MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER
Liberté
Égalité
Fraternité

LA LETTRE CYBER en Région Grand Est

Gendarmerie nationale

GENDARMERIE
NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

MAI 2024

LA THEMATIQUE DU MOIS:

LES JEUX OLYMPIQUES DE PARIS (JOP)

Retour sur les menaces les plus courantes (1)

Le mois dernier nous avons pu voir que les JOP pouvaient représenter une période particulièrement sensible pour notre sécurité informatique.

Revenons sur les risques les plus courants.

LE PHISHING

Définition

Le Phishing c'est quoi?

La Commission Nationale de l'Informatique et des Libertés (CNIL) définit sur son site internet le phishing comme une forme d'escroquerie sur internet:

« *Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.).* »

Au-delà du mail, le phishing s'étend désormais à TOUS les moyens de communication: SMS, Appel téléphonique, QR Code, publicité sur les réseaux sociaux etc… le principe reste le même mais la méthode employée est différente. Le but est toujours de manipuler la victime pour qu'elle donne des informations (financières, personnelles etc.) ou qu'elle clique sur un lien piégé.

D'accord, on en a entendu parler mais quel rapport avec les JOP?

Le site www.forbes.fr pose clairement cette question: « la cybercriminalité, nouveau sport olympique de Paris 2024? »

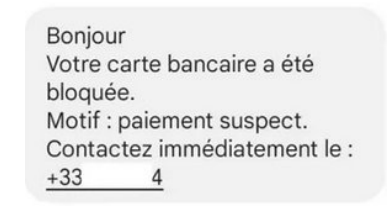
Le prix des billets, les difficultés d'hébergement, de circulation, de restauration... autant d'opportunités qui peuvent et qui seront exploitées par les escrocs.

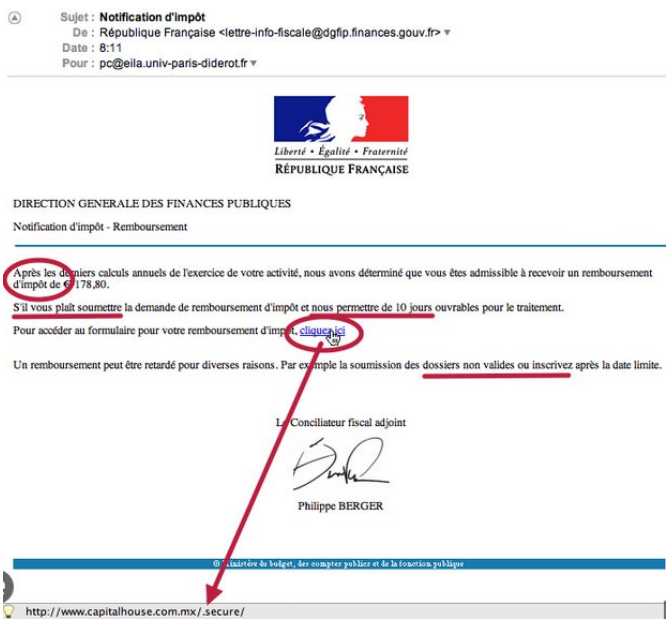
« Vous n'êtes pas concernés par la JO mais vous avez un besoin absolu de vous rendre à PARIS ? Découvrez nos transports réservés à ceux qui ne profitent pas des JO à prix avantageux ! »

C'est un exemple que je viens d'inventer mais au final, même si nous n'y assistons pas, les escrocs peuvent utiliser les JOP pour essayer de nous avoir.

Je reçois un mail offrant des places à prix réduits mais pour voir les offres, il faut cliquer sur un lien. ..Je n'ai pas l'intention d'y aller mais par curiosité, j'aimerais bien voir ces offres, ça pourrait intéresser un ami… OUPS ! le lien était piégé : mon ordinateur et mon réseau d'entreprise sont chiffrés et complètement bloqués.

Quelques exemples...





Quel est le risque pour vous? Et pour les autres?

- Vol d'informations sensibles : L'objectif principal du phishing est de voler des informations sensibles, comme les numéros de carte de crédit, les identifiants de connexion, les numéros de sécurité sociale, les adresses et bien plus encore. Ces informations peuvent être utilisées à des fins de vol d'identité ou de fraude financière ;
- Propagation de logiciels malveillants ;
- Fraude financière ;
- Le phishing peut être utilisé pour cibler des individus ou des entreprises spécifiques, y compris les employés d'une organisation. Les attaquants peuvent ainsi perturber les réseaux d'entreprise, accéder à des informations confidentielles et causer des perturbations graves.

Que faire pour ne pas se faire avoir?

- Ne communiquez jamais d'informations sensibles par messagerie ou téléphone à un interlocuteur que vous ne connaissez pas ;
- Avant de cliquer sur un lien, positionnez le curseur de votre souris sur celui-ci et vérifiez l'adresse du site qui s'affiche dans votre navigateur ;
- En cas de doute, vous pouvez contacter directement l'organisme concerné ;
- Activez la double authentification dès que possible et ne la communiquez jamais par message ou appel téléphonique.

+ D'INFOS

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: