La MInute Cyber 12

©REPUBLIK-IT

LA PRÉVENTION RÉCOMPENSÉE

Ces dernières semaines, le Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI), à travers son Département de la prévention et de la cyber-résilience, a vu ses actions de prévention être primées à trois reprises.

À l'occasion de la 12e édition du Mois de l'Innovation publique du ministère de l'Intérieur, organisée par la Direction interministérielle de la transformation publique (DITP) du 3 au 29 novembre 2025, le COMCYBER-MI s'est tout d'abord illustré dans la catégorie Innovation technologique. En effet, lors de ce rendez-vous annuel, valorisant initiatives locales et capacité d'innovation des acteurs publics, le COMCYBER-MI a décroché le prix de la meilleure affiche dans la catégorie Innovation technologique, pour son projet MI-FORTNITE Expérience – Cyber_Sanctuaire. Il s'agit d'une carte inspirée du jeu vidéo le plus joué au monde, Fortnite, et certifié PEGI 3, alliant conseils de prévention et informations pratiques en lien avec la cyber. À l'heure où les cybermenaces dépassent le champ des traditionnels réseaux sociaux pour se développer dans d'autres univers, tels que les jeux vidéos en ligne, cette innovation s'inscrit donc pleinement dans la sensibilisation des gamers et des jeunes personnes particulièrement ciblées par les cybercriminels. Cette récompense a été reçue lundi 24 novembre 2025, à l'hôtel de Beauvau, des mains de Monsieur le Préfet Hugues Moutouh, secrétaire général du ministère de l'Intérieur.

Le même jour, lors de cette 5e édition de la Nuit de la Cybersécurité (CyberNight), ayant rassemblé un millier de professionnels au Théâtre Mogador, à Paris, afin de célébrer les réalisations les plus marquantes dans cinq catégories, le projet MI-FORTNITE Expérience, créé et développé par l'adjudant Frédéric Hommel, a de nouveau été primé. Aux côtés de prestigieux candidats (Vinci, Schneider Electric, le ministère de la Santé, des Familles, de l'Autonomie et des Personnes handicapées, et le ministère du Travail et des Solidarités), cette initiative a en effet remporté l'adhésion du jury, et décroché la médaille d'or dans la catégorie Projets – Initiatives.

Enfin, à l'occasion de la 5e édition des Rencontres AGIR, événement phare dédié à l'innovation qui s'est tenu mardi 2 décembre au Beffroi de Montrouge (92), le projet MI-FORTNITE Expérience a reçu une troisième récompense. Ce salon unique, soutenu notamment par le GICAT, a permis à 100 porteurs de projets et 400 entreprises d'échanger, et de rapprocher les besoins opérationnels des administrations publiques avec les solutions innovantes des acteurs de l'industrie, des start-ups et de la recherche.

Après avoir été présenté au Directeur Général de la Gendarmerie Nationale, le général d'armée Hubert Bonneau, MI-FORTNITE Expérience a donc été mis à l'honneur devant plus de 800 participants, dont 9 délégations internationales, à travers le 1er Prix de la prévention et de l'innovation gendarmerie.

Trois distinctions qui soulignent pleinement l'importance de la prévention et de l'inventivité, et qui illustrent la mobilisation de tout un service.

Le vishing, une attaque de plus en plus utilisée par les cybercriminels

Le *vishing* (de l'anglais *voice phishing* ou « hameçonnage vocal ») est une technique d'ingénierie sociale, qui leurre les victimes en les incitant à divulguer des informations sensibles ou à installer un logiciel malveillant sur leur poste informatique.

Les cybercriminels collectent des informations sur leur future victime *via* ses réseaux sociaux, Internet ou des bases de données ayant « fuité ». S'ensuit un contact téléphonique, au cours duquel l'attaquant usurpe l'identité d'une personne ou d'une organisation de confiance (banque, support informatique, etc.), et fait état d'une situation d'urgence, afin d'inciter la victime à lui fournir des informations sensibles, comme ses données d'état civil, ses identifiants, codes personnels, mots de passe, informations bancaires. Grâce à ces informations, les cybercriminels peuvent ensuite initier des opérations frauduleuses ou usurper l'identité des victimes. Dans certains cas, l'acteur malveillant peut également pousser la victime à installer un logiciel tiers, compromettant ses terminaux numériques.

Le *vishing* prospère lorsque les cybercriminels ont un minimum d'informations concernant les centres d'intérêts de l'utilisateur. Ils exploitent ces connaissances pour créer un sentiment d'urgence impliquant un problème chez la victime, puis ils interviennent en proposant une solution simple et en se montrant apaisants.

Pour se prémunir de cette délinquance, l'éducation et la sensibilisation constituent la première ligne de défense. Il s'agit, par exemple, de se rappeler qu'aucune organisation légitime ne sollicite ses clients pour obtenir des données sensibles par téléphone sans vérification préalable. Adopter les bons réflexes est également primordial, notamment en vérifiant le numéro d'appel, en installant des solutions de sécurité, mais aussi en mettant en place une identification forte.

Une fiche cyber du COMCYBER-MI, consacrée à ce phénomène, sera publiée prochainement.

Article de blog – Trend Micro : trendmicro.com
Article de blog – Orange : pro.orange.fr

L'activité internationale du COMCYBER-MI

Au mois de novembre, l'adjoint au chef du département prévention & cyber-résilience, le capitaine Michaël Tourbier, s'est rendu à Dakar au Sénégal pour dispenser une formation au profit de policiers et de gendarmes sénégalais. Plusieurs enjeux forts en matière de lutte contre la cybercriminalité ont ainsi été abordés, donnant lieu à des échanges particulièrement riches : l'état des phénomènes cybercriminels, une présentation des méthodes et outils utilisés en France (accueil des victimes, appui aux enquêteurs, etc.), et des clés pour réagir en cas de cyber-attaques. Cette semaine de formation constituait en quelque sorte le prélude à des actions spécifiques du COMCYBER-MI en matière de lutte contre les fraudes en ligne en Afrique, dans un cadre européen.

Par la suite, le COMCYBER-MI a accueilli une délégation roumaine menée par l'Inspecteur général de la police locale, M. Benone-Marian Matei. Outre une présentation générale de l'écosystème cyber français, les échanges qui ont ponctué cette rencontre se sont portés sur l'état de la menace en matière de cybercriminalité, le renforcement capacitaire et la formation.

Enfin, le COMCYBER-MI a reçu le Directeur de la lutte contre la cybercriminalité d'Interpol, M. Neal Jetton. Des échanges particulièrement fructueux ont permis de dresser un état partagé de l'état de la menace cybercriminelle, et d'aborder l'activité du COMCYBER-MI dans le domaine du renseignement cybercriminel. Dans ce domaine, de solides perspectives d'approfondissement des échanges entre les deux structures ont été identifiées.

POUR ALLER + LOIN…

Rénovation de LRPGN

À l'occasion du salon AGIR, *AEF* rapporte que la Gendarmerie nationale rénove son logiciel de rédaction de procédures, LRPGN, afin d'offrir un produit avec les technologies du moment, comme l'Intelligence Artificielle (IA). Plusieurs besoins ont ainsi été identifiés par les enquêteurs pour synthétiser les procédures, retranscrire la parole, aider la rédaction de procès-verbaux ou détecter des vices, l'objectif étant de simplifier le quotidien et gagner du temps.

À l'occasion d'entretiens avec des personnels de différents services, ces derniers ont priorisé la mise en place d'un assistant de consultation procédurale, afin de synthétiser des procédures volumineuses. Les enquêteurs de la gendarmerie ont également évoqué les outils de retranscription automatique comme le *« speech-to-text »*, mais aussi d'assistance à la rédaction de procès-verbaux, notamment ceux de transport, parmi les plus fréquents et énergivores, ou encore de détection des vices de procédure.

Toutefois, ce recours aux nouvelles technologies ne saurait réduire le rôle du gendarme qui reste « toujours maître de valider ce que l'outil, [dont l'IA], lui propose », a indiqué le colonel Anthony Mimouni, directeur de programme. La gendarmerie espère une « première brique de logiciel rénové en 2027 », a-t-il précisé.

Transition post-quantique

L'industrie de la cybersécurité française franchit un cap stratégique avec la coopération entre Thales et le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), deux organismes habilités par l'ANSSI en tant que Centres d'Évaluation de la Sécurité des Technologies de l'Information (CESTI), qui ont inauguré une coopération inédite dans la préparation de la migration sécurisée des systèmes face à l'informatique quantique.

Leur projet baptisé « Giverny », présenté à l'European Cyber Week 2025, positionne ainsi l'écosystème national comme référence face à la menace des futurs ordinateurs quantiques capables de casser les schémas cryptographiques. Les experts en cryptographie de Thales et du CEA ont ainsi réalisé une première évaluation conjointe de deux algorithmes, HAWK et FAEST, et soumis ces derniers à des scénarios d'attaque réalistes.

Cette collaboration vise à anticiper les exigences du schéma européen de certification EUCC, et à préparer le tissu industriel à l'échéance fixée par l'ANSSI. Dès 2027, tous les produits sensibles visant une qualification devront en effet adopter des algorithmes post-quantiques, une obligation étendue à l'ensemble des solutions commercialisées après 2030. À terme, il s'agira d'offrir aux entreprises, administrations et fournisseurs de services, des garanties accrues de résilience face à la menace quantique.

Publication mensuelle éditée par :
Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 12 - DÉCEMBRE 2025
Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : LCL S. LAMBERT - LCL M. TETU - CEN M. MALET - CEN N. PETITPAS
Conception graphique et maquettage : Mme M. BARREAU

En attendant le prochain numéro de La MInute Cyber, suivez notre actualité :

sur LinkedIn et sur X (ex-Twitter) :
@ComCyberMI