MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

LA LETTRE CYBER en Région Grand Est

Gendarmerie nationale

GENDARMERIE

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

JANVIER 2025

LA THEMATIQUE DU MOIS:
Réseaux sociaux + Intelligence Artificielle = des escroqueries de plus en plus élaborées

Escroquerie, Intelligence Artificielle, ordre de virement, réseaux sociaux, évolution, social engineering, ce sont des termes que vous avez déjà vus dans nos lettres cyber passées mais imaginez : on combine tout ça pour réaliser une escroquerie, est ce que ça peut marcher ? Bien sûr que NON : on a été avertis, on ne se fait plus avoir !! On s'assure que notre interlocuteur est bien le bon !!

Oui mais les escrocs le savent et comme on le répète sans relâche, ils ne s'arrêtent jamais et cherchent toujours à évoluer… Ils profitent donc des évolutions technologiques, et même des actions préventives que nous pouvons mettre en place, pour les tourner à leur avantage.

Nous allons voir comment les escrocs profitent d'absolument tout ce qui pourrait leur être profitable et à quel point notre vigilance ne doit JAMAIS baisser.

« Arnaque au président »

L'arnaque au président consiste à manipuler une personne non décisionnaire dans une entreprise afin de l'amener à réaliser un virement bancaire important en prétextant généralement une urgence de commande ou encore un changement de RIB. Pour cette arnaque, pas de souci, « on a été avertis, on vérifie bien notre interlocuteur et on s'assure que le virement est légitime »

Oui mais qu'en est-il si c'est le PDG, ou tout autre collaborateur légitime « EN PERSONNE » qui vous le demande ?

Oui mais les escrocs connaissent notre vigilance, connaissent les points sur lesquels porter notre attention... alors pour continuer leurs méfaits, ils profitent de cela et se réinventent en profitant des évolutions technologiques.

Que peut on faire avec l'Intelligence Artificielle? (IA)

Connaissez-vous les DeepFake ?
Vous en avez entendu parler, même si vous ne savez pas exactement de quoi il s'agit..
Il est désormais très facile de créer une vidéo dans laquelle notre visage est remplacé par un visage connu récupéré à partir d'une photo ou d'une vidéo. Certaines applications mobiles le permettent déjà grâce à (ou à cause de) l'évolution de l'intelligence Artificielle. Les effets sont de plus en plus réalistes et élaborés. Mieux encore, il est également possible de reproduire la voix d'une personne que vous auriez au téléphone !

Suis-je en sécurité avec une messagerie chiffrée comme Whatsapp ou Signal par exemple?

Sans rentrer dans les détails, ces applications garantissent le chiffrement de bout en bout des messages et des appels passés. C'est-à-dire que seuls l'expéditeur et le destinataire peuvent les lire. Aucune autre personne n'est en mesure de déchiffrer ces messages.

Cela permet évidemment de garantir une certaine confidentialité des échanges entre deux personnes.

Mais alors imaginez !! Votre patron, comptable ou tout autre personne légitime vous contacte via une de ces messageries !! Aucun doute, votre vigilance redescend automatiquement, surtout si c'est sa voix, ou mieux encore son visage qui apparaît à l'écran. Ok, je fais le virement…

Cas Concret

Vous voyez ou je veux en venir n'est-ce pas ? Combinez l'IA, les nouveaux modes de communications, en y ajoutant un peu d'ingénierie sociale et le tour est joué. C'est ce qui est arrivé à plusieurs entreprises ces derniers temps. Des faits qui nous ont été remontés par une ancienne camarade que nous remercions pour ce témoignage.

Les escrocs se renseignent sur l'architecture de l'entreprise, sur le rôle de chacun, récupèrent des numéros de téléphone, visages, ou même les voix des dirigeants etc… puis contactent la bonne personne (victime) via une messagerie « de confiance » en usurpant l'identité du dirigeant choisi. Ils profitent d'un éventuel manque de vigilance dû à la pseudo-sécurité qu'apporte le cryptage de la messagerie, ou encore le fait de reconnaître son dirigeant, son compte, sa photo de profil, sa voix, son image…

On ne peut plus faire confiance à quelque chose d'aussi factuel dans la mesure où c'est devenu manipulable avec à l'IA.

Quelques conseils

- Globalement il est important de mettre en place une procédure de **validation** de virement en interne. Cette procédure doit pouvoir prendre en compte tout type de demande (envoi de nouveau RIB, appel téléphonique, messagerie chiffrée etc…), doit être mise en œuvre par n'importe quel collaborateur indépendamment de sa fonction et doit pouvoir être appliquée en tout temps et en toute circonstance (même un vendredi soir à 17h55 quand les décideurs sont en vol pour un séminaire...)
- Veillez également à vos interlocuteurs, quels qu'ils soient, sur ces messageries que l'on pense sécurisées. Si la transmission des messages l'est effectivement, les utilisateurs, eux, ne sont pas vérifiés... L'utilisateur doit dans tous les cas savoir maîtriser les informations communiquées selon leur degré d'importance et de confidentialité.
- Ne baissez jamais en vigilance, et sans rentrer dans une paranoïa accrue, gardez en tête que les escrocs peuvent tout tenter pour arriver à leurs fins.

+ D'INFOS

ANJ AUTORITÉ NATIONALE DES JEUX

Grand Est Cybersécurité — CENTRE D'ASSISTANCE DE PROXIMITÉ — 0 970 512 525

CYBER MALVEILLANCE .GOUV.FR

PHAROS — PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

e-Enfance 3018

CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

ANSSI Agence nationale de la sécurité des systèmes d'information

Région de gendarmerie du Grand Est
LA LETTRE CYBER en région Grand Est

Directeur de la publication: GCA O.KIM
Responsable éditorial: COL L. GRAU
Rédacteur: ADJ M.KNOBLOCH

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
Laurent.grau@gendarmerie.interieur.gouv.fr
Mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie: