COMMUNIQUÉ DE PRESSE

Paris, le 22/09/2022

CYBERMOI/S 2022 : AGIR ENSEMBLE FACE AUX RANCONGICIELS

Alors que nous sommes de plus en plus connectés, et que nous utilisons nos outils numériques chaque jour pour échanger (e-mails), partager (réseaux sociaux) et acheter (e-commerce), nous avons tendance à baisser notre garde face aux dangers latents. Offre alléchante, fenêtre de réponse limitée dans le temps, pièce jointe à télécharger ou lien de redirection… Nous avons toutes et tous reçu au moins une fois un e-mail frauduleux. Ces attaques, appelées hameçonnage ou phishing en anglais, visent entreprises comme particuliers afin de récupérer vos informations personnelles (mots de passe, codes d'accès en ligne, informations personnelles ou bancaires, etc.) ou à s'introduire dans votre réseau pour y placer un logiciel malveillant : un rançongiciel. Comment se protéger de ce type d'attaque sans pour autant sombrer dans la paranoïa ? Pour sa 4ème édition pendant tout le mois d'octobre, le Cybermoi/s partage des astuces simples pour vous aider à vous prémunir.

Se poser les bonnes questions et avoir les réponses adaptées

Vous recevez un e-mail ou un SMS que vous n'avez pas sollicité ? Appelez votre interlocuteur habituel plutôt que de faire confiance au numéro inscrit dans celui-ci. Tout vous semble normal, mais vous avez un petit doute ? Vérifiez l'adresse de l'expéditeur en cliquant dessus. Il est facile d'en faire apparaître une fausse. Tout vous semble normal, mais on vous demande de cliquer sur un lien ? Tapez vous-même l'adresse du site dans votre navigateur plutôt que de cliquer sur celui-ci. Les pirates redoublent de créativité et de professionnalisme. Leurs tentatives d'hameçonnage peuvent paraître plus vraies que nature. Un seul mot d'ordre si vous n'attendez pas d'e-mail, et si celui-ci contient une pièce jointe ou un lien : prudence !

Rançongiciels : sauvegardes et Plan de Continuité d'Activité

Que l'on travaille dans une TPE/PME, un grand groupe ou une administration, nous devons tous nous préparer face aux risques de rançongiciels. Si vous êtes dirigeant, outre l'importance de sensibiliser l'ensemble de vos collaborateurs aux risques posés par les rançongiciels et leur apporter des outils pour s'en prémunir, vous devez également vous assurer de :

- posséder des sauvegardes automatiques, et elles sont déconnectées du réseau ;
- tester vos sauvegardes de manière régulière ;
- avoir préparé un plan de continuité d'activité (PCA) ;
- avoir mis en place une cellule de crise ;
- exercer votre dispositif de crise.

Une attaque = un signalement

Vous êtes un particulier victime d'une tentative d'hameçonnage ? Signalez le mail grâce à votre boîte de messagerie, et trouvez de l'aide auprès de cybermalveillance.gouv.fr.
Vous êtes une entreprise ou une administration et victime d'un rançongiciel ? Mettez en place vos mesures de remédiation et votre dispositif de crise, puis alertez les autorités compétentes (police, gendarmerie, ANSSI) avant de chercher une assistance technique.

Cybermoi/s : une campagne réunissant acteurs publics, privés et associatifs

Pendant tout le mois d'octobre, nous nous mobilisons aux côtés de nombreuses entités afin de vous proposer un programme ambitieux et pédagogique, dans la vie personnelle comme professionnelle. Vous souhaitez devenir un acteur du Cybermoi/s pour sensibiliser votre entourage, familial ou professionnel aux enjeux de la sécurité du numérique ? Consultez les kits et ressources pédagogiques mis à disposition : affiches, posters, BD et kit de communication comprenant signature mail et bannières réseaux sociaux. Suivez et relayez la campagne tout au long du mois sur les réseaux sociaux avec le #Cybermois !

Derrière les contenus et événements créés à l'occasion du Cybermoi/s se trouve un groupe de travail co-piloté par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et Cybermalveillance.gouv.fr. Le Cybermoi/s regroupe une vingtaine d'entités, essentiellement des ministères, associations et organisations professionnelles, mais aussi des acteurs privés, qui travaillent tout au long de l'année afin de vous offrir des ressources clés en main qui renforceront vos mécanismes de défense face aux dangers des espaces numériques.

Lancé en France en 2019, le Cybermoi/s est la déclinaison de la campagne européenne *European Cybersecurity Month* (ECSM), portée par plus d'une vingtaine de pays en Europe. L'objectif ? Aborder à plusieurs voix les défis que représente la transition numérique. Retrouvez plus d'informations sur les autres campagnes européennes et les actions de l'ENISA, l'institution européenne en charge de l'ECSM : https://cybersecuritymonth.eu/

« La sécurité numérique ne se résume pas à des questions techniques complexes, bien souvent difficilement compréhensible pour les non-experts, c'est également, voire avant tout, des pratiques simples à adopter au quotidien, chez soi comme au travail. Le Cybermoi/s est un temps utile pour prendre conscience ou approfondir ses connaissances des enjeux de sécurité numérique et partager les bons réflexes. Face aux nombreuses menaces numériques qui nous guettent continuellement, il est indispensable que nous soyons tous avertis, vigilants et responsables ! », commente Guillaume Poupard, directeur général de l'ANSSI.

« Avec des environnements extrêmement numérisés, la cybersécurité est désormais l'affaire de tous : particuliers, entreprises et collectivités. Le cybermoi/s est une excellente opportunité de faire connaître et de rappeler les bonnes pratiques à observer tout au long de l'année. Et c'est précisément le sens de la mission d'intérêt public de sensibilisation et d'assistance que nous menons au quotidien sur la plateforme cybermalveillance.gouv.fr » ajoute Jérôme Notin, Directeur Général de Cybermalveillance.gouv.fr.

À PROPOS DE L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.
L'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr - communication@ssi.gouv.fr

Contacts Presse

Roxane ROSELL

roxane.rosell@ssi.gouv.fr

06 49 21 63 80

presse@ssi.gouv.fr

À PROPOS DE CYBERMALVEILLANCE.GOUV.FR

Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace sur le territoire français. Ses publics sont les particuliers, les entreprises (hors OIV et OSE) et les collectivités territoriales. Le dispositif est piloté par une instance de coordination, le Groupement d'intérêt public (GIP) ACYMA, composé de 56 membres issus du secteur public, du privé et du domaine associatif, et qui contribuent chacun à sa mission d'intérêt général. Cybermalveillance.gouv.fr référence sur sa plateforme des professionnels en sécurité numérique, répartis sur tout le territoire français, pour venir en aide aux victimes. En 2021, Cybermalveillance.gouv.fr a assisté plus de 173 000 victimes et accueilli plus de 2,5 millions de visiteurs uniques sur sa

plateforme.

Contact presse :

Béatrice HERVIEU

07 64 69 62 88

presse@cybermalveillance.gouv.fr

PREMIÈRE MINISTRE

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES
ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

MINISTÈRE DE LA JUSTICE

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE