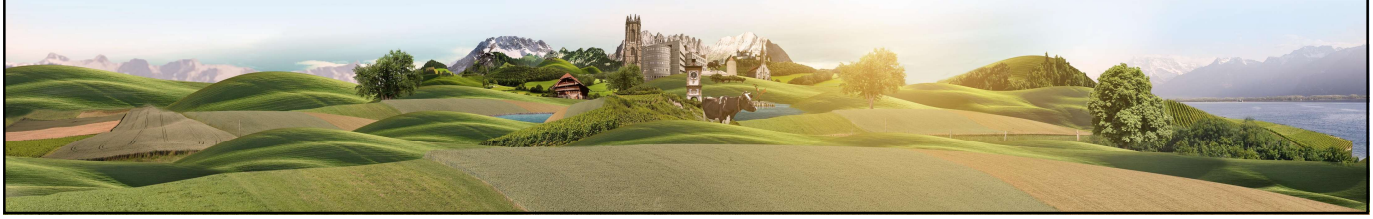
Banque Cantonale de Fribourg
Freiburger Kantonalbank
simplement ouvert - einfach offener

Arnaques financières et cas de fraude

Gilles Bersier, Luca Gotti et Laurent Pillet

23 avril 2025



1

Agenda

1. Ouverture
2. Sécurité informatique essentielle
3. Sécurité des services bancaires en ligne
4. Conclusion

2

2

Quelques chiffres

En %, combien de personnes confrontées à une arnaque ?

78.2 %

Combien de cas aboutissant à un vol ?

20 %

Somme volée en Suisse, par an, au plus de 55 ans ?

400 millions
(2018)

675 millions !
(2023)

3

3

Canaux touchés

E-Banking

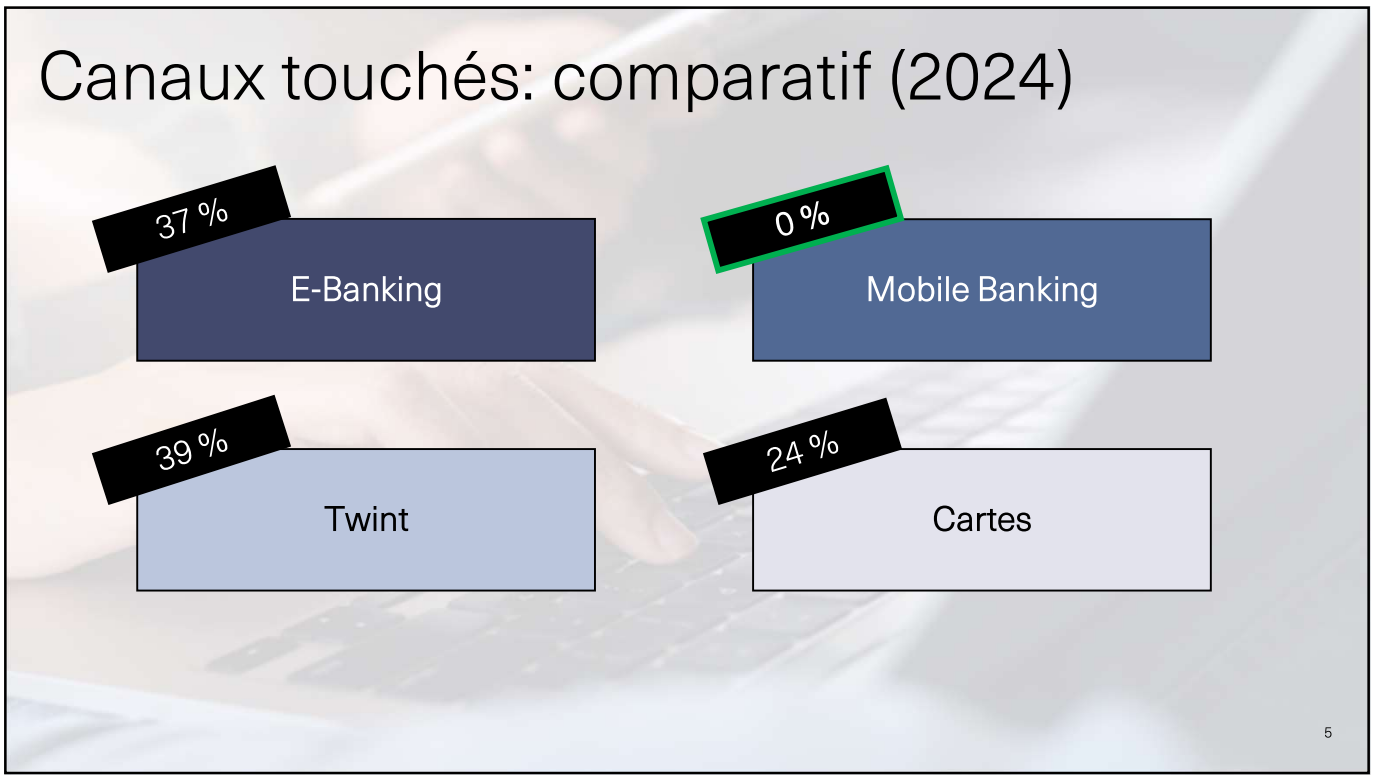
Mobile Banking

Twint

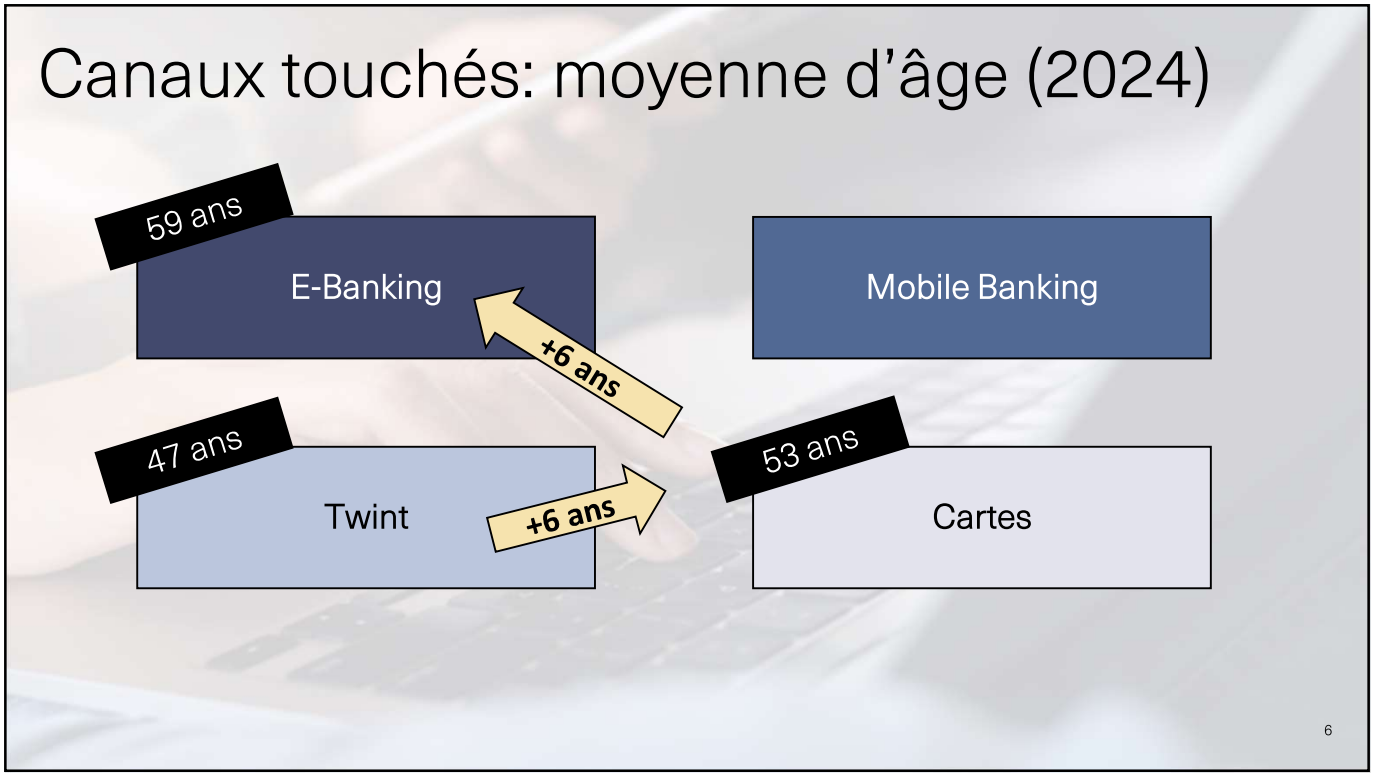
Cartes

4

4


Canaux touchés: comparatif (2024)
37 %
E-Banking
0 %
Mobile Banking
39 %
Twint
24 %
Cartes
5

5


Canaux touchés: moyenne d'âge (2024)
59 ans
E-Banking
Mobile Banking
+6 ans
47 ans
Twint
+6 ans
53 ans
Cartes
6

6

Êtes-vous prêts à nous aider à faire baisser ces chiffres ?

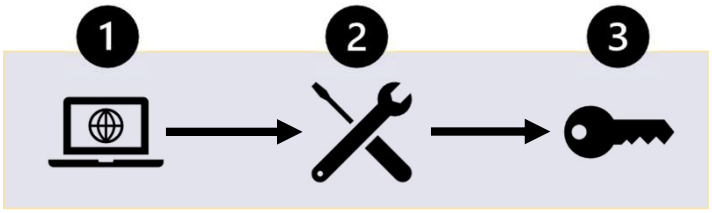
Tous ensemble, nous pouvons y arriver !

7

7

Sécurité informatique essentielle

1. Antivirus
2. Mises à jour
3. Mots de passe sécurisés



8

8

Antivirus

1ère **ligne de défense** de votre machine

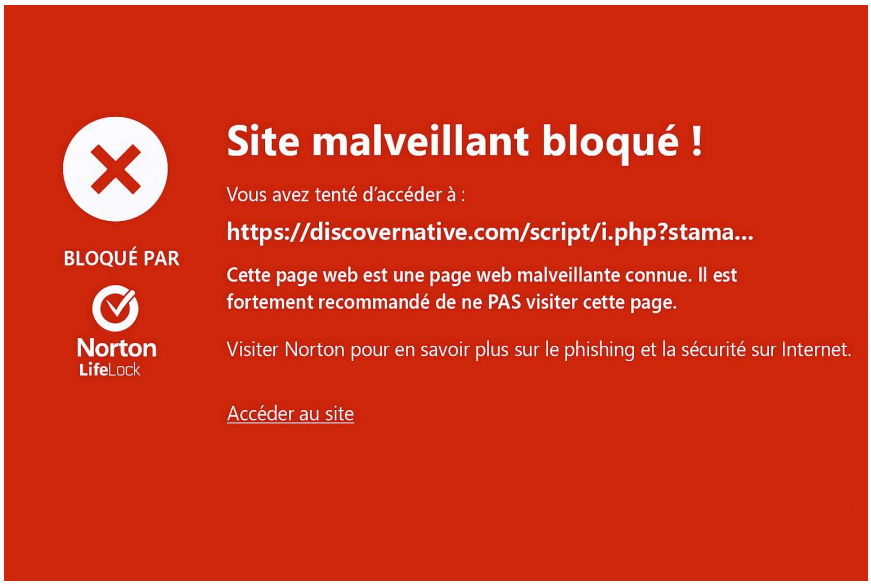
Chaque appareil numérique doit être protégé.

L'antivirus sur votre appareil est comparable au cadenas de votre porte d'entrée

9

9

Antivirus



10

10

Antivirus

McAfee
Avast
AVG
Avira
norton
eset
kaspersky
Bitdefender
Antivirus Plus
F-Secure
SOPHOS

11

11

Antivirus

Et sur nos téléphones portables ?

iOS (Apple) ≠ Android (Google)

Système fermé
Aucun antivirus n'existe
Toujours mettre à jour

Système ouvert
Antivirus à installer (PlayStore)
Toujours mettre à jour

12

12

Mises à jour

2

Pourquoi est-ce nécessaire de toujours faire ses mises à jour ?

Permet de recouvrir des failles de sécurités

Améliore les performances de l'appareil

Garantit une compatibilité optimale avec les autres app

Les mises à jour peuvent être faites automatiquement !
Si le système vous le propose, acceptez sans hésitation

13

13

Mots de passe sécurisés

3

Quelques règles pour créer **LE** mot de passe idéal !

- **12** caractères ou plus
- Utilisation de **majuscules**, **minuscules**, **chiffres** et **caractères spéciaux**
- Pas de suite logique (qwert, asdf, 12345, abcde, etc)
- Eviter les noms communs/propres (Maison123, Voiture$, 987Jean, etc)
- Utilisation d'un mot de passe **différent par site** (dans la mesure du possible)
- Caractères à bannir: ö, ä, ü, ç, etc → Ces caractères peuvent varier en changeant la langue du clavier !

14

14

Mots de passe sécurisés

Exemple d'un bon mot de passe :

lfb2j/a@SeVseS

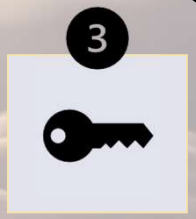
Il fait beau 200 jours par an à Sierre, en Valais, en Suisse

Passwortcheck

15

15

Mots de passe sécurisés



La majorité des sites vont vous **bloquer** après X tentatives. C'est pourquoi, certains organismes ne demandent que 8 caractères ou n'obligent pas, par exemple, l'utilisation de caractères spéciaux.

Merci de ne **jamais** transmettre votre mot de passe à un tiers !

16

16

Authentification à deux facteurs

Qu'est-ce qu'une authentification à deux facteurs (2FA) ?

1. N° de contrat / n° d'utilisateur / adresse mail / mot de passe
2. Codes SMS / Applications dédiées (CrontoSign Swiss, SwissID, MobileID)

17

17

Authentification à deux facteurs

A quoi ça sert ?

Une protection en plus

Barrière supplémentaire, même si votre mot de passe est volé.

18

18

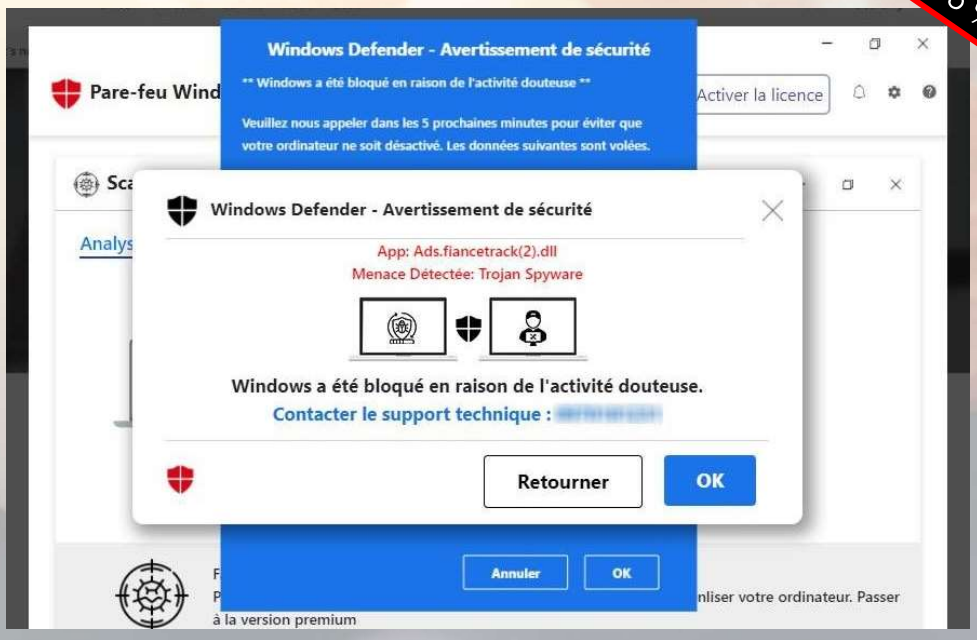
Sécurité des services bancaires en ligne

1. E-Banking
2. Twint
3. Phishing / Vishing
4. Bonnes pratiques en ligne
5. Comment réagir et résumé

19

19

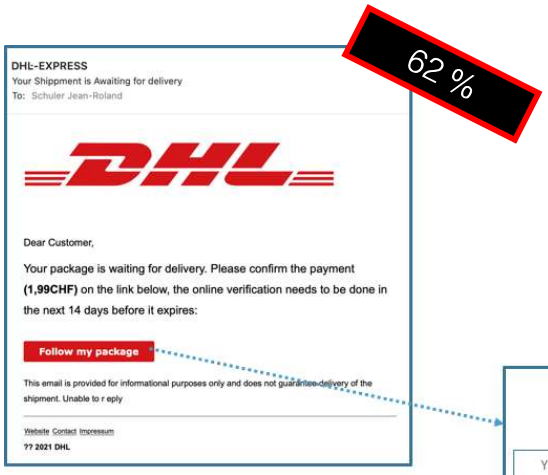
E-Banking: exemple concret



20

20

E-Banking: attention aux formulaires



Faux formulaire
=
Données volées !

21

21

Twint

Quelques **conseils** pratiques !

- Bien choisir son code NIP (6 chiffres)

  ~~123456 / 987654 / date de naissance / 333333~~
- Connaître les limites de son application
- Toujours **vérifier 2x les données** avant d'envoyer de l'argent
- N'envoyer de l'argent qu'à des **personnes de confiance**
- Ne jamais scanner de QR-Code / saisir des codes à chiffres envoyés par un inconnu

22

22

Twint

Reconnaître une arnaque Twint, quelques exemples

Pouvez-vous trouver ce qui cloche sur ces images ?

23

23

Cher(e) client(e) de TWT,

pour respecter les règlementations des paiements en ligne, il est impératif de procéder à une double authentification. Veuillez vérifier ci-dessous.

Activation mises à jour

lien frauduleux

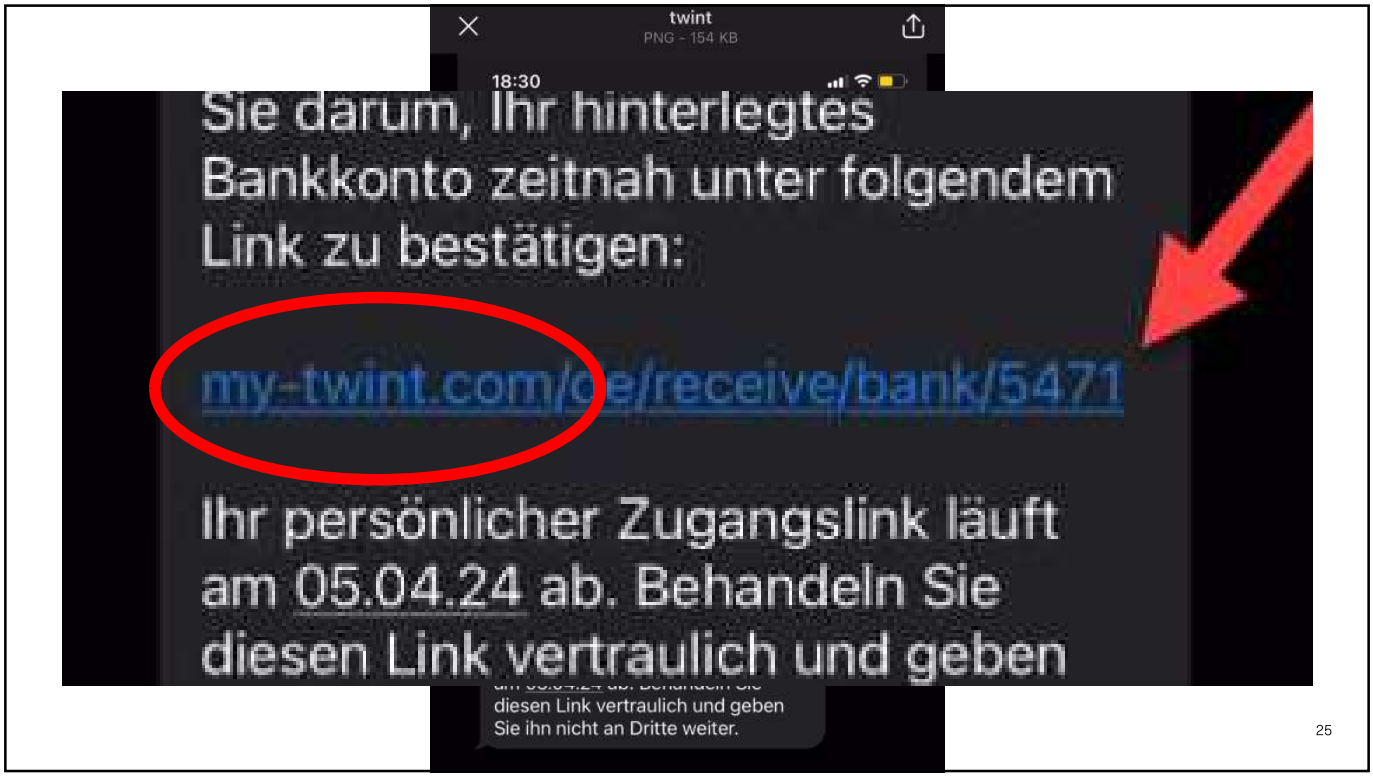
Zurich

TWINT AG
Stauffacherstrasse 41
CH-8004 Zurich

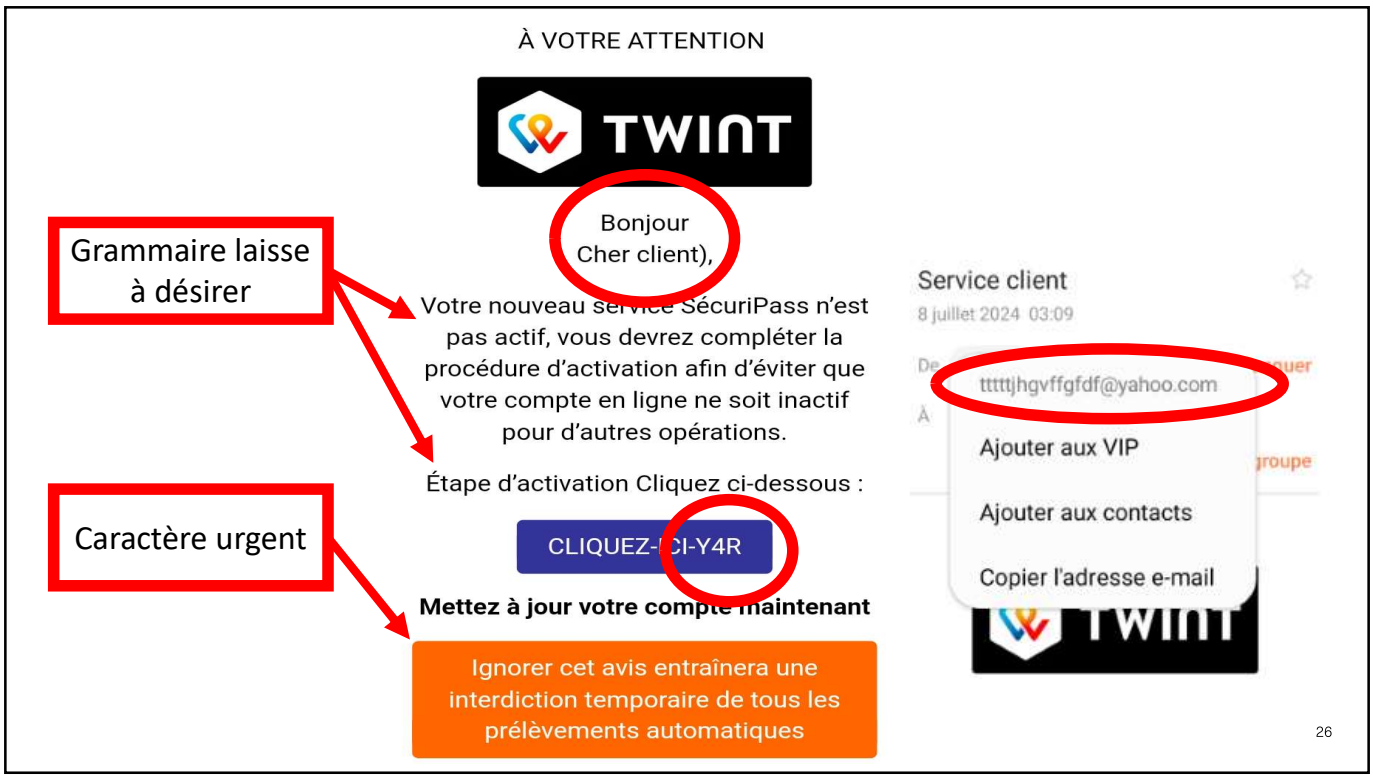
Numéro d'identification de la société (UID):
CHE-386.471.671

24

24

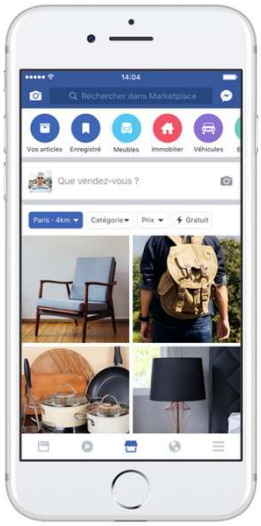

twint
PNG - 154 KB
18:30
Sie darum, Ihr hinterlegtes Bankkonto zeitnah unter folgendem Link zu bestätigen:
my-twint.com/ce/receive/bank/5471
Ihr persönlicher Zugangslink läuft am 05.04.24 ab. Behandeln Sie diesen Link vertraulich und geben
diesen Link vertraulich und geben
Sie ihn nicht an Dritte weiter.
25

25


À VOTRE ATTENTION
TWINT
Grammaire laisse à désirer
Bonjour
Cher client),
Votre nouveau service SécuriPass n'est pas actif, vous devrez compléter la procédure d'activation afin d'éviter que votre compte en ligne ne soit inactif pour d'autres opérations.
Étape d'activation Cliquez ci-dessous :
Caractère urgent
CLIQUEZ-ICI-Y4R
Mettez à jour votre compte maintenant
Ignorer cet avis entraînera une interdiction temporaire de tous les prélèvements automatiques
Service client
8 juillet 2024 03:09
ttttjhgvffgfdf@yahoo.com
Ajouter aux VIP
Ajouter aux contacts
Copier l'adresse e-mail
TWINT
26

26

Twint – Faux acheteurs



Revolut

PayPal

FAUX FORMULAIRE

27

27

Phishing / Vishing

Phishing	≠	Vishing
par écrit		par oral / vocal

28

28

Phishing

Il vaut mieux **supprimer** quelques mails ou SMS **authentiques** plutôt que d'**ouvrir** quelques mails ou SMS **frauduleux** !

Si une personne légitime n'a pas eu de réponse de votre part, elle vous recontactera

Il conviendra de **supprimer** le mail ou le SMS, si possible sans l'ouvrir au préalable, si:

- Il n'est pas attendu
- Un lien étrange apparaît
- Il est spécialement menaçant ou urgent
- L'expéditeur est inconnu
- Il annonce un problème imminent

29

29

Vishing

Les escrocs vont utiliser des techniques **d'ingénierie sociale** pour tenter de **manipuler vos émotions**

Leur but est de vous faire **révéler le plus d'informations** confidentielles possibles

Pour cela, ils vont **utiliser vos peurs**, vos **préoccupations** ou votre **excitation** (promesse de gain)

30

30

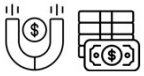
Vishing

Comment reconnaître un Vishing ?

Appel de la Police, du gouvernement, des services fiscaux

Demandent un paiement par carte ou un partage d'écran

Demandent des infos d'authentification (mot de passe)



Les offres présentées sont trop belles pour être vraies

31

Vishing

Lutter contre le Vishing

Evitez tous les appels de numéros inconnus et si l'appel semble suspect, raccrochez !!!

Bloquez les appels frauduleux dans les paramètres du téléphone

32

Phishing / Vishing

FRAUDE

Reconnaître une arnaque de type phishing, quelques exemples

Pouvez-vous trouver ce qui cloche sur ces images ?

33

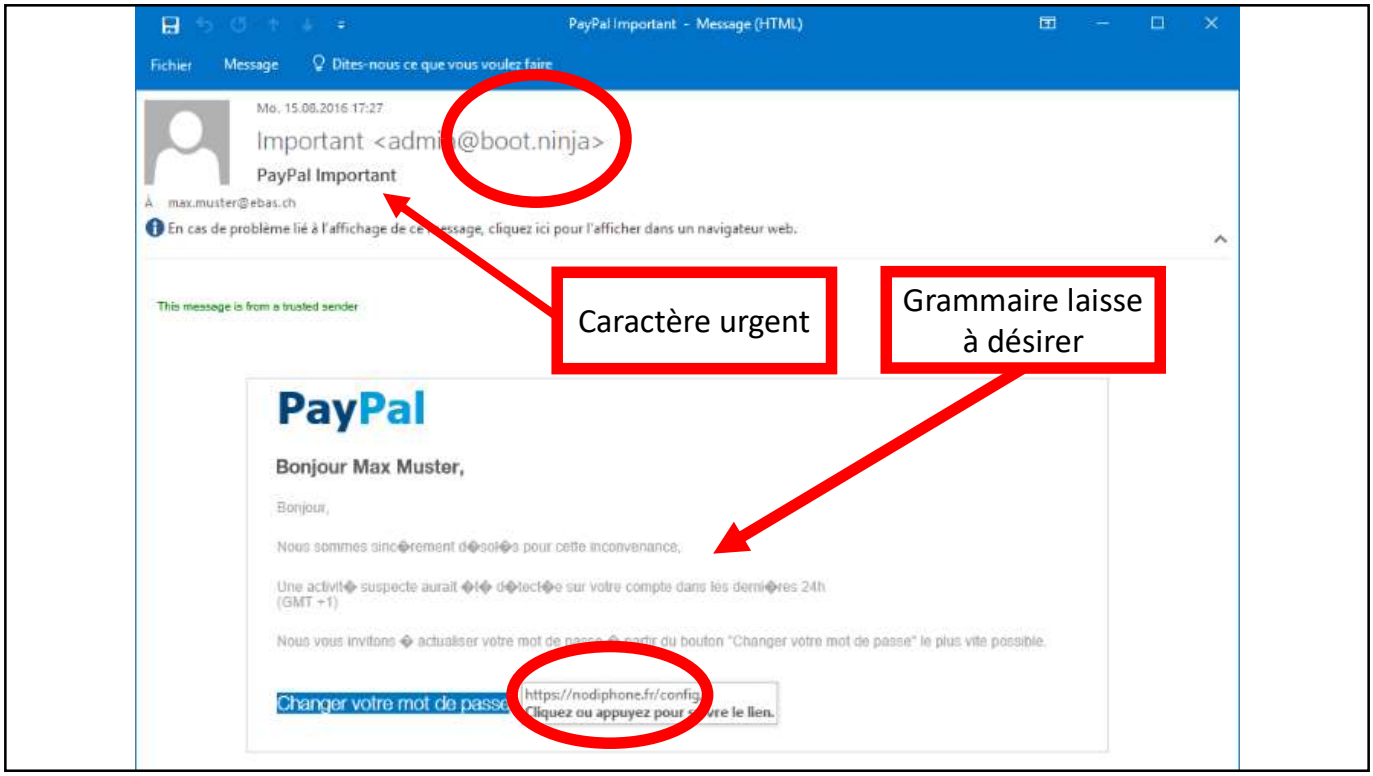
33

34

34


PostFinance
perfectioncooperative.org/www.postfinance.ch/PostFinance.htm
PostFinance
La 1ère partie ne correspond pas à PostFinance
Home
Clientèle privée
Clientèle commerciale
Contact Center
Notre profil
Mot de passe oublié? / modifier
Si disponible:
Identification de l'utilisateur
Suivant
Numéro e-finance à 9 chiffres ou
nom d'utilisateur choisi librement
3 Identification de l'utilisateur:
Entrer uniquement si le même numéro e-finance est utilisé par plusieurs utilisateurs (p. ex. compte partenaire, comptes commerciaux)
Aide avancée
Devenez client en ligne
Démo e-finance
35

35


PayPal Important - Message (HTML)
Fichier
Message
Dites-nous ce que vous voulez faire
Mo. 15.08.2016 17:27
Important <admi@boot.ninja>
PayPal Important
À max.muster@ebas.ch
En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur web.
This message is from a trusted sender
Caractère urgent
Grammaire laisse à désirer
PayPal
Bonjour Max Muster,
Bonjour,
Nous sommes sincèrement désolés pour cette inconvenance,
Une activité suspecte aurait été détectée sur votre compte dans les dernières 24h (GMT +1)
Nous vous invitons à actualiser votre mot de passe à partir du bouton "Changer votre mot de passe" le plus vite possible.
Changer votre mot de passe
https://nodiphone.fr/config
Cliquez ou appuyez pour suivre le lien.

36

Usurpation d'identité

DISPONIBLE

Vrai nom d'une personne connue

Adresse e-mail frauduleuse

Bonjour Laurent,

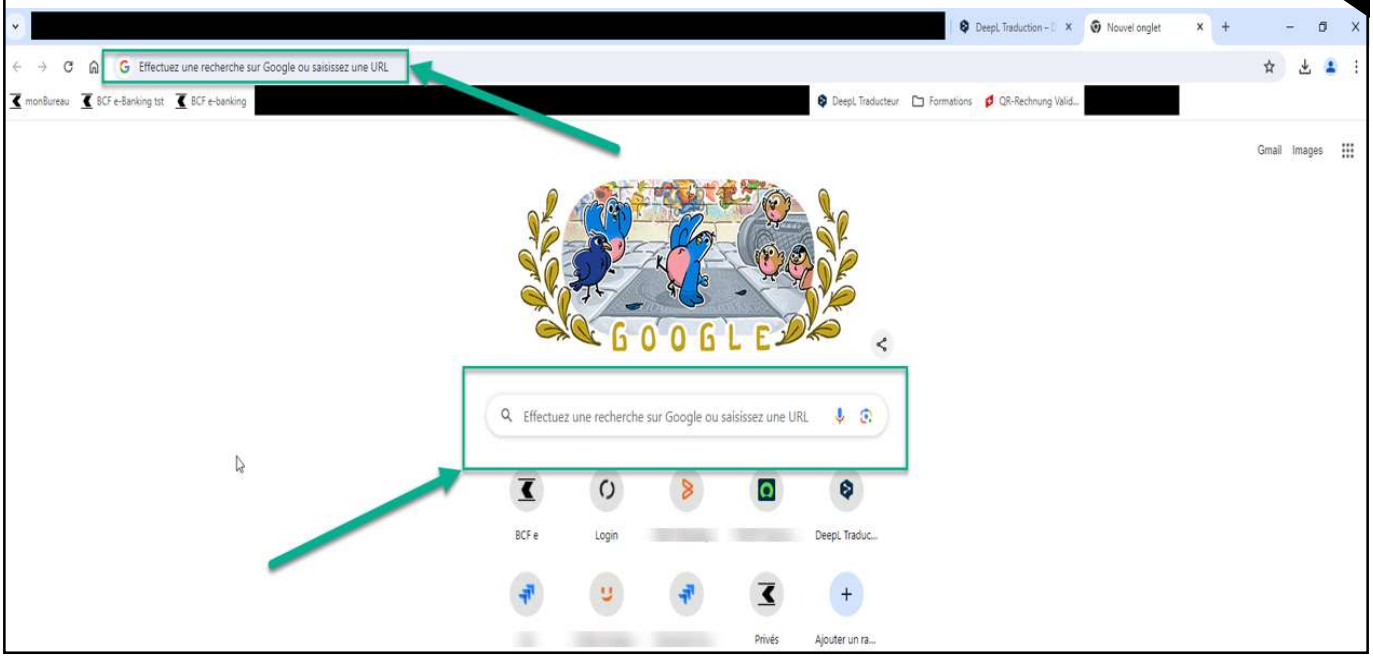
J'ai une tâche qui nécessite ton attention. Envoie-moi ton numéro de WhatsApp et attends mon texte.

Cordialement,

37

37

Bonnes pratiques en ligne



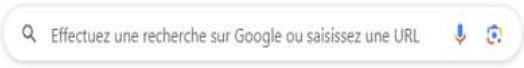
38

Bonnes pratiques en ligne

Recherche «Google»

Précision dépend de la formulation

Permet une recherche globale uniquement



Saisie d'URL

Accès direct au site si URL exacte

Evite de se tromper de site

39

39

Bonnes pratiques en ligne

Enregistrer son mot de passe dans le navigateur ?

JAMAIS !!!

Risques

Vulnérabilité aux virus

Sécurité insuffisante

Risque de synchronisation

Failles fréquentes

40

40

Résumé: cas les plus courants

1. Alerte Microsoft / Windows avec partage d'écran
2. Attention aux formulaires
3. Faux acheteurs / vendeurs
4. Faux policier

41

Réagir en cas d'attaque

1. Mettre fin à l'appel / supprimer le mail ou SMS
2. Se déconnecter des produits digitaux / éteindre le PC / quitter le réseau
3. Appeler sa banque
4. Contacter la Police / dénonciation pénale

Parlez-en ou demandez de l'aide!!!

42

42