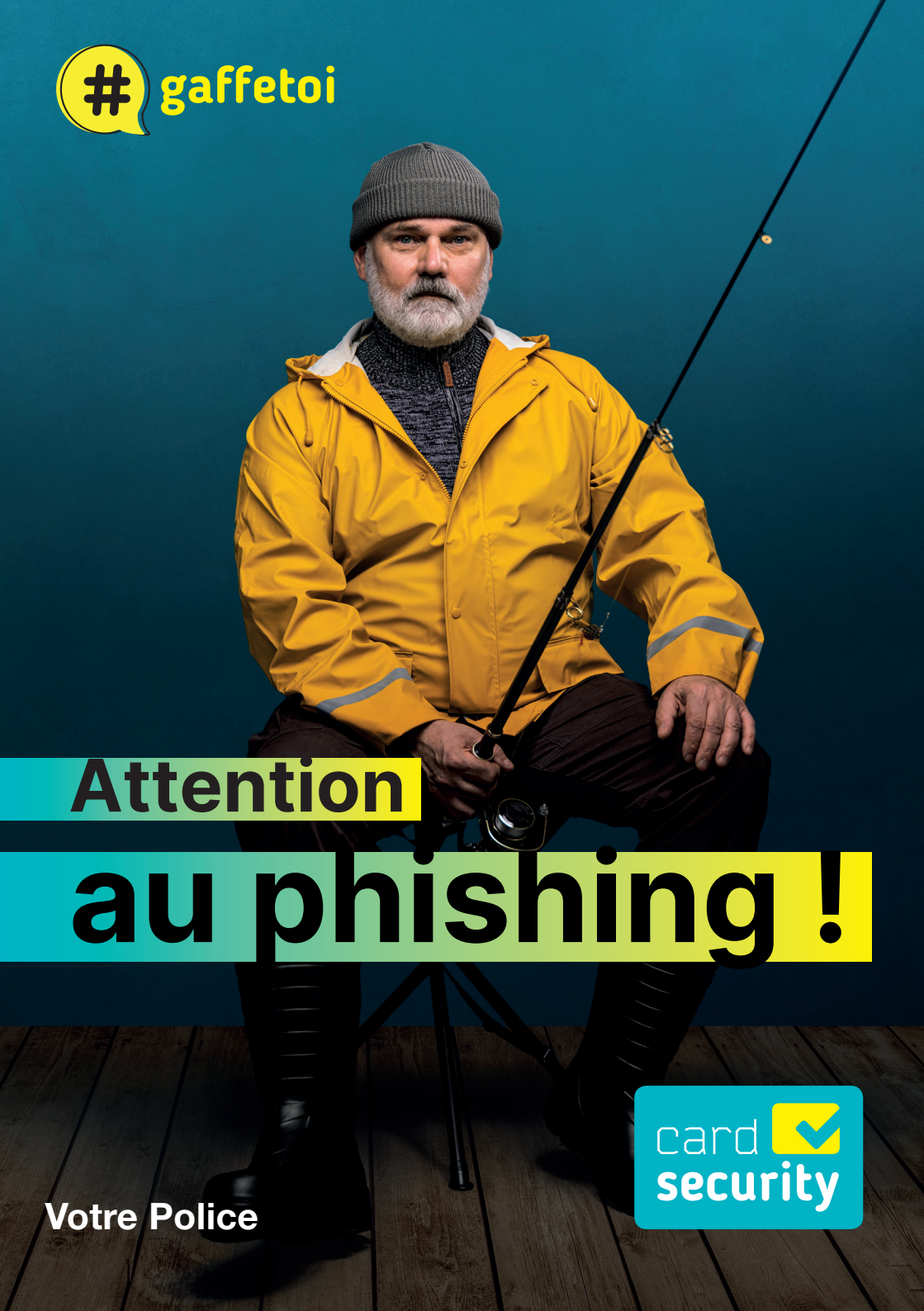
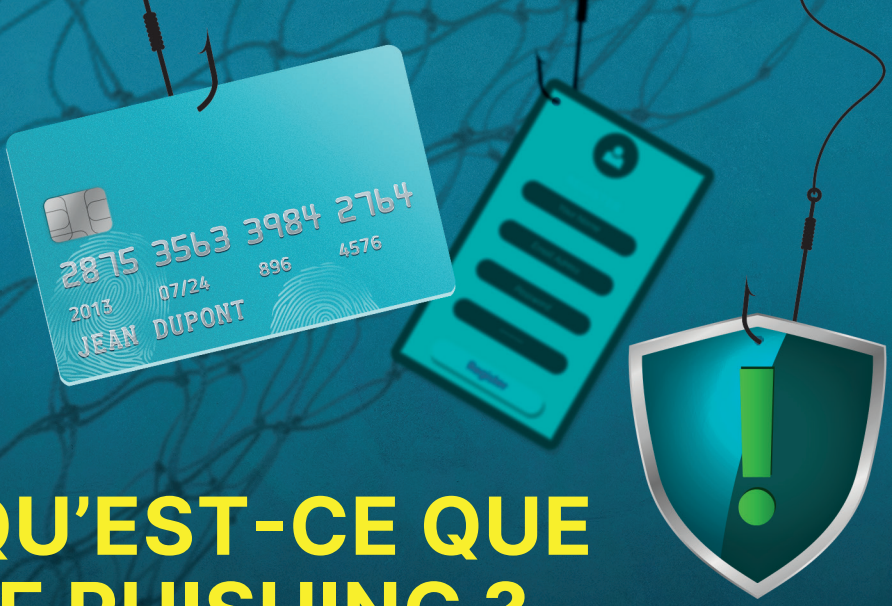
#gaffetoi



Attention au phishing !

card security

Votre Police



QU'EST-CE QUE LE PHISHING ?

Le phishing (hameçonnage) est actuellement la tactique de prédilection des cyber-escrocs, à l'origine de la plupart des fraudes à la carte bancaire.

Les cyber-escrocs entrent en contact avec leurs cibles par divers moyens, tels que les SMS, les messages WhatsApp ou les e-mails, se faisant habilement passer pour des établissements bancaires, des émetteurs de cartes ou même des services de livraison. Les victimes sont invitées à cliquer sur un lien contenu dans le message. Or celui-ci les conduit vers un site web piraté sur lequel elles saisissent leurs données personnelles.

Une fois en possession de ces données, les cyber-escrocs procèdent à des retraits d'argent ou à des achats en ligne. Les victimes peuvent alors subir des pertes financières considérables en un temps record.

Répondre aux e-mails de phishing en révélant ses identifiants ou ses codes est une action à haut risque : en cas de négligence, les titulaires de cartes endossent généralement la responsabilité des dommages subis.

CONSEILS POUR SE PRÉMUNIR CONTRE LES ATTAQUES DE PHISHING

Contrôlez l'expéditeur.

Face à un e-mail suspect, examinez attentivement l'adresse de l'expéditeur. Connaissez-vous l'expéditeur ? L'adresse e-mail vous paraît-elle authentique ? N'hésitez pas à contacter l'expéditeur officiel, comme votre banque ou le service de livraison, pour confirmer la légitimité de l'e-mail.

Repérez les erreurs.

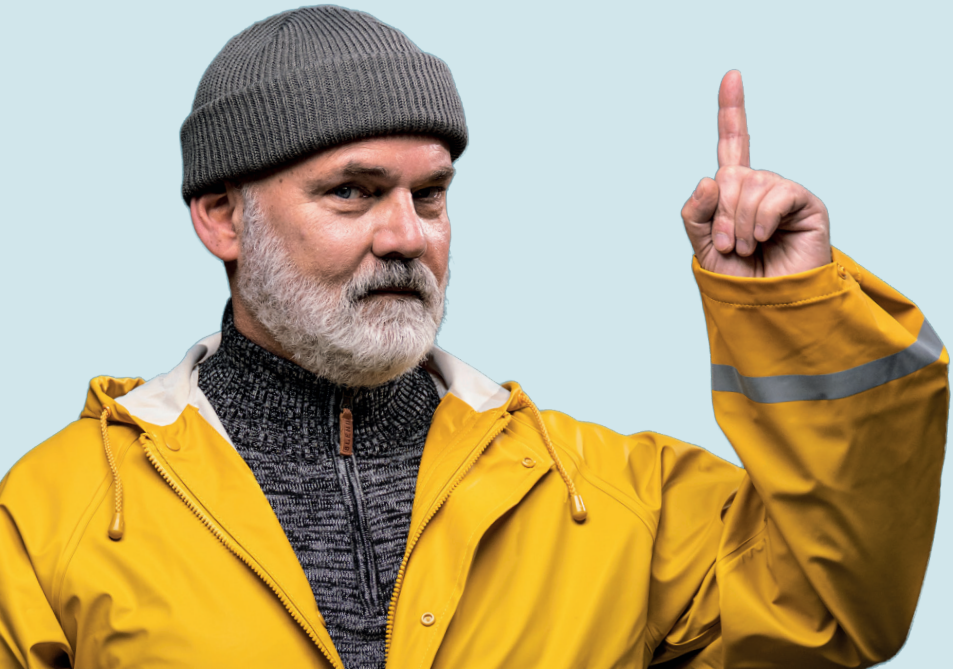
Lisez attentivement les e-mails non sollicités à la recherche de signes de fraude éventuelle. Prêtez attention aux logos suspects, aux fautes d'orthographe ou aux noms d'entreprises mal écrits. Ouvrez l'œil !

Protégez vos données personnelles.

Les banques ou les émetteurs de cartes ne demandent jamais d'informations confidentielles ou d'identifiants de connexion par e-mail. Ils ne communiquent pas non plus par ce biais pour vous avertir de toute activité inhabituelle sur votre compte ou votre carte. Ne répondez pas à de telles demandes.

Ne cédez pas à la pression.

Restez sur vos gardes si vous êtes soumis(e) à des pressions ou des menaces graves. Les attaques de phishing sont souvent accompagnées de délais serrés ou de menaces de poursuites judiciaires.



Examinez les liens.

Ne cliquez pas sur un lien ou sur une pièce jointe provenant d'un expéditeur inconnu ou d'un message non sollicité. Ils pourraient vous rediriger vers un site web compromis ou contenir un logiciel malveillant (malware).

Saisissez manuellement tout lien vers un site internet et assurez-vous qu'il s'agit bien de l'URL officielle de l'entreprise. Faites preuve de vigilance en présence d'un lien anormalement long et gardez à l'esprit que les sites web sécurisés commencent par « https:// ».

En cas de doute, ne payez pas.

Avant de partager vos données de carte et vos codes de sécurité, assurez-vous d'être à l'origine de la transaction.

Activez l'application de votre émetteur de cartes.

Pour limiter les risques de fraude, activez l'application de votre fournisseur de cartes, qui vous permettra de vérifier et, dans certains cas, de confirmer chaque transaction (3-D Secure).

Vérifiez chaque paiement.

Avant d'autoriser un paiement, examinez-le attentivement et vérifiez l'identité du destinataire ainsi que le montant à régler.

Ne divulguez jamais vos codes.

Ne partagez jamais vos codes de confirmation, car il pourraient être utilisés par des cyber-escrocs pour configurer un système de paiement mobile comme Google Pay afin de dérober de l'argent sur votre compte.

Informez-vous sur les sites marchands.

Consultez toujours les Conditions Générales de Vente des sites marchands et recherchez des labels de qualité tels que « Trusted Shops ».

Mettez à jour vos appareils.

Les programmes obsolètes sur l'ordinateur ou le smartphone présentent un risque pour la sécurité. Actualisez régulièrement vos appareils et mettez-les à jour afin de combler les éventuelles failles de sécurité. Utilisez également des logiciels antivirus et de sécurité.

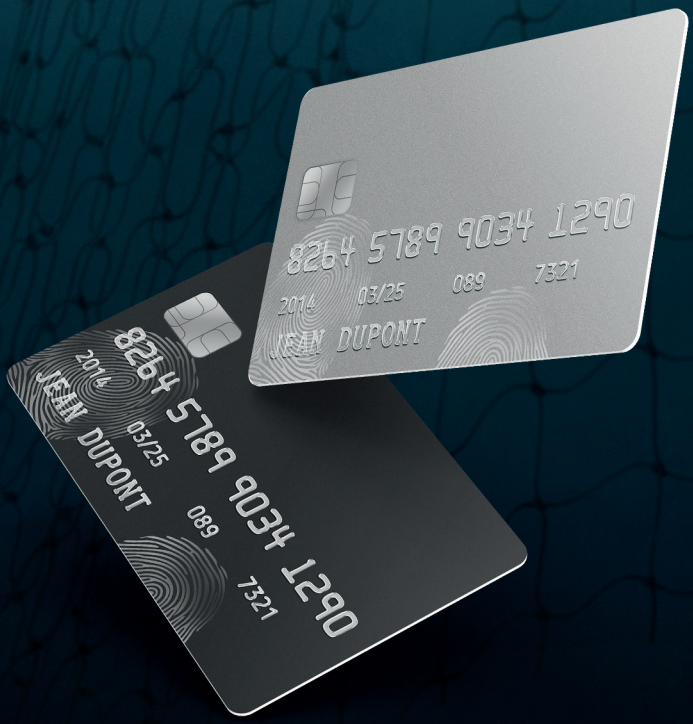
Portez plainte.

Si vous êtes victime d'une attaque de phishing, faites immédiatement bloquer votre carte de débit ou de crédit et modifiez les identifiants de connexion de l'ensemble de vos comptes. Déposez une plainte auprès de la police.

LE PAIEMENT PAR CARTES RESTE SÛR.

Les cartes de débit et de crédit, réputées pour leur sécurité, sont des moyens de paiement largement adoptés, suscitant ainsi l'intérêt des cyber-escrocs. Face à l'essor des attaques de phishing et à l'amélioration des techniques criminelles, de plus en plus de victimes se retrouvent piégées par ces arnaques.

En suivant quelques règles élémentaires, vous pouvez vous prémunir contre la plupart des fraudes à la carte bancaire. La vigilance est de mise !



Vers le quiz :
card-security.ch/fr/quiz

Pour en savoir plus sur la sécurité des cartes :
card-security.ch

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

Ihre POLIZEI
Votre POLICE
La vostra POLIZIA
Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali