VOS VIREMENTS EN LIGNE

4 FOVI ou Faux ordres de virement

Le principe :

Créer un climat de confiance avec la victime pour obtenir, dans l'urgence, un virement bancaire international.

Le piège :

Les entreprises sont particulièrement visées par ces FOVI : par exemple, le « Changement de RIB » qui consiste pour les fraudeurs à envoyer un mail à un salarié du service comptabilité de l'entreprise, en se faisant passer pour un fournisseur (ou son dirigeant), et lui demander de diriger ses versements vers un autre compte bancaire appartenant aux escrocs.
Mais les particuliers sont désormais également ciblés via des escroqueries à l'assurance vie ou à l'optimisation fiscale.

Comment se préserver :

- Assurez-vous que les procédures internes de votre entreprise vous permettent d'assurer un contrôle avant le départ des fonds.
- Restez vigilant sur la qualité de vos interlocuteurs (faites un contre appel pour confirmer le numéro de téléphone, vérifiez l'organigramme de la société sur internet...) et la qualité des documents transmis.
- N'effectuez jamais de virement dans l'urgence.
- **Appelez immédiatement votre banque en cas de constatation d'une escroquerie afin d'interrompre le virement.**

VOTRE CARTE BANCAIRE

5 SKIMMING

Le principe :

Mise en place d'un dispositif sur le distributeur de billets ou les bornes automatiques de paiement (ex : parking, stations services...) destiné à capturer les données de la bande magnétique de votre carte et à enregistrer physiquement ou par vidéo votre **code secret**.

Le piège :

Les données de votre carte bancaire seront utilisées pour effectuer des achats par internet ou des retraits d'espèces.

Comment se préserver :

- Composez votre code confidentiel en masquant le clavier.
- **Ne quittez pas l'écran des yeux**, n'écoutez pas les conseils d'inconnus.
- Si votre carte reste coincée dans le distributeur, ne recomposez jamais le code.
- **N'utilisez pas un distributeur de billets qui semble avoir été modifié**. En cas de doute, contactez votre agence.
- **Portez une attention particulière à la possible capture des données de votre CB notamment lors des paiements à l'étranger sans composition du code secret.**

Document réalisé en partenariat avec :

BNP PARIBAS — Banque de Nouvelle Calédonie *La banque, en mieux.* — SOCIETE GENERALE CALEDONIENNE DE BANQUE — OPT Nouvelle-Calédonie SERVICES FINANCIERS — Gendarmerie nationale — FEDERATION BANCAIRE FRANCAISE Comité Nouvelle-Calédonie — BCI Groupe BRED

BNP PARIBAS — Banque de Nouvelle Calédonie *La banque, en mieux.* — SOCIETE GENERALE CALEDONIENNE DE BANQUE — OPT Nouvelle-Calédonie SERVICES FINANCIERS — Gendarmerie nationale — FEDERATION BANCAIRE FRANCAISE Comité Nouvelle-Calédonie — BCI Groupe BRED

SURFEZ COUVERT

Évitez les pièges tendus par les cyber-escrocs

LA CYBERCRIMINALITÉ AU QUOTIDIEN

VOTRE ARGENT

1 SCAM 419 ou Loterie

Le principe :

Abuser de votre crédulité en vous faisant entendre par mail que vous pouvez gagner une grosse somme d'argent ou le gros lot d'une loterie, en facilitant un transfert de fonds d'un pays tiers vers la Nouvelle-Calédonie.

Le piège :

Dans tous les cas, on vous demande d'abord d'envoyer une somme d'argent par mandat cash (quelques milliers de francs) pour débloquer un lot que vous avez soi-disant gagné ou la rémunération qui vous est promise.

Comment se préserver :

- N'effectuez pas de paiement par mandat cash.
- N'ouvrez pas des mails de provenance inconnue.
- Ne répondez jamais à ce type de mail.
- Supprimez systématiquement ces courriers.

ATTENTION : ARGENT FACILE = ESCROQUERIE

VOS DONNÉES PERSONNELLES

2 PHISHING ou Hameçonnage

Le principe :

Rediriger les internautes, à leur insu, vers un site pirate en lieu et place du site internet qu'ils ont demandé.

Le piège :

Le but est de récupérer vos données confidentielles (numéro de compte, données de votre carte de crédit), qui seront ensuite utilisées pour vider vos comptes ou effectuer des achats par internet.

Comment se préserver :

- N'ouvrez pas des mails de provenance inconnue.
- Ne communiquez jamais vos mots de passe et codes secrets sur internet **(votre banque ne demandera jamais d'informations confidentielles par mail)**.
- Assurez-vous, lors de connexions sur un site sécurisé, que l'adresse commence bien par **https**. En cas de doute, déconnectez-vous et téléphonez immédiatement à votre agence.

VOS ACHATS EN LIGNE

3 FRAUDES ET ESCROQUERIES

Le principe :

Vous faire croire que vous allez conclure une très bonne affaire.

Le piège :

L'objectif est de vous faire acheter un produit (qui n'existe pas ou dont la qualité ne correspond pas à la description) et / ou à divulguer des informations personnelles.

Comment se préserver :

- **N'effectuez jamais de paiement par mandat cash.**
- Assurez-vous de l'adresse et des références du vendeur (annuaire, moteur de recherche).
- Pour les achats à l'étranger à des particuliers ou des entreprises non référencées : réglez de préférence à réception ou par un **moyen de paiement sécurisé**.
- Ne communiquez pas vos coordonnées bancaires (numéros de carte bancaire, date de validité) sur un site non sécurisé (adresse ne commençant pas par **https**).
- Lors de la consultation d'un site gratuit, il n'y a pas lieu de communiquer vos coordonnées bancaires.
- Liez systématiquement les conditions générales de ventes, y compris les petites lignes.