Comment se protéger ?

» Se méfier des messages provenant d'expéditeurs inconnus.

» Ne jamais cliquer sur les liens ou ouvrir les pièces jointes.

» Toujours vérifier l'e-mail de l'expéditeur et l'URL.

» Se connecter uniquement sur des sites officiels (et non via des liens).

» Mettre à jour le navigateur web et le système d'exploitation.

» Ne jamais divulguer ses identifiants de connexion ou les données de ses cartes.

» Utiliser des mots de passe forts et l'authentification à 2 facteurs (2FA).

» Activer le service de notification pour recevoir un message en cas de paiement.

» Vérifier ses transactions et ses paiements.

Teste tes connaissances !

Que faire d'autre ?

» Demander à sa banque ou à l'établissement émetteur de sa carte les fonctionnalités permettant de sécuriser sa carte.

» N'activer que les fonctionnalités effectivement utilisées au quotidien.

» Porter plainte en cas de vol.

Pour en savoir plus sur la sécurité des cartes :
www.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

#gaffetoi

Attention au phishing !

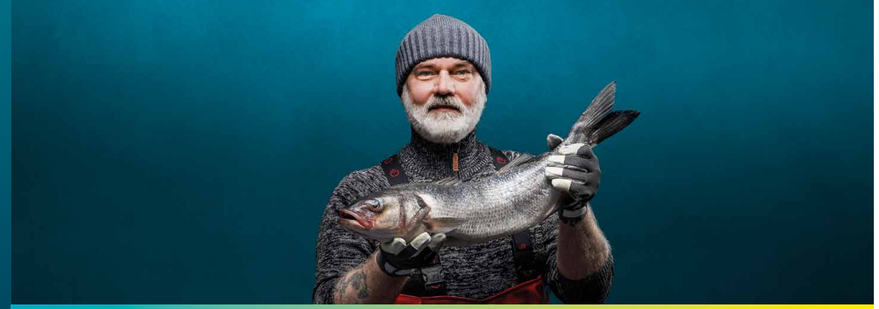
Protège-toi des fraudes à la carte.

card security

Votre Police

#gaffetoi de ce type de FRAUDE

Les cartes de débit et de crédit sont des moyens de paiement populaires et très sûrs, qui sont de plus en plus utilisés. Les escrocs, attirés par cette aubaine, tentent de dérober de l'argent à leurs victimes en recourant constamment à de nouvelles arnaques. Heureusement, la plupart des fraudes à la carte peuvent être évitées, à condition toutefois que les titulaires de cartes respectent certains principes de base.



Phishing

Si les attaques de phishing se distinguent souvent par leur présentation et leur contenu, le principe qui les sous-tend reste toutefois le même. Les victimes potentielles reçoivent des messages par e-mail, téléphone portable ou réseaux sociaux. Ces messages ressemblent à s'y méprendre à des communications officielles provenant d'une banque, d'une société émettrice de cartes bancaires ou d'un service de livraison. Les victimes sont invitées à cliquer sur le lien contenu dans le message. Elles sont alors redirigées vers un site web piraté sur lequel des informations personnelles leur sont extorquées. Y répondre, c'est dire adieu à son argent !

Pharming

Ce type d'escroquerie est apparenté au phishing. Les personnes ciblées saisissent une adresse web authentique et, au moyen d'un virus ou d'un cheval de Troie, sont redirigées à leur insu vers une page piratée. Comme dans le cas du phishing, les victimes sont ensuite invitées à saisir leurs données personnelles et les informations figurant sur leur carte. Grâce à ces informations, les cybercriminel(le)s ont ensuite les coudées franches pour leur dérober de l'argent. Ce type d'arnaque est appelé « pharming », ou dévoiement, car des « exploitations (fermes) » entières de serveurs contenant des sites web piratés sont gérées en arrière-plan.

Carding

Dans le cas du carding, les escrocs utilisent les données de cartes volées ou piratées pour faire des achats en ligne ou retirer de l'argent au Bancomat. Pour ce faire, ils ciblent délibérément les cartes ou les sites marchands dont les systèmes de sécurité sont vulnérables. Les données sont collectées illégalement en amont suite à des arnaques par hameçonnage, des violations de la protection des données ou du skimming, pour être ensuite vendues sur le darknet. Les victimes n'apprennent souvent la fraude que lorsqu'elles se font dérober de l'argent. Il peut s'écouler des mois entre le moment où les données sont volées et l'arnaque proprement dite.

Scamming

Les escrocs qui pratiquent le scamming appâtent leurs victimes avec des offres alléchantes qui n'ont qu'un seul but : amener les victimes à effectuer des paiements anticipés sous un prétexte quelconque. Le scamming se présente sous différentes formes : l'arnaque sentimentale (romance scam), l'arnaque à l'investissement (investment scam), l'arnaque au logement (flatmate ou holiday scam), l'arnaque au job (employment scam) ou la promesses de gains à la loterie (lottery scam).