Campagnes de messages d’escroquerie usurpant l’identité de la Police et de la Gendarmerie

Publié le 11 janv. 2022

chantage par mail message hacker boite mail

586825 Temps de lecture : 21 min

Vous avez reçu un message (mail) d’une personne prétendant appartenir à la Brigade de Protection des Mineurs (BPM) ? Ce message indique que vous vous êtes rendu coupable de plusieurs graves infractions à la loi (pédopornographie, pédophilie…) et vous informe que, sans réponse de votre part, votre dossier sera transmis aux autorités pour de possibles poursuites judiciaires ? Il mentionne également que l’affaire sera rendue publique en cas de non-réponse ? Pas de panique ! Il s’agit d’une tentative d’escroquerie qui vise à vous effrayer pour vous dérober de l’argent !

Depuis l’été 2020, Cybermalveillance.gouv.fr a identifié de nombreuses campagnes de messages d’escroquerie, toujours en cours, qui usurpent l’identité de la Police Nationale, de la Gendarmerie Nationale et, plus récemment, du service européen de Police, Europol, ou de l’organisation de police internationale, Interpol.

Cet article analyse cette menace et prodigue des conseils et des recommandations pour y faire face.

Voici deux exemples de ce type de message ci-dessous :

DIRECTION GÉNÉRALE DE LA POLICE JUDICIAIRE
DIRECTION DE PROTECTION DES MINEURES

Attention !
ARNAQUE

Paris le 05 Octobre 2020

A votre attention:

Je suis **Mme YVETTE BERTRAND**, commissaire divisionnaire, chef de la brigade de protection des mineurs (BPM), je vous contacte peu après une saisie informatique de la Cyber-infiltration (autorisée, notamment en matière de pédopornographie, pédophilie, Cyber pornographie, exhibitionniste, trafic sexuelle depuis 2014) pour vous informer que vous faites l'objet de plusieurs Poursuites Judiciaires en vigueur:

_ La pédopornographie
_ La pédophilie
_ L'exhibitionniste
_ La Cyber pornographie
_ Le trafic sexuelle

Pour votre information, La loi de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez commis les infractions après avoir été ciblé sur internet (site d'annonce), puis pendant des échanges Mails (Messagerie Instantané) avec plusieurs mineurs, les photos dénudées de vous que vous envoyez aux mineurs ont été enregistrés par notre cyber-gendarme et constituent les preuves de vos infractions.

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications pour qu'elles soient mises en examen et vérifiés afin d'évaluer les sanctions, cela dans un délai strict de 72 heures. Passé ce délai nous nous verrons dans l'obligation de transmettre notre rapport à **Mme Myriam Quéméner** procureur adjoint au tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, le transmettre à la Gendarmerie la plus proche de votre lieu de résidence pour votre arrestation et vous fiché comme délinquant sexuel, transmettre votre dossier à plusieurs chaînes de télévision nationale d'information pour une diffusion ou votre famille, vos proches et toutes la France entière verront ce que vous faites devant votre ordinateur.

Pour tous informations écrivez à cette adresse : protection.mineurs@secretary.net

Maintenant vous êtes prévenu.
Cordialement,
Mme YVETTE BERTRAND, Commissaire Divisionnaire,
Chef de la brigade de protection des mineurs (BPM)

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE
BRIGADE DE PROTECTION DES MINEURS
Adresse: 12 QUAI DE GESVRES 75004 Paris

Message frauduleux usurpant l'identité de la Police Nationale

DIRECTION GÉNÉRALE DE LA GENDARMERIE

Je suis Mr Christian RODRIGUEZ, directeur général de la gendarmerie nationale. Je vous contacte peu après une saisie informatique de cyber-infiltration (Autorisée, notamment en matière de pédopornographie, Site Pornographique, Cyber pornographie, pour vous informer que vous faites l'objet de plusieurs poursuites judiciaires en vigueur :

* LA PÉDOPORNOGRAPHIE

* SITE PORNOGRAPHIQUE

* CYBER PORNOGRAPHIE

* DÉTOURNEMENT DE MINEURS

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications afin qu'elles soient mises en examen et vérifiées de sorte à évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport

À Mme Mélanie BRIARD, substitute du procureur de la République près le tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, et vous serez fiché comme délinquant sexuel. Votre dossier sera également transmis aux médias pour une diffusion où votre famille, vos proches et toute l'Europe entière verront ce que vous faites devant votre ordinateur.

Maintenant vous êtes avertis.

Cordialement,

Directeur général de la gendarmerie nationale.

DIRECTION CENTRALE DE LA GENDARMERIE
BRIGADE DE PROTECTION DES MINEURS
Adresse : 4 rue Claude-Bernard 92130 Issy-les-Moulineaux

Message frauduleux usurpant l'identité de la Gendarmerie Nationale

1. De quoi s'agit-il ?

Les internautes victimes de cette tentative d'escroquerie reçoivent un message d'une personne qui prétend appartenir à la Brigade de Protection des Mineurs (BPM). Cette personne se présente comme « *Commissaire Divisionnaire, Chef de la BPM* ». Pour crédibiliser la démarche et la légitimité du message reçu, il est mentionné le nom de différents cadres, fictifs ou existants, de la Police Nationale, de la Gendarmerie Nationale, voire du service européen de Police, Europol, dont l'identité est usurpée tels (voir encadré en fin d'article).

Ce message indique, qu'après enquête de la « *Cyber-infiltration* », l'internaute s'est rendu coupable de différentes infractions sur des mineurs : **pédopornographie**, **pédophilie**, **exhibitionnisme**, **cyber pornographie**, **trafic se xuel**. L'escroc adopte par la suite un discours juridique en mentionnant les circonstances aggravantes relatives aux prétendus faits retenus à l'encontre de la victime et affirme disposer de preuves des infractions. La victime est menacée de poursuites judiciaires si elle ne répond pas au message dans un délai de 72 heures.

Son dossier sera alors transmis au « *Procureur adjoint du tribunal de grande instance de Créteil »,* spécialisé dans le domaine de la cybercriminalité. Là encore, toujours dans le but de crédibiliser la démarche frauduleuse, l'identité de différents cadres appartenant au ministère de la Justice, existants ou fictifs, est usurpée (voir encadré en fin d'article).

L'escroc indique également que la victime se verra établir un mandat d'arrêt à son encontre, qu'elle sera fichée comme « *délinquant sexuel* » et que le dossier sera transmis à des « *chaînes de télévision nationales d'information* » afin que les proches de la victime soient informés de ses soi-disant agissements.

Dans certains cas rapportés, et toujours dans le but de crédibiliser l'escroquerie, le message mentionne la prétendue **adresse IP de la machine de la victime** (une adresse IP est un numéro d'identification d'un équipement qui est connecté à Internet).

Enfin, l'escroc mentionne dans son message une **adresse de messagerie** (mail) pour permettre à la victime de répondre et poursuivre l'échange où il lui demandera par la suite une somme d'argent pour abandonner les charges.

2. Faut-il avoir peur et en quoi est-ce une escroquerie ?

La réponse est simple : **non !** Car il s'agit d'une simple arnaque qui vise à escroquer des victimes crédules en leur faisant peur avec de fausses accusations. Dans le cadre de ces campagnes de messages malveillants, l'objectif des escrocs est de dérober de l'argent en utilisant différents ressorts.

Tout d'abord, **un message anxiogène avec un logo officiel** fortement mis en avant, l'utilisation et l'usurpation d'identité de certains services de la Police Nationale (Brigade de Protection des Mineurs, Direction Centrale de la Police Judiciaire…), de la Gendarmerie Nationale, d'Europol et du ministère de la Justice ainsi que des faits reprochés d'une grande gravité (pédopornographie, pédophilie…).

Au niveau de l'argumentaire, **l'escroc indique détenir les preuves** des faits reprochés à la victime et utilise des termes judiciaires pour effrayer encore plus la victime, en mentionnant, par exemple, « *la loi de mars 2007* » ou bien des circonstances aggravantes pouvant être retenues dans le cadre de ce type de faits. Le message insiste sur **le caractère urgent de la réponse (72 heures)** de la victime pour ne pas être sanctionnée. Il joue également sur la peur des conséquences d'une erreur dans le cadre de l'enquête ou encore sur le sentiment de culpabilité et de honte, en menaçant que **les proches de la victime seront mis au courant des faits et que les médias en parleront.**

Par ailleurs, pour crédibiliser la démarche, les **noms de cadres de la Police Nationale et de la Gendarmerie Nationale, voire d'Europol, ainsi que du ministère de la Justice** sont mentionnés et utilisés en usurpant leur identité. Pour preuve de l'usurpation d'identité, Mme Yvette Bertrand, commissaire divisionnaire de police de la Police Nationale, a bien fait partie de la Brigade de Protection des

Mineurs (BPM) entre 1995 et 2010 mais a fait valoir ses droits à la retraite le 1er octobre 2014, comme l'indique le Journal officiel.

En outre, si le message n'a pas été envoyé par une adresse se terminant par @interieur.gouv.fr, c'est qu'il s'agit d'un message frauduleux. En effet, les administrations publiques communiqueront toujours en utilisant leur nom de domaine comme @interieur.gouv.fr pour le ministère de l'Intérieur ou bien @dgfip.finances.gouv.fr pour le service des impôts. Sur les nombreux cas rapportés de cette arnaque, aucun message ne disposait d'adresse émettrice se terminant par @interieur.gouv.fr. De même, **les adresses de messagerie auxquelles les victimes sont invitées à répondre pour poursuivre l'échange ne disposent pas, elles non plus, du nom de domaine @interieur.gouv.fr**. On peut par exemple citer protection.mineurs@secretary.net, brigadeprotectiondesmineurs33@gmail.com ou brigade.protection@post.com.

De même, l'**adresse IP** qui est parfois indiquée dans les messages reçus par les victimes, par exemple 146.29.7.458, est très souvent farfelue. En effet, les nombres qui constituent une adresse IP réelle ne dépassent jamais le nombre 255, ce qui n'est pas le cas dans l'exemple d'adresse IP citée précédemment.

À noter que ce message contient de nombreuses fautes de présentation et d'orthographe inhabituelles pour un courrier officiel et qui pourraient éveiller l'attention des victimes. Par exemple, *« Brigade de protections des mineurEs »* au lieu de *« Brigade de protection des mineurs »*.

Enfin, la Préfecture de Police de Paris et la Gendarmerie Nationale ont récemment communiqué sur les réseaux sociaux sur cette campagne de messages d'escroquerie usurpant l'identité de la Brigade de Protection des Mineurs :

Préfecture de Police
@prefpolice

📢 Rappel 📢 De faux mails de la Brigade de protection des mineurs (BPM) circulent toujours !
Une enquête est en cours :
❌ Ne répondez pas à ces mails
❌ Ne les relayez pas sur les réseaux sociaux

Comment savoir si le courriel est frauduleux ? La réponse ci-dessous 👇

> **Préfecture de Police** @prefpolice · 1 oct.
> ⚠️ Attention de faux mails de la Brigade de protection des mineurs (BPM) ont été recensés !
> Si le mail n'a PAS été envoyé par une adresse se terminant par @ interieur.gouv.fr
> ➡️ mail frauduleux !
>
> N'appelez pas la BPM, des investigations sont déjà en cours.

Twitter : https://twitter.com/prefpolice/status/1323210514600763393
Facebook : https://www.facebook.com/prefecturedepolice/posts/5457159684309529

Tous ces éléments tendent ainsi à démontrer que ces messages ne sont que des tentatives d'arnaques. Autrement dit, si vous recevez un tel message de chantage et que vous n'y donnez pas suite, il ne se passera certainement rien de plus.

3. Comment ont-ils pu avoir mon adresse de messagerie ?

Pour obtenir votre adresse de messagerie et vous envoyer ces messages frauduleux, **les escrocs peuvent recourir à différentes méthodes comme l'hameçonnage** (*phishing* en anglais), qui est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des informations personnelles (informations d'identité, mots de passe…) en lui envoyant un message usurpant l'identité d'un tiers de confiance.

Par ailleurs**, votre adresse de messagerie circule déjà sur Internet**. En effet, vous l'utilisez régulièrement sur différents sites Internet pour vous identifier et communiquer. Ces sites ont parfois revendu ou échangé leurs fichiers d'adresses de messagerie avec différents partenaires plus ou moins scrupuleux dans des objectifs marketing. **Ces fichiers d'adresses sont parfois également récupérés par des cybercriminels** pour pouvoir être utilisés dans des campagnes publicitaires frauduleuses, pour des attaques par hameçonnage, ou pour ce type de campagnes de messages d'escroquerie.

Les informations dérobées circulent entre cybercriminels sous forme de fichiers qu'ils s'échangent ou se revendent.

4. Que faut-il faire si on reçoit ce type de message ?

1. **Ne paniquez pas !** En effet, vous n'avez sans doute rien de réellement compromettant à vous reprocher. Par ailleurs, la consultation de sites pornographiques, dans le respect de la loi, n'est pas répréhensible.

2. **Ne répondez pas !** Car cela montrerait aux cybercriminels que votre adresse de messagerie est « valide » et que vous portez de l'intérêt au message d'escroquerie qu'ils vous ont envoyé.

3. **Conservez les preuves !** Le message reçu pourra vous servir pour signaler cette tentative d'escroquerie aux autorités.

4. **Signalez la tentative d'escroquerie** dans le cadre de l'enquête ouverte par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) du ministère de l'Intérieur. Pour cela, transférez le message reçu à l'adresse suivante : fraude-bretic@interieur.gouv.fr.

5. Et si vous avez donné suite à l'arnaque et avez payé ?

1. **Rassemblez les preuves !** Conservez le message reçu, les échanges avec l'escroc ainsi que toute autre information que vous avez pu collecter et qui pourra vous servir pour déposer plainte auprès des autorités.

2. **Déposez plainte** au commissariat de police ou à la brigade de gendarmerie ou encore par écrit au procureur de la République du tribunal judiciaire dont vous dépendez en fournissant toutes les preuves en votre possession.
   Vous pouvez être accompagné gratuitement dans cette démarche par une association de France Victimes au 116 006 (appel et service gratuits), numéro d'aide aux victimes du ministère de la Justice. Service ouvert 7 jours sur 7 de 9h à 19h.

3. **Contactez votre banque** pour essayer de vous faire rembourser. Certaines banques exigeront la preuve du dépôt de plainte pour instruire votre demande.

L'infraction suivante peut être retenue :

Escroquerie (article 313-1 du code pénal) : l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien

quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.

6. Comment se prémunir de ce type de messages ?

1. **Soyez vigilant lorsque vous communiquez votre adresse de messagerie** à des tiers.

2. **Ne répondez pas aux messages dont vous ne connaissez pas l'expéditeur.** Vous éviterez ainsi de le renseigner sur la validité de votre adresse de messagerie.

3. **Évitez les sites non sûrs ou illicites** tels ceux hébergeant des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

4. **N'ouvrez pas les courriels ou leurs pièces jointes et ne cliquez jamais sur les liens** provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu, mais dont le contenu du message est inhabituel ou vide. Consultez nos conseils sur l'hameçonnage (*phishing* en anglais).

5. **Ne communiquez jamais d'informations sensibles** (informations d'identité…) par messagerie, par téléphone ou sur Internet.

6. **Utilisez des mots de passe différents et complexes pour chaque site et application** utilisés pour éviter que, si un compte est piraté, les cybercriminels puissent accéder aux autres comptes utilisant ce même mot de passe.

7. **Vérifiez l'adresse du site qui s'affiche dans votre navigateur.** Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.

8. **Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien** (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

9. **Soyez vigilant lorsque vous répondez à des formulaires d'inscription, des bons de commande ou participez à des jeux concours** : certains acteurs n'appliquent pas toujours les bonnes pratiques et votre adresse de messagerie pourrait figurer dans des bases de données à votre insu. Vérifiez la fiabilité d'une marque avant d'accorder votre consentement pour éviter que votre adresse de messagerie ne soit communiquée à des tiers.

7. Besoin de plus de conseils ?

Pour être conseillé dans vos démarches, contactez au besoin la plateforme Info Escroqueries du ministère de l'Intérieur au 0 805 805 817 (appel et service gratuits). Le service est ouvert de 9h à 18h30 du lundi au vendredi.

Exemple de message reçu par des victimes :

DIRECTION GÉNÉRALE DE LA POLICE JUDICIAIRE
DIRECTION DE PROTECTION DES MINEURES

Paris le 05 Octobre 2020
A votre attention:

Je suis Mme Yvette BERTRAND, commissaire divisionnaire, chef de la brigade de protection des mineurs (BPM), je vous contacte peu après une saisie informatique de la Cyber-infiltration (autorisée, notamment en matière de pédopornographie, pédophilie, Cyber pornographie, exhibitionniste, trafic sexuelle depuis 2014) pour vous informer que vous faites l'objet de plusieurs Poursuites Judiciaires en vigueur:
– La pédopornographie
– La pédophilie
– L'exhibitionniste
– La Cyber pornographie
– Le trafic sexuelle

Pour votre information, La loi de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez commis les infractions après avoir été ciblé sur internet (site d'annonce), puis pendant des échanges Mails (Messagerie Instantané) avec plusieurs mineurs, les photos dénudées de vous que vous envoyez aux mineurs ont été enregistrés par notre cyber-gendarme et constituent les preuves de vos infractions.

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications pour qu'elles soient mises en examen et vérifiés afin d'évaluer les sanctions, cela dans un délai strict de 72 heures. Passé ce délai nous nous verrons dans l'obligation de transmettre notre rapport à Mme
Myriam QUÉMÉNER, procureur adjoint au tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, le transmettre à la Gendarmerie la plus proche de votre lieu de résidence pour votre arrestation et vous fiché comme délinquant sexuel, transmettre votre dossier à plusieurs chaînes de télévision nationale d'information pour une diffusion ou votre famille, vos proches et toutes la France entière verront ce que vous faites devant votre ordinateur.

Pour tous informations écrivez à cette adresse : protection.mineurs@secretary.net
Maintenant vous êtes prévenu.
Cordialement,
Yvette BERTRAND, Commissaire Divisionnaire,
Chef de la brigade de protection des mineurs (BPM)

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE
BRIGADE DE PROTECTION DES MINEURS
Adresse: 12 QUAI DE GESVRES 75004 Paris

Liste des personnels, fictifs ou existants, de la Police Nationale, de la Gendarmerie Nationale, d'Europol et du ministère de la Justice dont l'identité est usurpée :

- **Jean-Michel ALDEBERT**
- **Hugo ARER**
- **Mireille BALLESTRAZZI**
- **Fabien BASQUIN**
- **Solange BASTIDES**
- **Laure BECCUAU**
- **Véronique BECHU**
- **Anne BENEJEAN**
- **Christine BERNIER**
- **Yvette BERTRAND**
- **Christine BOBET**
- **Marc BOGET**
- **Catherine DE BOLLE**
- **Catherine BONNET**
- **Jérôme BONET**
- **Mélanie BRIARD**
- **Bruno BUSSENET**
- **Maryvonne CAILLIBOTTE**
- **Karine CHABOT**
- **Patrick CHAUDET**
- **Chantal CLAVIJO**

- **Philippe COLMAR**
- **Véronique DEGERMANN**
- **Laurence DELAUTEL**
- **Véronique DELCOURT**
- **Céline DUMONT**
- **Bertrand DUPLEX**
- **Martine DUPUIS**
- **Vianney DYEVRE**
- **Jacqueline FOURNIER**
- **Éric FREYSSINET**
- **Marc GUIRIMAND**
- **Sabine HAEUBLEIN**
- **Rémy HEITZ**
- **Jérôme KASPARIAN**
- **Stéphane LAPEYRE**
- **Jean-Philippe LECOUFFE**
- **Richard LIZUREY**
- **Jean-Pierre LONGIN**
- **François-Xavier Masson**
- **Éric MAUREL**
- **Jean-Philippe MESCLE**
- **Marc DE MESMAEKER**
- **Christophe MOLMY**
- **Jean-Dominique NOLLET**
- **Emmanuelle OSTER**
- **Isabelle PARNETTI**
- **Louis PAUTY**
- **Brigitte PERONNET**
- **Catherine PONTHIER**
- **Sébastien POSSEMÉ**

- **Myriam QUÉMÉNER**
- **Christian RODRIGUEZ**
- **Christian SAINTÉ**
- **M. Jürgen STOCK**
- **Bernard THIBAUD**
- **Patrick TOURON**
- **Frédéric VEAUX**
- **Brigitte VERNET**