MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ALERTECYBERGEND 80
Gendarmerie départementale de la Somme

28 janvier 2026

FRAUDE AU PRÉSIDENT

LE PIÈGE DE LA VARIANTE "CARTES CADEAUX"

Une **menace** bien réelle : une **entreprise locale** a été la cible de cette cyber-escroquerie **sophistiquée**. Si la **vigilance** de l'employée a permis d'éviter le pire, ce scénario révèle des méthodes de manipulation de plus en plus **affûtées**. La **fraude au Président** ne vise plus seulement les **virements massifs**, mais cible désormais directement les **collaborateurs** via des moyens de paiement détournés.

DÉCRYPTAGE : LE MODE OPÉRATOIRE DE L'ESCROC

L'attaque repose sur une ingénierie sociale précise et une exécution en trois phases clés :

1. Le ciblage stratégique (Le "Sourcing")

L'escroc utilise les réseaux sociaux professionnels pour identifier les nouveaux arrivants. Une personne récemment embauchée est la cible idéale : elle souhaite prouver sa réactivité, connaît encore mal les circuits de validation internes et n'ose pas toujours contester un ordre venant de la direction.

2. La mise en confiance et l'isolement

- ✗ **L'usurpation** : Un mail est envoyé au nom du dirigeant. En apparence légitime, l'adresse réelle (visible au survol de la souris) est pourtant frauduleuse.
- ✗ **Le canal privé** : L'escroc exige de basculer la communication sur SMS. Cela permet de sortir du cadre sécurisé de l'entreprise et d'instaurer une fausse confidentialité.
- ✗ **La mission "spéciale"** : Le prétexte est souvent une urgence (cadeaux clients, récompense équipe) nécessitant l'achat de cartes-cadeaux (Xbox, Amazon, PCS, ...).

3. Le piège financier

L'employée est incitée à avancer les fonds avec sa carte bancaire personnelle contre une promesse de remboursement. Une fois les cartes achetées, l'escroc demande une photo des codes numériques au dos. Une fois ces codes transmis, l'argent est instantanément siphonné. Le préjudice est immédiat et le remboursement devient complexe, pour ne pas dire impossible.

NOS CONSEILS PRÉVENTIFS : COMMENT RÉAGIR ?

1. Analysez la source avant d'agir

Prenez toujours 5 secondes pour survoler l'adresse de l'expéditeur avec votre souris. Une lettre manquante ou un domaine générique (@gmail.com) est le signe d'une fraude certaine.

2. Méfiez-vous de l'urgence et de la confidentialité

L'escroc mise sur le stress pour court-circuiter votre esprit critique. Si l'on vous demande de garder une mission "secrète" ou de ne pas passer par les canaux habituels, c'est une alerte rouge. Un dirigeant ne vous demandera jamais d'engager vos fonds personnels.

3. Pratiquez le "Contre-Appel"

C'est la règle d'or. Au moindre doute, contactez votre supérieur via son numéro de téléphone habituel ou de vive voix. Ne rappelez jamais le numéro qui vous a envoyé le SMS suspect.

4. Protégez vos informations sur les réseaux

Limitez la visibilité de vos informations professionnelles sur les réseaux sociaux. Évitez de publier des détails trop précis sur votre nouveau poste dès votre arrivée, car cela donne des munitions aux cybercriminels pour personnaliser leurs attaques.

***RAPPEL :** La sécurité est l'affaire de tous. Si vous recevez un tel message, informez immédiatement votre direction ou votre service informatique.*
Votre signalement peut protéger l'ensemble de vos collègues.