

LA LETTRE CYBER en région Grand Est



AVRIL 2024

LA THEMATIQUE DU MOIS: LES JEUX OLYMPIQUES DE PARIS (JOP)

Les JOP constituent un des plus gros évènements jamais organisés dans notre pays. Ceux-ci devraient attirer l'attention du monde entier concernant le sport.

Mais qu'en est-il du Cyber? La France pourrait-elle à cette occasion aussi attirer l'attention des hackers ?

Pas de suspens, la réponse est OUI.

Nous allons donc essayer jusqu'aux JOP de vous sensibiliser autour de cet évènement.



BILLETTERIES / LOGEMENTS



BILLETTERIES:

Vous souhaitez acheter des billets pour les JOP et vous trouvez une opportunité intéressante via une publicité ou un mail ? Vous devez impérativement faire très attention.

Si la recherche n'a pas été initiée par vous-même, méfiez-vous des faux sites, vous pourriez soit perdre votre argent, ne jamais recevoir de billet et risquer de communiquer vos données personnelles à des hackers qui en feront mauvais usage, soit recevoir un billet qui vous sera refusé à l'entrée du stade car il s'agira en fait d'une copie, d'un billet revendu plusieurs fois ou d'un faux.

Un prix trop attractif doit impérativement vous alerter. Il ne faut pas se mentir, un billet pour les JOP, c'est cher !!

Par défaut, ne faites donc jamais confiance à des opportunités publicitaires. Faites vos recherches vous-même ou allez sur le site officiel (<https://tickets.paris2024.org>)

LOGEMENTS:

De fausses annonces de logement vont voir le jour dans et en dehors de Paris : il faut en effet prendre en compte qu'il y aura partout des épreuves, des zones entraînements etc... Même si vous partez en vacances, faites donc très attention aux locations trop attractives. Vérifiez que les logements existent réellement, qu'ils sont disponibles et vraiment en location. Passez par des plateformes professionnelles.



Restauration / Transports



Une attention particulière devra également être portée cet été sur la restauration et les transports.

Des arnaques ont déjà vu le jour au détriment de certains restaurateurs. Des escrocs leur ont proposé la mise à disposition d'emplacements avec un Foodtruck dans Paris en leur faisant miroiter la possibilité de vendre leur cuisine en plein cœur de la capitale durant les JO. Évidemment, de telles opportunités n'existent pas...

Il n'y a en fait aucune limite à l'imagination des escrocs sur le net. Ils pourraient par exemple vous proposer de réserver une table à un prix particulièrement attractif dans un restaurant situé à proximité d'un site des JO et au moment d'une importante épreuve, impliquant si possible des membres de l'équipe de France. Le paiement (ou un acompte important) serait évidemment immédiatement exigé (normal, les places proposées sont en nombre limité !.) alors que l'établissement n'existe pas ou ne propose pas de réservation en ligne. Ce genre d'escroqueries sera vraisemblablement aussi tenté dans le domaine des transports, avec de faux sites proposant la vente en ligne de carnets de tickets de métro à des prix particulièrement bas, ou encore avec de fausses plateformes de réservation de taxis.

De manière générale, soyez très prudents quand vous êtes destinataires d'une publicité par courriel (avec un lien sur lequel cliquer...) faisant la promotion d'une offre très (trop) alléchante.



Vente de produits dérivés

Évidemment, comme pour tout évènement d'ampleur, des produits dérivés seront vendus sur place et en ligne. Sur place, une surveillance physique pourra permettre de minimiser le phénomène de contrefaçon, en revanche, en ligne, il est compliqué de contrôler les flux. Encore une fois, au risque de nous répéter : si vous souhaitez offrir un cadeau ou vous faire plaisir avec un T-shirt ou un mug, achetez-les sur un site officiel! C'est peut-être plus cher mais c'est plus sûr. Si vous trouvez des bons plans, vérifiez-les bien avant de perdre de l'argent et de jamais voir arriver votre bien.



DDOS

Le DDOS ou Attaque par Déni de Service Distribué est une attaque dont le but est d'engorger un système informatique ou un site internet par une multitude de requêtes.

Les systèmes de transport, les plateformes de réservation d'hôtels ou des sites officiels de vente de produits dérivés pourraient faire l'objet de ce type d'attaques visant à les paralyser et à en empêcher l'accès. Pourquoi ? Peut-être pour vous inciter à vous rendre, par dépit, sur un faux site alternatif créé par des escrocs !

Dans la logique de ce que nous vous avons exposé plus haut, soyez donc patients si c'est trop long ou si ça ne fonctionne pas sur les sites officiels.



QUISHING

De plus en plus fréquemment, vous découvrez des QR codes sur les tables des bars et des restaurants, des bornes de paiement, des ascenseurs ou encore des points d'informations. Ces QR Codes sont bien pratiques puisqu'il suffit de les scanner pour voir la carte ou les informations voulues.

Malheureusement, cette facilité récente conduit déjà à des dérives: des hackers peuvent créer de faux QR Codes (certains parfois collés sur les vrais !), qui vous emmènent sur un faux site web où on pourrait vous demander de saisir des informations personnelles ou bancaires ou vous faire télécharger un fichier infecté.

Pour ne pas vous faire berner: vérifiez l'URL du site vers lequel vous êtes redirigés, et méfiez-vous des informations qui vous sont demandées. Assurez-vous que ces informations sont cohérentes avec celles qui pourraient vous être demandées par l'émetteur « officiel » du QR Code.

POUR CONCLURE:

Nous avons invités ce mois-ci à la plus grande vigilance sur des thématiques précises, mais cette vigilance doit être de mise en permanence.

Techniquement, ces points de vigilance doivent se porter sur LES LIENS, LES PUBS, LES SITES, et globalement tout ce qui est trop attrayant.

Les mois prochains, nous reviendront sur les notions de ransomware ou phishing, qui pourraient être des attaques plus fréquentes durant les JOP en utilisant cet évènement comme vecteur d'infection.

+ D'INFOS



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
Rédacteurs : ADJ M. KNOBLOCH - ADJ E. DUBOIS

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 :

