

Eviter l'arnaque au Président :

Recommandations pour les ONGD

MAI 2025



INTRODUCTION



Comme les entreprises, les ONGD peuvent être prises pour cible par des escrocs afin de leur soutirer indûment de l'argent. Toutes les organisations, quelle que soit leur taille, peuvent être un jour victime de ces attaques. La mise en place de mécanismes de contrôle et procédures internes adaptées et actualisées rend des organisations moins vulnérables et, en s'inscrivant dans un cadre de gouvernance responsable et participatif, permet de réduire considérablement les risques.

Les progrès informatiques, dont l'IA générative, ont donné aux criminels de nouvelles technologies pour contrefaire des identités, s'informer sur les organisations cibles et mener à bien leurs actions. La capacité à générer des deepfakes vont rendre dans le futur les arnaques de plus en plus crédibles et difficiles à identifier et constituent un nouveau défi.

Afin d'appuyer les ONGD et leur personnel pour se prémunir contre ces arnaques, le Cercle de Coopération a développé le présent document qui a pour objet de présenter les stratégies mises en œuvre par les criminels pour attaquer les organisations et de proposer des recommandations à mettre en place par les ONGD pour faire face à cette menace.

Définition de l'arnaque au Président

L'arnaque ou fraude au Président est une escroquerie qui vise des personnes avec un certain niveau de responsabilité au sein d'une organisation, en exploitant leur autorité et leur crédibilité pour obtenir des informations sensibles ou effectuer des transferts de fonds vers des comptes bancaires extérieurs à l'organisation.

Grâce à cette technique, les cybercriminels vont tromper les employé.e.s d'une organisation en se faisant passer pour la direction ou pour une personne de confiance (fournisseur, appui légal, ...). L'objectif final est généralement de persuader l'employé.e ou un membre du CA de l'ONG de divulguer des informations confidentielles ou de réaliser, à leur insu, des transactions financières frauduleuses.

Les escrocs savent se montrer très persuasifs et pertinents et disposent souvent d'informations précises sur l'ONG, sur la direction, sur les projets en cours, ou encore sur les déplacements ou absences de certain.e.s salarié.e.s clés.

L'arnaque se déroule en deux étapes :

1. La collecte d'informations sur votre ONGD

Les escrocs vont rechercher les informations au sujet l'organisation visée sur le site Internet et les réseaux sociaux.

Les sources d'information pour les criminels sont :

- Les réseaux sociaux du personnel, de la direction et des membres du conseil d'administration
- Les calendriers partagés de l'organisation
- L'actualité de l'organisation sur les réseaux sociaux et le site web
- Les rapports annuels et comptes publiés

Grâce à ces sources, les escrocs connaissent l'organigramme de l'ONG, les absences, les congés des dirigeant.e.s et des personnes responsables des finances et peuvent ainsi identifier les moments durant lesquels l'organisation est la plus vulnérable.

Afin de préparer leur coup, ils peuvent contacter l'organisation de manière directe et entrer en contact avec les employé.e.s afin de soutirer d'autres informations plus précises comme la durée d'absence d'un.e collaborateur.ice ou des informations sur les procédures de paiement.

Il arrive également que les criminels piratent un compte de courrier électronique d'un membre de l'organisation afin de collecter les données d'un carnet d'adresses ou pour avoir accès à des informations partagées dans les échanges de mails. Le fait de posséder ces informations leur permettra de gagner la confiance de la personne cible.

Grâce à toutes ces informations, les escrocs pourront déterminer un scénario optimal pour mener à bien leur action.

2. La prise de contact et la manipulation

La deuxième étape va consister en la prise de contact avec la ou les personnes clés de l'organisation qui seront la cible de leur action. Ils prendront contact par téléphone ou par courrier électronique avec pour intention de les inciter à faire un virement vers un compte extérieur à l'organisation.

Le prétexte souvent utilisé par les criminels est celui de l'urgence de faire un virement afin de répondre à un besoin particulier et vital pour l'organisation ou pour le bon déroulement d'une activité importante pour l'ONG.

Le moment choisi pour l'attaque coïncide souvent avec l'absence d'une personne clé de l'organisation, pendant les vacances ou son absence prolongée. Ce contexte doit amener la personne cible à agir de façon exceptionnelle, quitte à enfreindre les procédures en place, pour faire face à une situation inhabituelle.

L'escroc peut lancer une attaque en envoyant un message depuis une adresse mail interne à l'organisation en piratant l'adresse mail d'un membre de l'équipe ou du conseil d'administration ou en utilisant une adresse email privée au nom, par exemple, d'une personne du CA ou de la direction.

L'attaque peut également se faire via un appel téléphonique.



Les criminels adaptent leurs contenus au contexte et organisent maintenant leurs attaques en luxembourgeois !

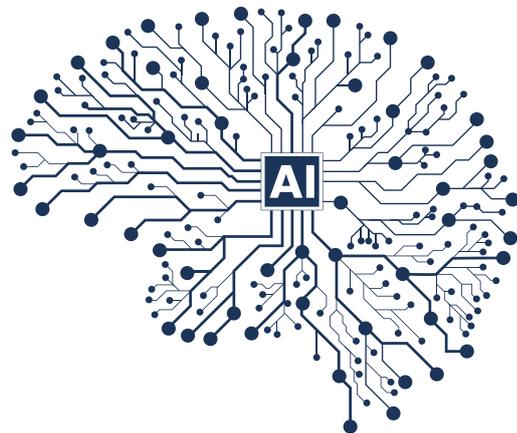
Et ass geheim, dofir benotzen
ech meng privat Adress

Eis Firma huet seng
Bankdetailler geännert

Maacht w.e.g. den Transfer
sou séier wéi méiglech, et ass
ganz dréngend



Il faut être plus vigilant.e que jamais : une vulnérabilité accrue face aux arnaques à cause de l'intelligence artificielle



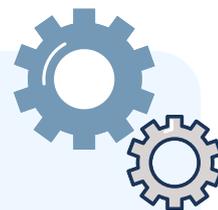
L'intelligence artificielle (IA) augmente considérablement la capacité d'action des criminels :

Grâce aux technologies d'IA générative, il est désormais possible d'imiter ou d'utiliser la voix, l'image ou le style d'une personne du CA ou de la direction d'ONG avec une grande vraisemblance. Cela permet aux fraudeurs de créer des messages vocaux, des vidéos, ou des e-mails trompeurs.

l'IA est aussi capable de falsifier des documents officiels tels que des ordres de virement, des factures, ou des devis. Des outils basés sur l'IA peuvent générer en quelques secondes des documents crédibles, avec des logos, signatures numériques et mentions légales identiques à ceux de l'organisation, d'une personne de confiance (Avocat, ministère) ou d'un fournisseur.

L'automatisation offerte par l'IA permet aussi aux fraudeurs de mener des attaques plus ciblées, plus facilement : elle analyse en quelques secondes les réseaux sociaux, les publications de l'ONGD et identifie les maillons faibles dans l'organigramme. En combinant toutes ces informations, les escrocs peuvent orchestrer rapidement des scénarios plus réalistes et mieux personnalisés.

La boîte à outils des escrocs :



Les faux appels téléphoniques



Les faux ordres de virement



La demande de données sensibles



Fausse facture ou demande de changement du RIB par un fournisseur



Le faux technicien



Le deepfake

- **Les faux appels téléphoniques**

Les fraudeurs utilisent des techniques de manipulation vocale pour imiter la voix d'une personne en charge de la direction ou de la coordination ou membre du CA et convaincre un.e employé.e de divulguer des informations confidentielles ou d'effectuer des actions frauduleuses. La personne peut également se faire passer pour un prestataire ou un bailleur de fonds.

- **Les faux ordres de virement**

Un criminel se fait passer pour la direction, la personne responsable des finances ou un membre du conseil d'administration et envoie un e-mail urgent à un.e employé.e du service financier ou gestionnaire financier demandant le transfert de fonds vers un compte bancaire créé par les fraudeurs. Le mail présente souvent des anomalies qui sont parfois difficiles à déceler (et le seront de plus en plus grâce à l'IA) : le nom de la personne qui expédie le mail est conforme, mais l'adresse mail utilisée comporte des erreurs, le nom de domaine est différent.

- **La demande de données sensibles**

L'escroc se fait passer pour membres du CA ou la direction de l'ONG et contacte un.e collaborateur.ice du service informatique ou des ressources humaines, demandant l'envoi de données sensibles (informations de connexion, données bancaires, fiches de paie, etc).

- **Fausse facture ou demande de changement du relevé d'identité bancaire (RIB) par un fournisseur**

Les criminels utilisent également des documents falsifiés tels que des ordres de virement, factures, etc. comme justificatifs pour déclencher des transactions frauduleuses. Ils peuvent se faire passer pour un des fournisseurs de l'ONGD ou un bailleur et exiger le paiement de factures ou de remboursements sur un autre compte bancaire que celui utilisé habituellement. L'émission de fausses factures est une autre technique et se base sur l'envoi d'une fausse facture éditée au nom d'un prestataire de l'ONG et envoyée par la poste ou électroniquement avec un RIB changé.

- **Le faux technicien**

Un faux technicien informatique peut contacter l'organisation, en prétextant une mise à jour à réaliser ou un outil à installer et demande de prendre la main à distance sur le poste de travail ou demande de l'information sur les accès au serveur ou ordinateurs.

- **Le deepfake**

Depuis quelque temps, des arnaques au Président utilisant l'intelligence artificielle et plus particulièrement la technologie du deepfake ont été signalées. Par exemple, lors d'une visioconférence, les escrocs "imitent" l'apparence et la voix d'une ou de plusieurs personnes pour tromper la vigilance d'un.e décisionnaire.



Recommandations : Comment éviter de tomber dans le piège ?

1) Sensibilisation du personnel

Organisez des sessions de sensibilisation et de responsabilisation du personnel, des bénévoles et des CA en présentant les manières dont les escrocs opèrent habituellement.

Il est important de les former à la détection de courriels de phishing, des demandes frauduleuses et des modes de communication inhabituels de la part de la direction ou du CA.

La sensibilisation des équipes et plus spécifiquement des responsables de communication, doit aussi expliquer les risques divulguer des informations sur le fonctionnement de l'organisation, les périodes d'absence et plus particulièrement la publication de voyages privés de responsables financiers, direction et membres du conseil d'administration.

Dans le cadre de la mise en œuvre de projets avec des partenaires locaux, il est important également de sensibiliser le partenaire qui met en œuvre le projet des risques de fraude et de l'informer sur les procédures à mettre place et sur les pratiques à adopter pour mitiger ces risques.

Prendre en compte les moments de vulnérabilité accrue de l'organisation pour faire des rappels sur les risques et sur les procédures

- Faire circuler des mails rappelant les mesures de précaution à prendre avant les périodes de vacances
- Informez régulièrement sur les différents types de fraudes et n'oubliez pas de sensibiliser systématiquement les nouvelles personnes engagées (membres du CA, les équipes, les bénévoles et les stagiaires)

2) Développer au sein de votre organisation un cadre sécurisé pour éviter les fraudes

Elaborer un cadre sécurisé pour la gestion financière :

Mettez en place des procédures de validation à plusieurs niveaux, notamment pour les transactions financières et les demandes de données sensibles. Vous pouvez par exemple demander l'approbation de plusieurs personnes ou une double vérification.

Idéalement, la procédure de validation interne doit garantir une distinction claire entre les fonctions de demande ou d'achat de biens et services, celles de paiement, et celles d'enregistrement comptable. La direction et le conseil d'administration doivent veiller à ce que cette séparation soit effectivement mise en œuvre. Cela permet d'éviter que des paiements non autorisés soient réalisés

Pour les petites ONGD, il est sans doute parfois difficile de réaliser une telle séparation des fonctions. D'où la nécessité pour le CA de veiller au comportement intègre de la direction et de l'équipe et de mettre en place les 3 procédures suivantes :

- **Exiger la double signature** : la bonne pratique est d'imposer la double signature pour toute transaction avec un montant à déterminer par le CA au-delà duquel cette procédure est obligatoirement requise. Cette activité nécessiterait la signature de deux personnes comme par exemple celles du trésorier et celle de la direction.
- **Vérifier régulièrement les mouvements bancaires par les personnes en charge des aspects financiers au sein de l'ONGD** (trésorier et/ou direction)
Cela peut se faire par un listing des paiements effectués ou des commandes passées. Il est conseillé de le faire de manière régulière, si possible une fois par mois. Cette vérification permet de détecter des dépenses non autorisées et des virements suspects.
- **Limiter les accès aux comptes et pièces justificatives** : les CA des ONGD et la direction doivent veiller à ce que les comptes – qu'ils soient sur support informatique ou papier – ne soient accessibles qu'aux personnes autorisées tant en écriture qu'en lecture. Cela suppose que les comptes et pièces justificatives soient conservés dans des endroits sécurisés et, en cas de support informatique, que seules les personnes autorisées y aient accès avec identification et mot de passe.

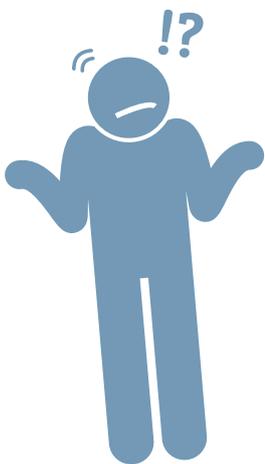
Environnement informatique sécurisé contre le piratage : il est important de mettre en place des mesures de sécurité informatique adaptées aux risques. Cela comprend l'utilisation de pare-feux, d'antivirus à jour, de filtres anti-spam et de solutions de détection d'intrusion. Les connexions aux messageries et plateformes sensibles doivent être protégées si possible par une authentification à deux facteurs et des mots de passe complexes, régulièrement renouvelés.

Le chiffrement des communications et des fichiers sensibles est aussi recommandé pour empêcher l'accès non autorisé en cas de fuite ou d'interception. Si nécessaire, il est recommandé de faire appel à un appui professionnel pour faire un état des lieux de l'environnement IT au sein de l'ONGD et adapter les outils en fonction des recommandations émises.

3) Prudence avec les « demandes urgentes » :

Lors de l'attaque, les escrocs vont concevoir un faux scénario d'urgence. Si des transactions inhabituelles sont sollicitées de manière urgente, les personnes responsables doivent redoubler de prudence et toujours vérifier l'authenticité des demandes de transfert de fonds ou sollicitation d'envoi d'informations sensibles. Pour ce faire, il faut contacter directement les personnes responsables de l'organisation (la direction ou le conseil d'administration) en utilisant le téléphone en plus du courrier électronique car l'adresse mail a pu être piratée. Osez poser des questions, même à des supérieurs hiérarchiques, et même si cela semble maladroit ou déplacé.

Dans ces contextes d'urgence, il faut considérer avec une attention particulière les transmissions inhabituelles de nouvelles coordonnées bancaires et vérifier par téléphone auprès de vos partenaires ou prestataires ces changements.



Que faire si vous êtes victime d'une arnaque au Président ou autre escroquerie ?

Voici les recommandations de la police grand ducale en cas d'escroquerie :

1) Identifiez immédiatement les transactions financières effectuées frauduleusement.

2) Limitez l'accès à vos informations et système informatique :

- Isolez et éteignez l'ordinateur concerné pour que des expert.e.s puissent réaliser une analyse approfondie.
- Désinstallez le/les logiciels que les escrocs vous auraient incité à installer.
- Modifiez tous les mots de passe, tant sur l'ordinateur que sur tous les comptes Internet même les comptes privés.
- Le cas échéant, faites examiner votre ordinateur par un spécialiste qui désinstallera tous les logiciels malveillants des fraudeurs.

3) Contactez votre organisme bancaire pour demander le blocage des mandats/demandes de paiement. Vérifiez également que les informations bancaires frauduleuses (changement de RIB, fausses factures) ne sont pas utilisées en interne.

4) Si nécessaire, bloquez votre carte de paiement en contactant immédiatement votre banque ou en appelant SIX Payment Services au numéro de téléphone (+352) 49 10 10, accessible 24h/24 et 7j/7.

Et enfin **5) Déposez une plainte officielle auprès de la police.**



Même si le dommage subi n'est pas significatif, il est important de porter plainte afin de contribuer à la prévention de l'arnaque et d'éviter que d'autres personnes tombent dans le même piège.

Collectez toutes les données qui prouvent les faits et les dommages subis. Consignez toutes les données que vous avez reçues des escrocs comme les numéros de téléphone, les noms et l'adresse du site web, et transmettez-les à la Police lors du dépôt de la plainte.

Merci de contribuer à ce document évolutif

Il s'agit d'un document évolutif et nous vous remercions pour vos commentaires et recommandations pour des améliorations futures.

Si vous avez des outils à partager ou des informations qui pourraient nous être utiles n'hésitez pas à les partager avec nous et les autres ONGD.

Vous pouvez également prévenir le Cercle de Coopération lorsque des tentatives de fraude ont lieu. Cela nous permettra éventuellement d'aviser les autres ONGD en cas de risque accru ou d'identifier de nouvelles pratiques mises en œuvre par les escrocs et d'en avertir les autres organisations.

Merci pour votre collaboration.

Pour toute question liée à ce document, merci d'adresser votre demande à :

fx.dupret@cercle.lu

Réalisation :

François-Xavier Dupret fx.dupret@cercle.lu

Mise en forme :

Pauline Philippe pauline.philippe@cercle.lu