MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

Paris, le 27/05/2024

COMMUNIQUÉ DE PRESSE

SENSIBILISER À L'HAMEÇONNAGE SUR LES ESPACES NUMÉRIQUES DE TRAVAIL : LANCEMENT DE L'OPERATION CACTUS

Face aux nombreux actes de malveillances qui ont touché les espaces numériques de travail (ENT) ces derniers mois, les autorités françaises en charge des sujets de cybersécurité ont souhaité mener une action de prévention collective forte pour responsabiliser les jeunes aux enjeux de cybersécurité.

Une opération de sensibilisation en direction d'une cible particulièrement exposée

Ces derniers mois, les établissements scolaires ont été victimes d'une série d'attaques particulièrement malveillantes, via les espaces numériques de travail (ENT) des élèves. Ces actions cybercriminelles ont ainsi entraîné une atmosphère anxiogène et une perturbation des enseignements, conduisant la ministre à décider une fermeture temporaire des ENT, fin mars 2024.

Les jeunes (11-18 ans) représentent une cible particulièrement exposée aux risques cyber. Multi-équipés, ils sont également ultra connectés, et font souvent preuve d'un excès de confiance, à tort, dans leurs usages numériques et les pratiques cyber associées. L'entourage familial ne dispose pas nécessairement des informations et des réflexes à adopter pour protéger leurs enfants, d'où la nécessite de mieux prévenir et sensibiliser aux risques cyber, mais aussi aux dangers de la cybercriminalité, auxquels sont exposés les mineurs, tant comme auteurs que comme victimes.

Une mobilisation des pouvoirs publics collective et inédite

Face à ce constat, la section de lutte contre la cybercriminalité du Parquet de Paris et de la JUNALCO (J3) a proposé de mener une campagne de sensibilisation commune à destination des plus jeunes. Le ministère de l'Éducation nationale et de la Jeunesse (HFDS -DGESCO-DNE), le ministère de l'Intérieur et des Outre-mer (Commandement du Ministère de l'Intérieur dans le cyberespace), Cybermalveillance.gouv.fr (GIP ACYMA) et les magistrats de la section de lutte contre la cybercriminalité ont travaillé conjointement à la mise en place d'une opération basée sur une simulation d'hameçonnage, qui constitue la première menace cyber en France[1].

1 Rapport d'activité 2023 Cybermalveillance.gouv.fr

L'objectif de cette action est principalement de sensibiliser et de responsabiliser les élèves en marquant leur esprit avec des messages forts dans une vidéo courte, format auquel ils sont particulièrement sensibles. Il s'agit de les inciter à la prudence pour ne pas s'exposer à être victime, et à les avertir du risque pénal encouru en tant qu'auteur.

Présentation de la campagne Cactus
Les collégiens du département des Yvelines (78) et l'ensemble des collégiens de l'académie d'Orléans-Tours, ont reçu, via les ENT, un message les incitant à cliquer sur un lien pour se procurer gratuitement des « *jeux crackés et des cheats gratuits* ».

En cliquant sur le lien, ils sont dirigés vers un message vidéo d' 1min15 qui vise à les informer, les responsabiliser et les dissuader de réaliser des actions illégales sur Internet, au travers d'une communication forte des autorités en charge des sujets de cybersécurité en France[2].

Un champion de e-sport partage son expérience de joueur et souligne qu'il n'a jamais eu besoin de tricher pour gagner. Gendarme de profession, il rappelle également des conseils en termes de prévention avec des règles simples et des bonnes pratiques à suivre. Enfin, le spot se conclut avec l'intervention de la vice-procureure de J3 qui insiste sur les moyens mis en œuvre par la justice pour retrouver les auteurs de ces infractions et les peines encourues.

Le contenu de cette vidéo, construit collectivement, s'inscrit dans une démarche d'intérêt public et est complémentaire des actions déjà menées par le ministère de l'Éducation nationale et de la Jeunesse. L'opération, expérimentale, s'adresse à des académies volontaires.

À terme, cette action pourrait se généraliser à tous les établissements scolaires.
À ce titre, un kit contenant tous les éléments de la campagne sera mis à disposition de chacune des académies afin de leur permettre de déployer cette action de sensibilisation.

NOS CONSEILS

Hameçonnage :

- Ne pas cliquer sur les liens ou les pièces-jointes qui vous sont proposés dans un message non sollicité.
- Au moindre doute, lors de la réception d'un message inattendu ou alarmiste, contacter directement l'organisme concerné

Pour en savoir plus : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Virus stealer (vol d'identifiants**) :**

- Ne pas télécharger, ni utiliser de logiciels, d'applications, d'extensions de navigateur et de vidéos piratés ou d'origine douteuse qui peuvent souvent contenir un virus (lequel pourra ensuite aspirer vos données personnelles et confidentielles)
- Face à un message suspect (inattendu, alarmiste, aguicheur…), ne pas ouvrir les pièces jointes ou cliquer sur les liens

Pour en savoir plus : https://www.cybermalveillance.gouv.fr/medias/2024/03/240322_Fiche_VirusStealer.pdf

Contacts presse

Ministère de l'Intérieur et des Outre-mer – ComCyberMI
Tél : 06 58 97 59 56 / 06 07 72 01 70

[2] Lien : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/action-prevention1-ent

Mél : officierspresse@gendarmerie.interieur.gouv.fr / damien.malet@gendarmerie.interieur.gouv.fr / nicolas.weimer@gendarmerie.interieur.gouv.fr

Ministère de l'Éducation nationale et de la Jeunesse
Tél : 01 55 55 30 10
Mél : spresse@education.gouv.fr
www.education.gouv.fr/espace-presse

Parquet du tribunal judiciaire de Paris
Tél : 06 07 18 42 28
Mél : scom.parquet.tj-paris@justice.fr

Cybermalveillance.gouv.fr
Tél : 01 83 75 14 10
Mél : presse@cybermalveillance.gouv.fr