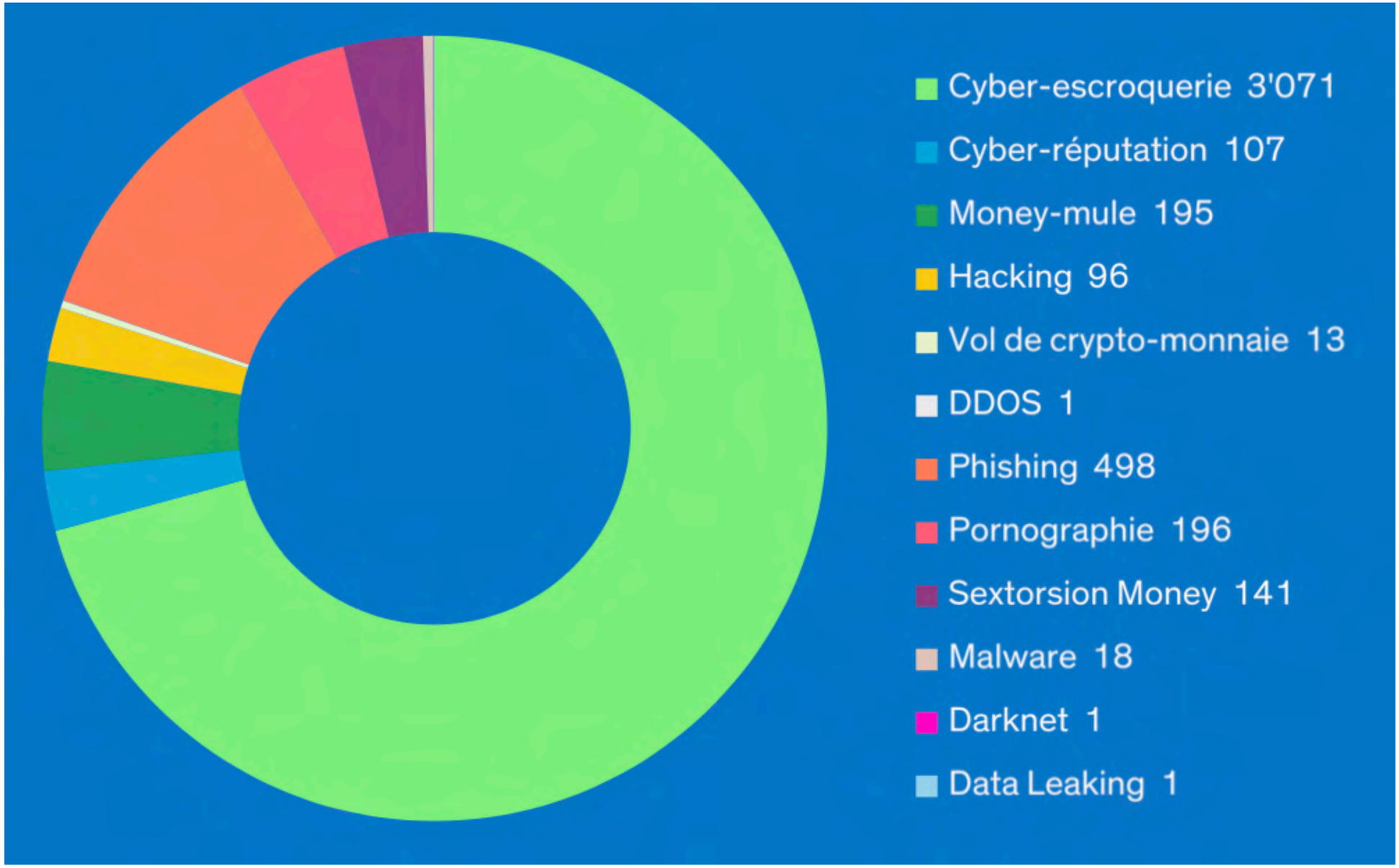


Préjudice total

CHF 26’724’228.-

- Seul **10%** des incidents annoncés
- Préjudice estimé à **CHF 200’000’000.-**

Source : Police Cantonale Vaudoise



Source : Police Cantonale Vaudoise

Moyenne de 125’000.- par cas

Source : Police Cantonale Vaudoise

Chiffres en résumé

- **Augmentation** de presque 50% entre 2022 et 2023
- Préjudice total estimé à 200 millions de CHF (sur Vaud)
- En termes de **nombres** de plaintes :
  - 75% sont de cyber-escroqueries
- En terme de **préjudice**
  - 90% est dû aux cyber-escroqueries
  - 50% est causé par les fraudes à l'investissement, soit 100 millions CHF !

La population des Seniors plus visée ?

- Oui et non

- Certains phénomènes touchent **certaines populations** :
  - Âge : enfants, ados, actifs, seniors,
  - Activité : privés, industriels, retraités
  - Genre : célibataires, veufs, homme, femme

Facteurs spécifiques aux Seniors

- **Confiance** naturelle, remets moins en question
- Instinct **protecteur** et désir d'aider les proches

- Situation **financière**
  - besoins d'économies
  - trop à l'aise

- Moins à l'aise avec les **technologies**, notamment la cybersécurité
- Équipements **obsolètes**

Tendances actuelles adressées les Seniors

Tendances actuelles adressées les Seniors

- Exploitations **humaines** :
  - Abus de confiance, tromperies, phishing

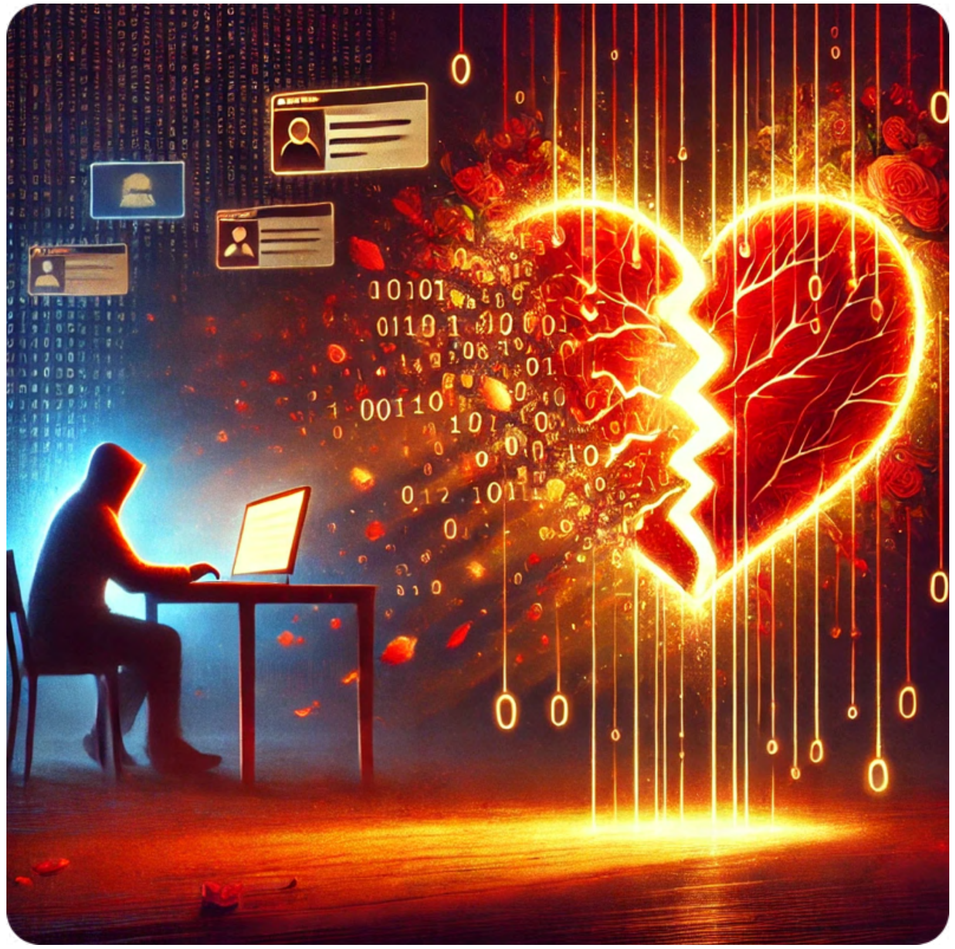
Tendances actuelles adressées les Seniors

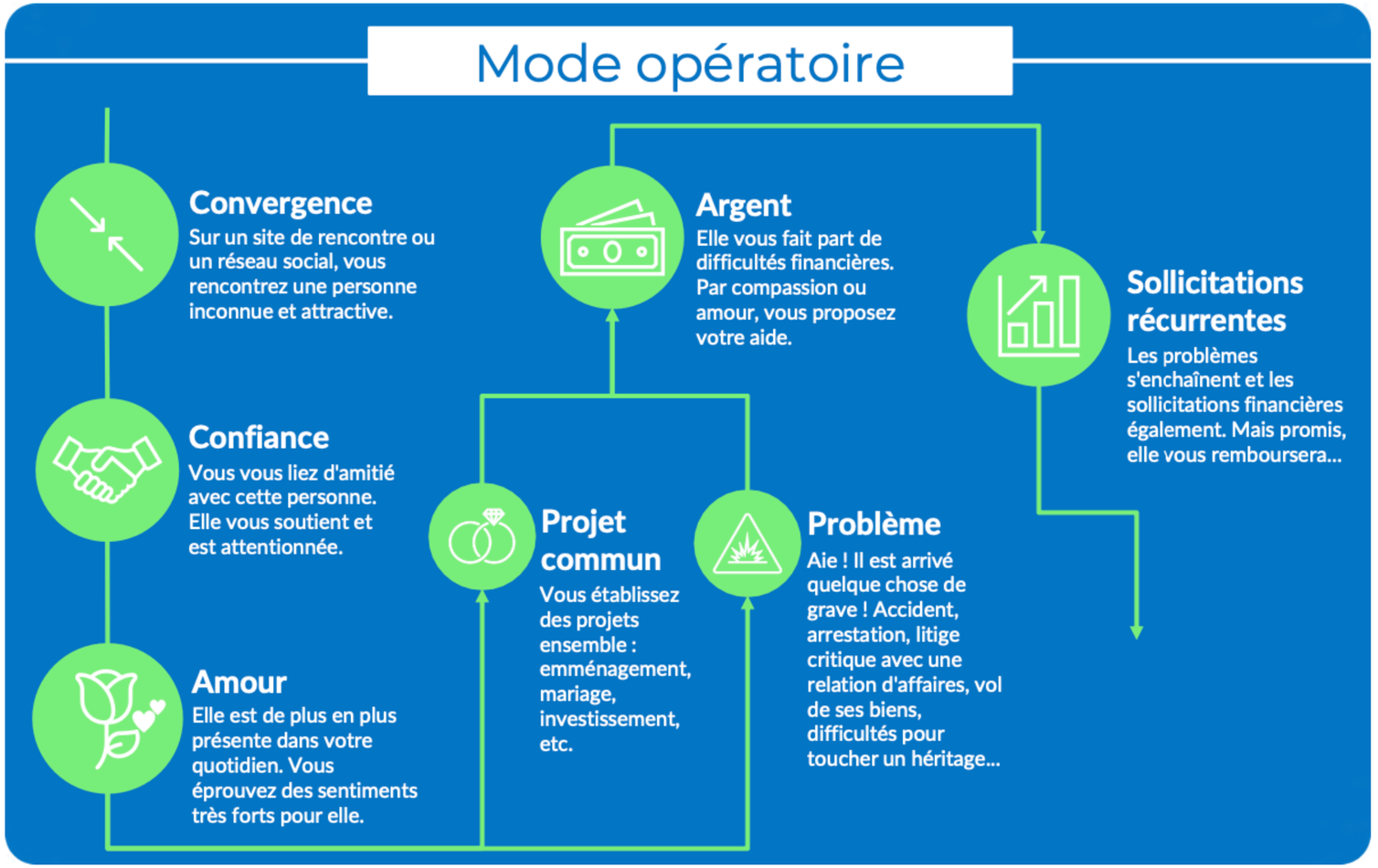
- Exploitations **humaines** :
  - Abus de confiance, tromperies, phishing
- Exploitations **techniques** :
  - Virus et malwares

Tendances actuelles adressées les Seniors

- Exploitations **humaines** :
  - Abus de confiance, tromperies, phishing
- Exploitations **techniques** :
  - Virus et malwares
- **Modes opératoires** courants :
  - Fraude à l'**investissement**, loteries, gains fictifs
  - **Romance scams**, faux neveu, faux petit-enfant
  - **Faux supports techniques**
  - Escroqueries administratives, faux banquier/policier
  - Fausses **annonces**
  - Cyber-**extorsion** : ransomware, sextorsion, etc.

Arnaque aux sentiments





Source : Police Cantonale Vaudoise

Fraude à l'investissement

Mode opératoire

Hameçonnage
Par téléphone, via un site Internet ou une publicité ciblée, les réseaux sociaux ou les applications de rencontre, les auteurs vous proposent un investissement très rentable.

Confiance
Les auteurs vous mettent en confiance en utilisant le jargon financier approprié.

Investissement initial
Vous investissez une première somme, souvent d'un petit montant, pour essayer.

Ça marche !
Vous constatez que votre premier investissement fonctionne. Les auteurs vous pressent à investir plus.

Élément déclencheur
Vous souhaitez récupérer les fonds que vous avez gagné. Malheureusement les auteurs vous expliquent que ce n'est pas possible.

Sollicitations récurrentes
Les auteurs vous poussent à investir d'autres fonds pour récupérer vos premiers investissements mais vous ne récupèrerez jamais un sous.

Source : Police Cantonale Vaudoise

Faux support technique

Mode opératoire

Appel
L'escroc vous appelle directement par téléphone.

Blocage
Votre navigateur est bloqué par une fenêtre d'alerte vous demandant de contacter un numéro au plus vite.

Support
Votre interlocuteur vous rassure en affirmant être un technicien en mesure de vous aider.

Virus
Il vous indique qu'il peut nettoyer et protéger immédiatement votre ordinateur.

Transactions frauduleuses
Pour payer la prestation, vous devez fournir vos informations de carte de crédit ou vous connecter à votre e-banking. Des transactions sont effectuées à votre insu.

Prise de contrôle
L'escroc pourrait vous faire installer un programme de contrôle de votre ordinateur à distance (TeamViewer, Anydesk, Splashtop...)

Source : Police Cantonale Vaudoise

Faux acheteur

Mode opératoire

Vente
Vous publiez une annonce sur un site de petites annonces ou réseau social.
Un acheteur potentiel vous contacte.

Avance de frais
Il vous propose de mandater une entreprise de transport (DHL, ExpedEasy, DPD, etc.) pour récupérer la marchandise chez vous.
Celle-ci vous demande de payer pour débloquer la livraison.

Cartes cadeaux
Vous débourserez probablement plus que la valeur de votre marchandise, généralement en cartes cadeaux, sans jamais être remboursé.

Vol de données
Pour recevoir l'argent de l'acheteur :
- Vous devez remplir vos données de carte de crédit dans un formulaire en ligne.
- Vous êtes contacté par un service financier tiers vous demandant vos accès e-banking, de scanner un code QR ou d'insérer des codes dans votre application Twint.

Transactions frauduleuses
Des paiements seront faits avec votre carte de crédit ou depuis votre compte bancaire ou compte Twint à votre insu.

Source : Police Cantonale Vaudoise

Bonnes pratiques

Bonnes pratiques

- **Jamais se fier** à une personne que vous ne connaissez que par Internet
  - N’envoyez pas d’argent
- Ne **pas faire confiance**, reconnaître des signes de fraude Exemples : faux cousin

Bonnes pratiques

- **Jamais se fier** à une personne que vous ne connaissez que par Internet
  - N’envoyez pas d’argent
- Ne **pas faire confiance**, reconnaître des signes de fraude Exemples : faux cousin
- Ne pas cliquer, vérifier les **liens**

Bonnes pratiques

- **Jamais se fier** à une personne que vous ne connaissez que par Internet
  - N’envoyez pas d’argent
- Ne **pas faire confiance**, reconnaître des signes de fraude Exemples : faux cousin
- Ne pas cliquer, vérifier les **liens**
- **Cohérence** de la demande ?
  - Trop beau pour être vrai ? Exemples : sentiments, prix bas, gain/loto, investissement
  - Pourquoi l’interlocuteur aurait besoins d’informations personnelles ? Exemples : PIN, mots de passe

Bonnes pratiques

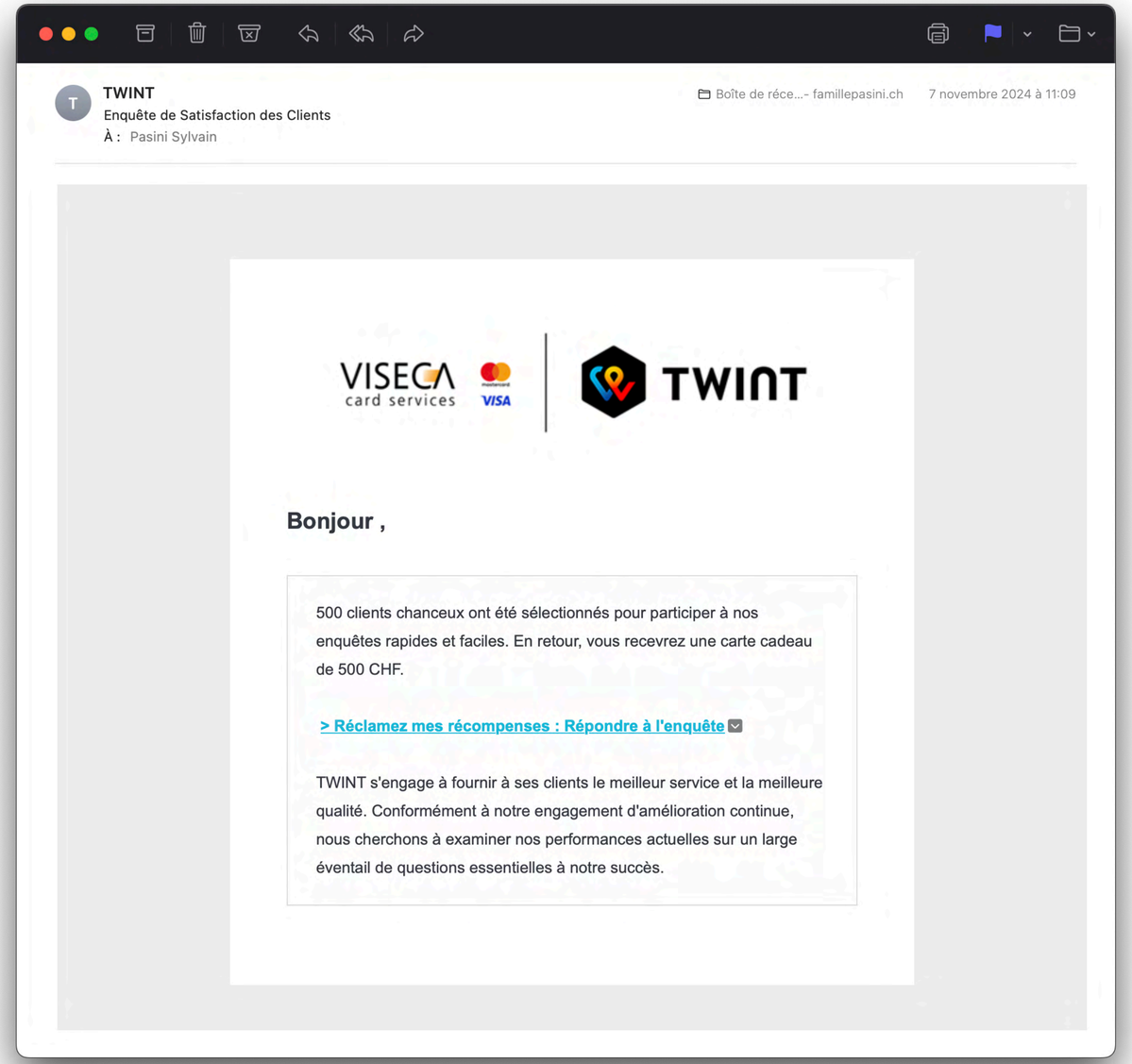
- **Jamais se fier** à une personne que vous ne connaissez que par Internet
  - N'envoyez pas d'argent
- Ne **pas faire confiance**, reconnaître des signes de fraude Exemples : faux cousin
- Ne pas cliquer, vérifier les **liens**
- **Cohérence** de la demande ?
  - Trop beau pour être vrai ? Exemples : sentiments, prix bas, gain/loto, investissement
  - Pourquoi l'interlocuteur aurait besoins d'informations personnelles ? Exemples : PIN, mots de passe
- Gestion des **mots de passe**
  - Complexité
  - Utilisation unique (penser aux vols : phishing, direct, bases de données serveur)
  - Utilisation d'un gestionnaire
  - Authentification à deux facteurs

Bonnes pratiques

- **Jamais se fier** à une personne que vous ne connaissez que par Internet
  - N'envoyez pas d'argent
- Ne **pas faire confiance**, reconnaître des signes de fraude Exemples : faux cousin
- Ne pas cliquer, vérifier les **liens**
- **Cohérence** de la demande ?
  - Trop beau pour être vrai ? Exemples : sentiments, prix bas, gain/loto, investissement
  - Pourquoi l'interlocuteur aurait besoins d'informations personnelles ? Exemples : PIN, mots de passe
- Gestion des **mots de passe**
  - Complexité
  - Utilisation unique (penser aux vols : phishing, direct, bases de données serveur)
  - Utilisation d'un gestionnaire
  - Authentification à deux facteurs
- **Mettre à jour** -> correctifs de sécurité

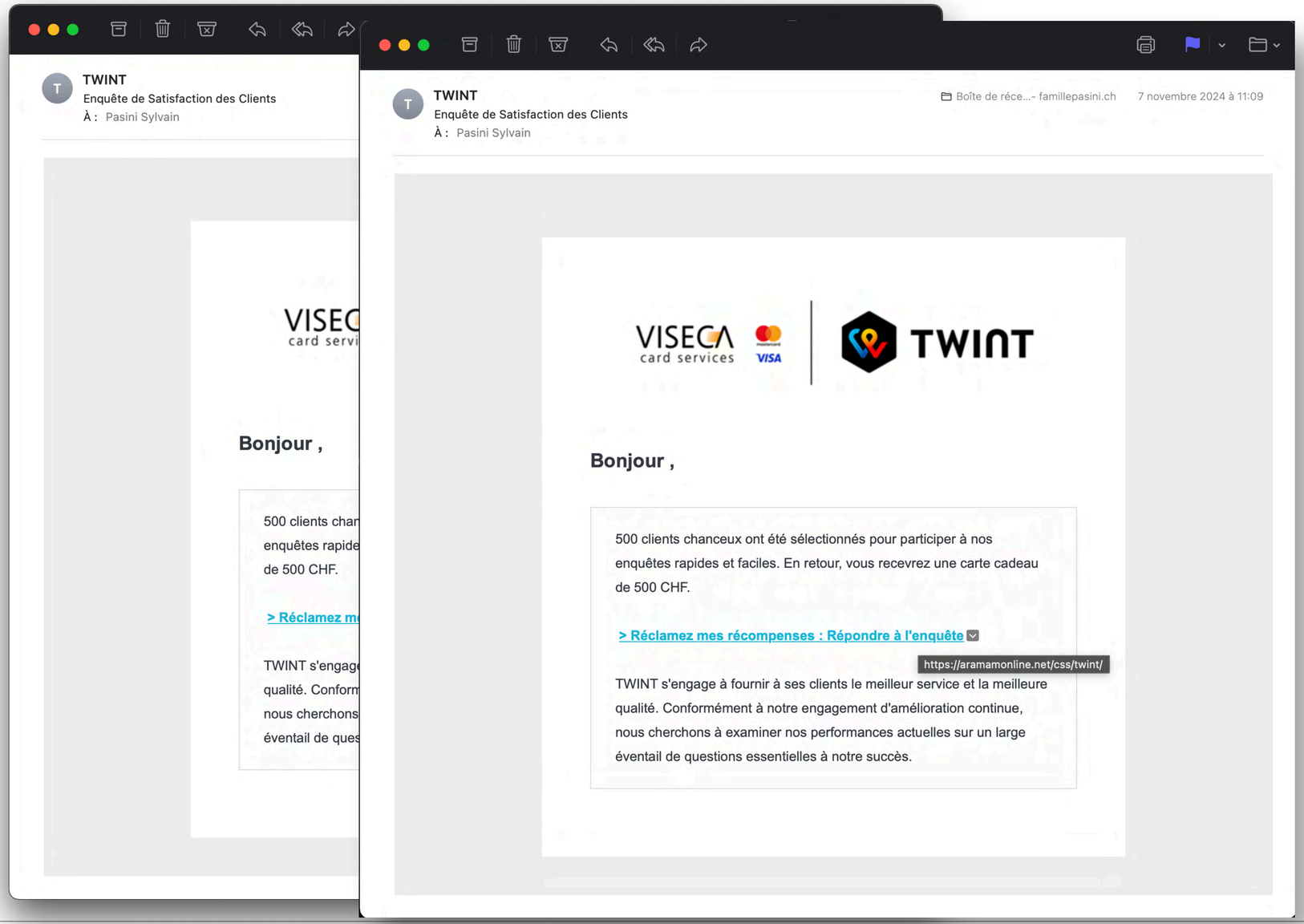
Reconnaître un « phishing »

- L’objectif :
  - Voler vos identifiants



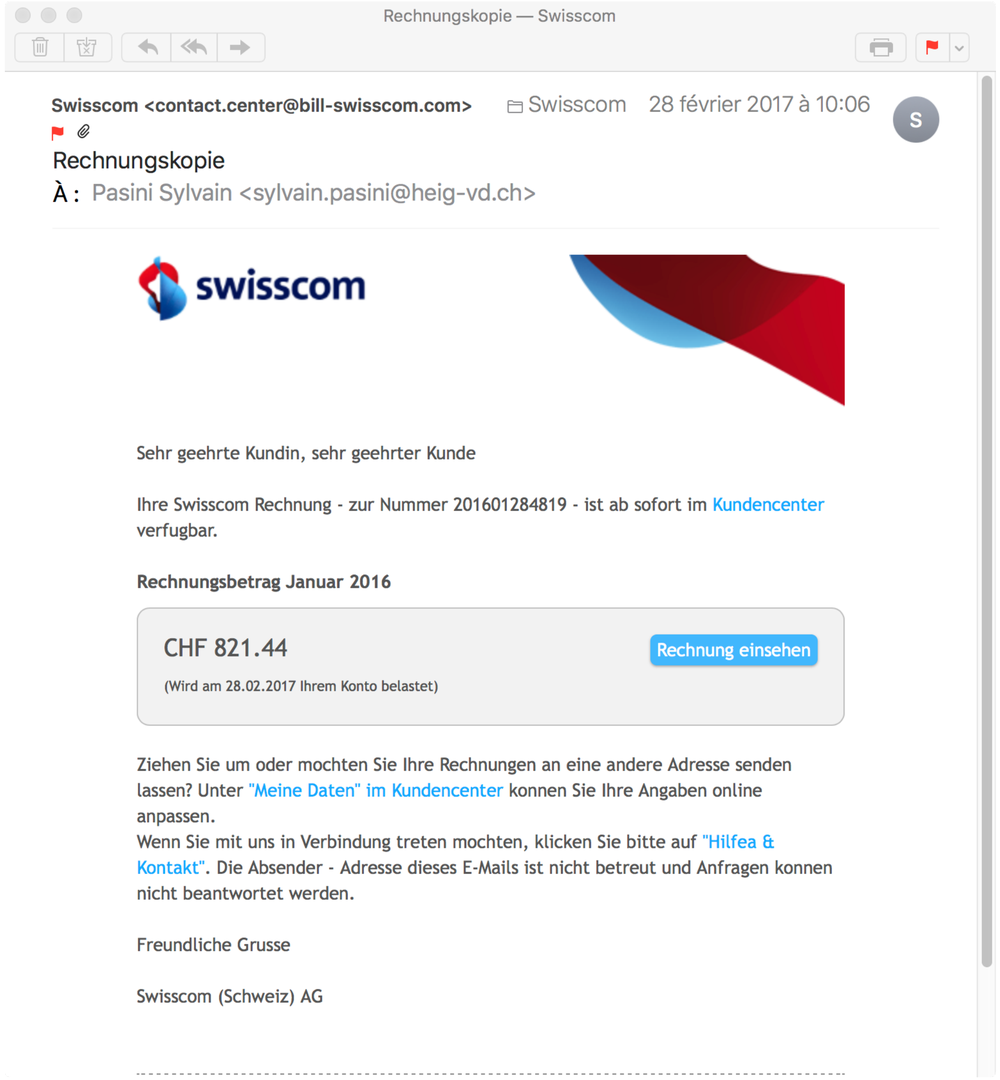
Reconnaître un « phishing »

- L’objectif :
  - Voler vos identifiants



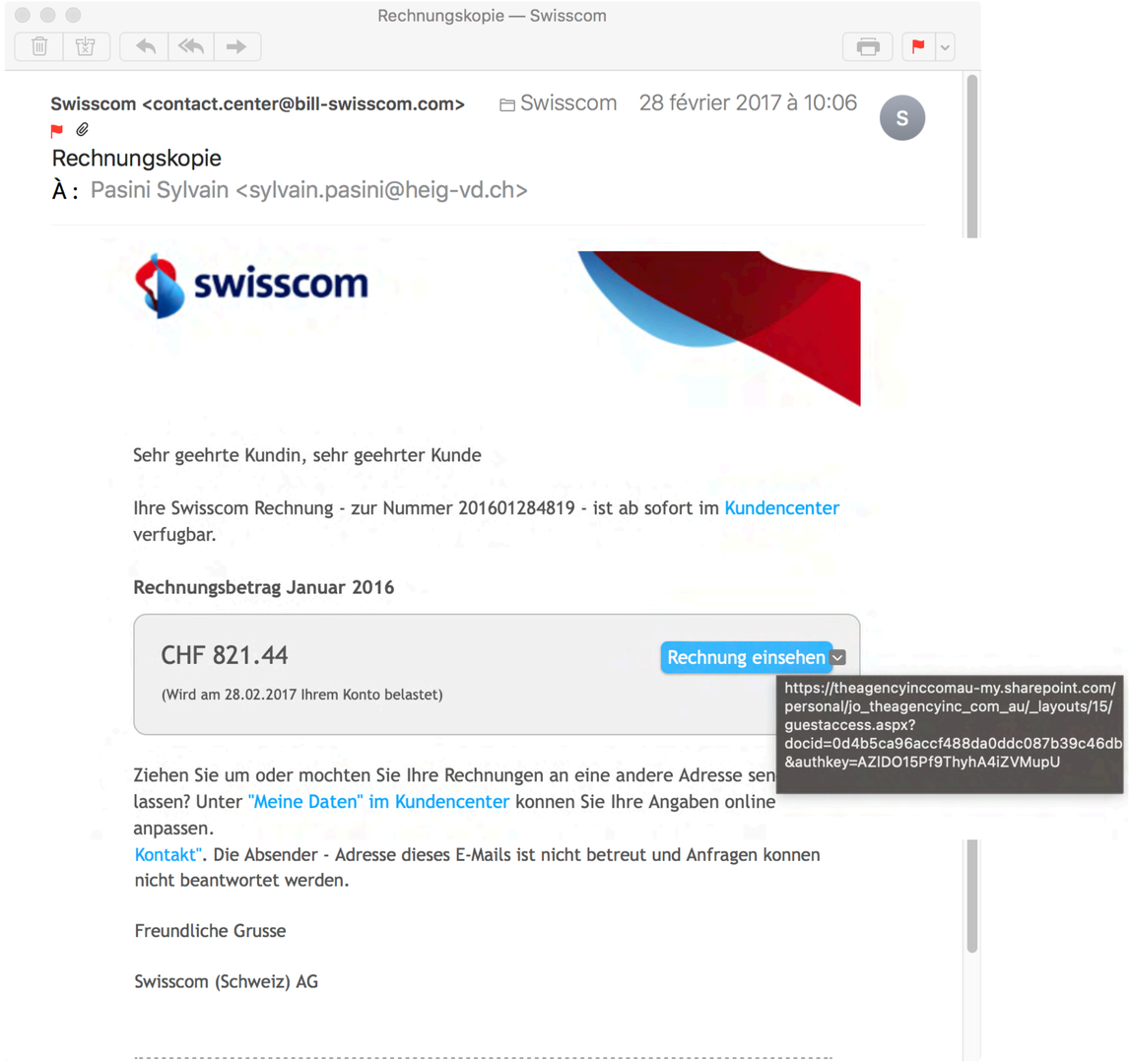
Reconnaître un lien

- Le lien ne pointe pas vers le bon site



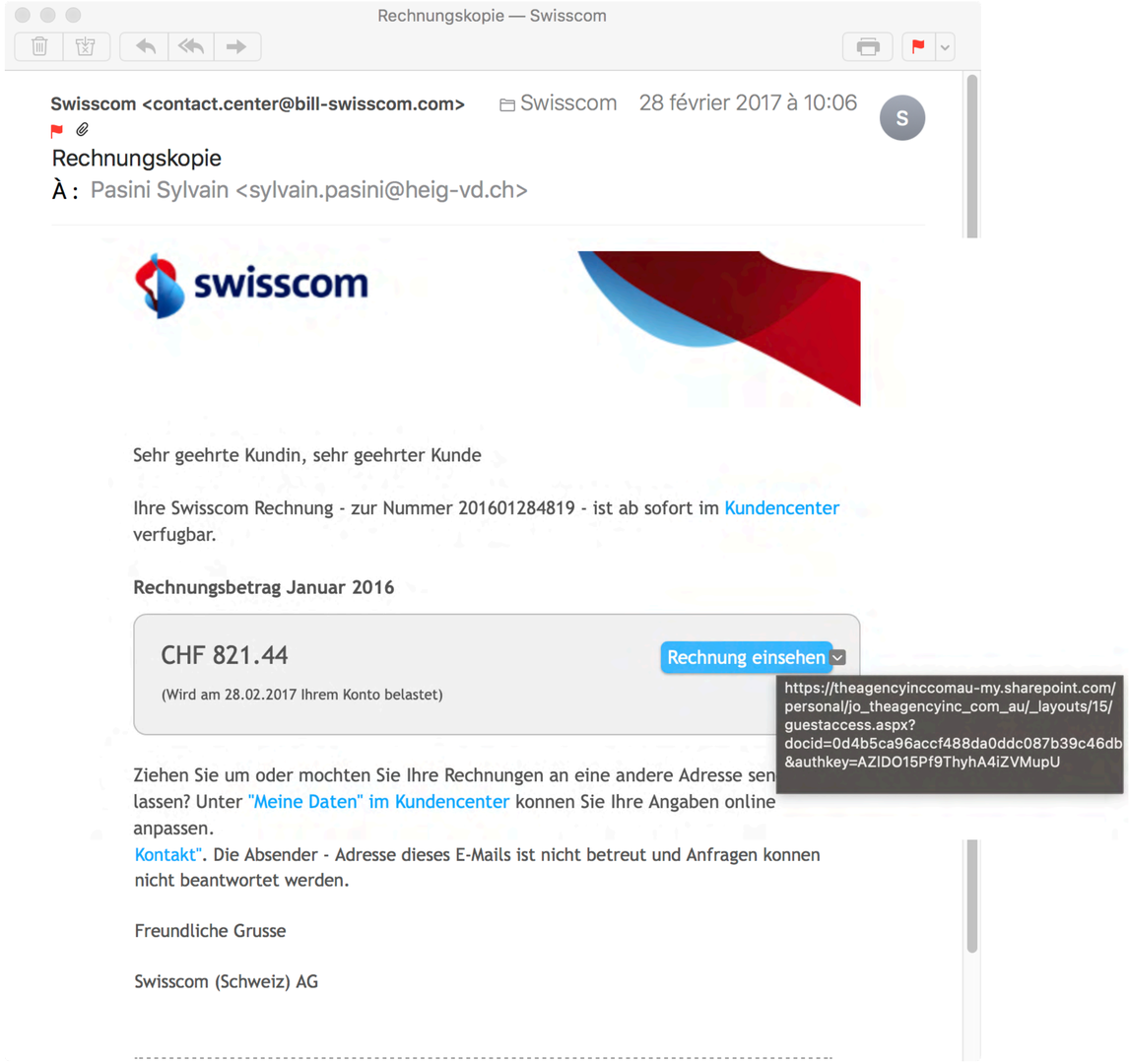
Reconnaître un lien

- Le lien ne pointe pas vers le bon site



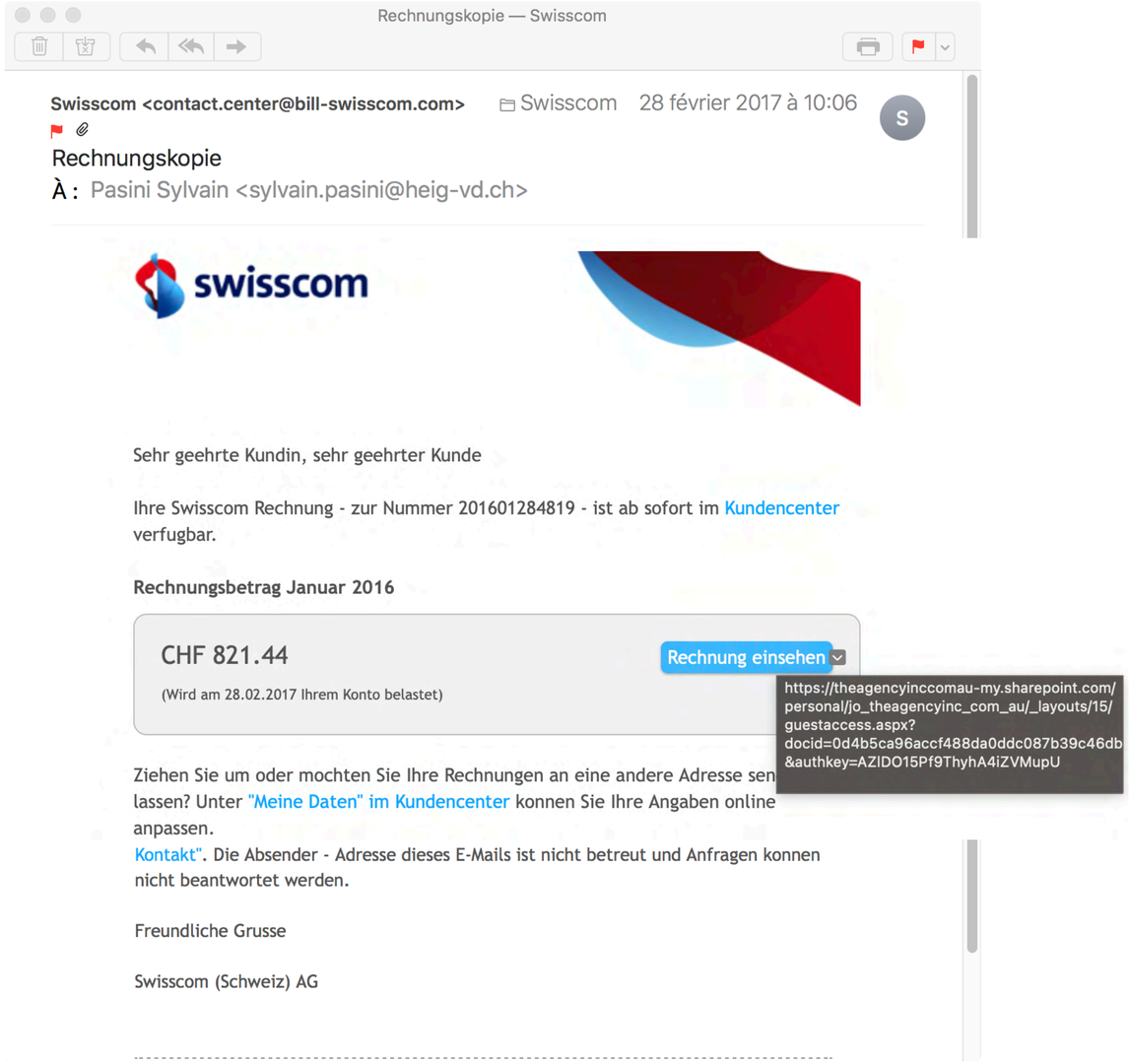
Reconnaître un lien

- Le lien ne pointe pas vers le bon site
  - http://security-check.paypal.com
  - http://paypal.security-check.com



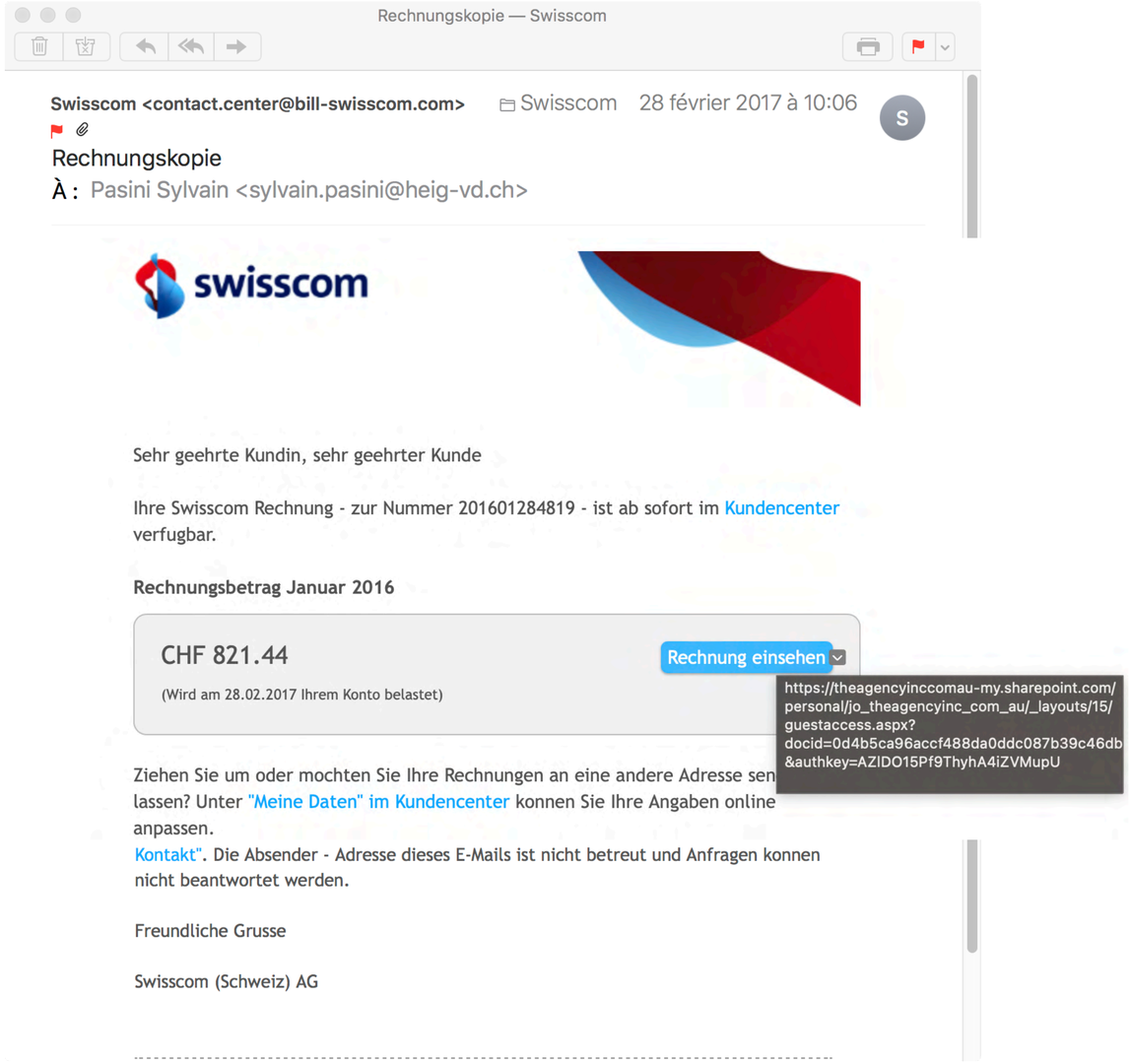
Reconnaître un lien

- Le lien ne pointe pas vers le bon site
  - http://security-check.paypal.com
  - http://paypal.security-check.com



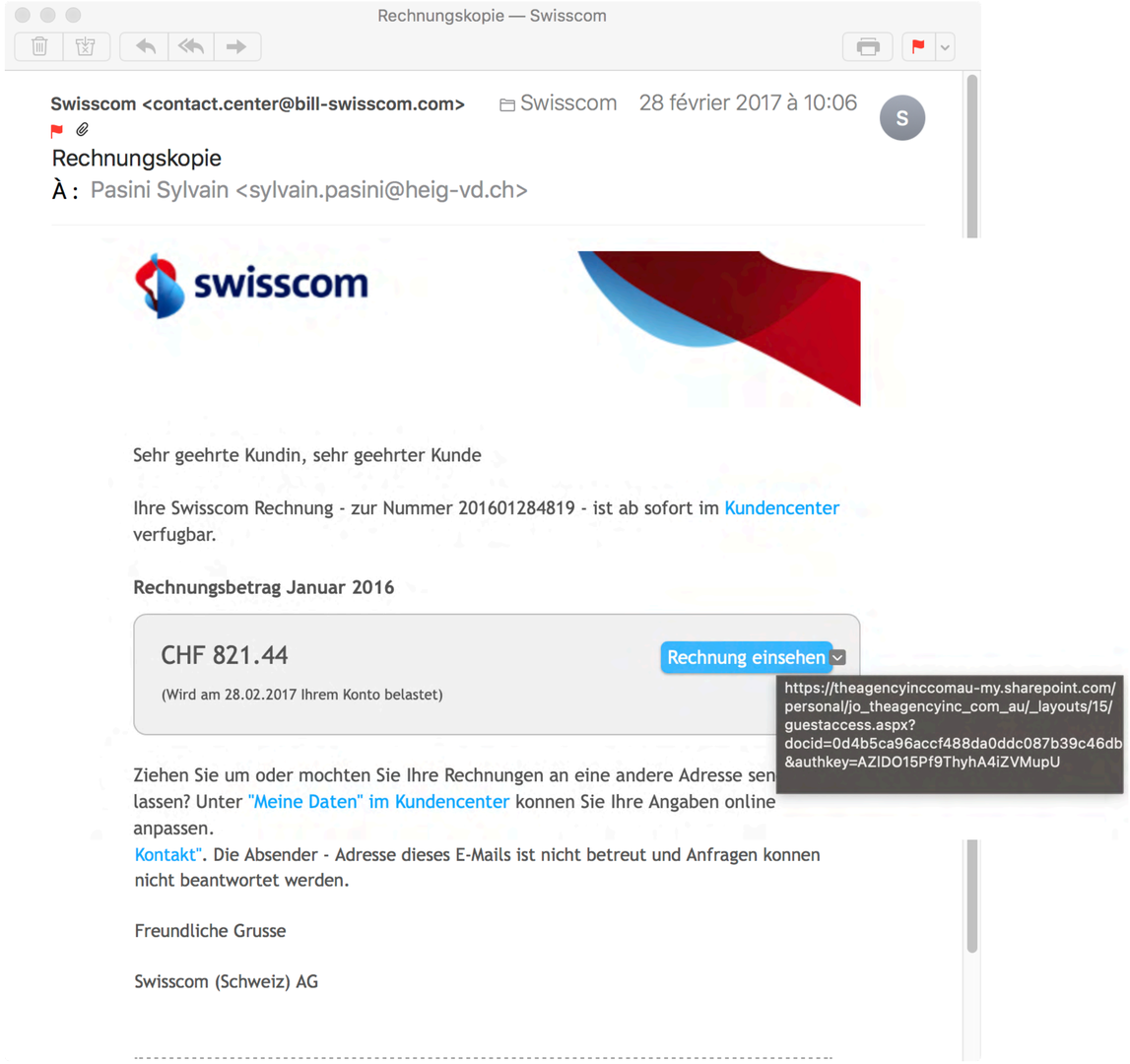
Reconnaître un lien

- Le lien ne pointe pas vers le bon site
  - http://security-check.paypal.com
  - http://paypal.security-check.com
  - http://support.apple.com
  - http://apple.support.com



Reconnaître un lien

- Le lien ne pointe pas vers le bon site
  - http://security-check.paypal.com
  - http://paypal.security-check.com
  - http://support.apple.com
  - http://apple.support.com



Ressources

canton de vaud
VOTREPOLICE

SKPPSC
Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral de la cybersécurité OFCS

RTS
Cyber arnaques :
escrocs et victimes 2.0

PRO SENECTUTE
PLUS FORTS ENSEMBLE

Vous êtes victime ?

- L’accepter
- En parler / la signaler
- Cesser tout contact avec l’escroc
- Si argent impliqué, contacter votre banque
- Déposer plainte pénale

Merci pour votre attention !

Prof. Sylvain Pasini
Responsable du pôle de compétences Y-Security, HEIG-VD

sylvain.pasini@heig-vd.ch
http://ch.linkedin.com/in/sylvainpasini