PRINSOTEL

Recommandations d'action pour nos clients suite à la cyberattaque du 16 mai 2024

Suite à cette attaque, c'est notre obligation de vous fournir quelques instructions afin d'assurer la sécurité de vos données personnelles :

1. Nous **ne** vous demanderons, jamais et en **aucun** cas, vos coordonnées bancaires par voie électronique. Si vous recevez un appel ou un message vous demandant ce type de données, ne les partagez JAMAIS.

2. Si vous recevez de la publicité de PRINSOTEL par e-mail, SMS ou sur les réseaux sociaux, **vérifiez toujours l'identité** de l'expéditeur et, en cas de doute, ne cliquez jamais sur un lien qui vous semble douteux.

3. **Méfiez-vous des appels passés en notre nom** ou faites depuis l'un de nos hôtels. Vérifiez qu'il s'agit bien d'un appel venant d'un opérateur connu et, encore une fois, ne partagez jamais des données privées.

En outre, par ce document, nous souhaitons vous avertir de toutes les tentatives de fraude possibles à la suite de l'incident, telles que le *phishing, spear phishing, vishing, smishing, pharming, whaling*, et autres, pour que vous puissiez être vigilant face à ces actions malveillantes.

Vous trouverez ci-dessous les descriptions de ces types d'attaques ou fraudes afin que vous puissiez identifier tout comportement anormal et les éviter :

- ***Phishing :*** Le *phishing* (ou hameçonnage) est une technique d'ingénierie sociale consistant à envoyer des courriels en supplantant l'identité d'entreprises ou des organismes publics et en demandant à l'utilisateur ses coordonnées personnelles et bancaires. Au moyen d'un lien inclus dans le courriel, on tente de rediriger l'utilisateur vers un site web frauduleux pour lui amener à saisir son numéro de carte de crédit, son numéro de pièce d'identité, son mot de passe pour accéder aux services bancaires en ligne, etc.

  Ces courriels frauduleux comportent souvent le logo ou l'image de marque de l'entreprise ou organisme en question, peuvent contenir des erreurs grammaticales et tentent parfois de faire passer un message d'urgence et de peur afin de contraindre l'utilisateur à faire les actions demandées.
  Un courriel de *phishing* peut également comporter une pièce jointe infectée par un logiciel malveillant (*malware*). L'objectif de ce logiciel malveillant est d'infecter l'ordinateur de l'utilisateur et de lui voler des informations confidentielles.

- ***Spear phishing :*** Dans ce cas, les attaquants créent de faux courriels, de pages web fausses et même des messages courts faux qui semblent authentiques pour demander aux utilisateurs ses informations de connexion. C'est ainsi que les escrocs s'emparent des données d'accès aux boutiques en ligne, aux réseaux sociaux ou aux espaces de stockage en nuage. Dans le pire des cas, ils s'emparent même des informations bancaires ou des données de cartes de crédit. Les escrocs savent bien que bon nombre d'utilisateurs ne prennent pas la sécurité des mots de passe au sérieux et utilisent le même mot de passe pour différents services. Ainsi, une simple page web d'hameçonnage peut être utilisée pour obtenir des données sensibles, des informations qui ont un valeur économique élevé sur le marché noir numérique.

- ***Vishing :*** Le terme *vishing* est une combinaison des mots « voice » (voix) et « phishing » (hameçonnage), c'est pourquoi on parle aussi parfois de *voice phishing* (hameçonnage vocal). En se servant de cette technique, les attaquants utilisent la technologie VoIP

(*Voice over IP*) pour passer de nombreux appels frauduleux gratuits ou très économiques afin d'obtenir des codes, des mots de passe ou des données bancaires de la victime qui, souvent, ne se doute de rien.

- ***Smishing :*** Le terme *smishing* est une combinaison des éléments SMS et *phishing*. Comme dans le cas du *phishing*, les cybercriminels qui envoient ces messages se font passer pour des représentants d'une entreprise ou d'une organisation de confiance, mais au lieu d'envoyer des courriels, ils envoient des SMS (*Short Message Service*). Ces messages servent soit à inciter la victime à partager les détails de son compte, soit à installer des logiciels malveillants et des chevaux de Troie sur l'appareil de la victime à son insu.

- ***Pharming :*** Le *pharming*, combinaison des mots « phishing » et « farming », est une escroquerie en ligne similaire au *phishing*, dans laquelle le trafic d'un site web est manipulé afin de voler des données sensibles. C'est ainsi un type de cyberattaque d'ingénierie sociale dans laquelle les criminels redirigent les utilisateurs qui tentent d'accéder à un site web donné vers un autre site différent et faux. Ces « faux » sites tentent de s'emparer des données personnelles identifiables et des identifiants de connexion de la victime, tels que ses mots de passe, ses numéros de sécurité sociale, ses numéros de compte bancaire, etc. ou bien tentent d'installer des logiciels malveillants de *pharming* sur l'ordinateur de la victime.

- ***Whaling :*** Le *whaling* est une méthode utilisée par les cybercriminels pour prétendre occuper des postes à responsabilité au sein d'une organisation afin d'attaquer directement des cadres supérieurs ou d'autres personnes importantes au sein de l'organisation, dans le but de voler de l'argent, d'obtenir des informations confidentielles ou d'accéder à leurs systèmes informatiques à des fins criminelles. Le *whaling*, également connu sous le nom de fraude au PDG (*CEO fraud*), est similaire au *phishing* en ce sens qu'il utilise des méthodes telles que l'usurpation de sites web et d'adresses électroniques pour tromper la victime et l'amener à révéler des informations confidentielles ou à effectuer des virements d'argent, entre autres.

Nous sommes sincèrement désolés de cette situation, mais nous tenons à vous assurer que votre tranquillité d'esprit est notre priorité, et que nous avons abordé et maîtrisé cette situation de manière rapide et efficace.

Prinsotel travaille d'ores et déjà sur le plan d'action élaboré après l'incident et, en particulier, sur la mise en place de mesures de sécurité renforcées afin d'éviter que des situations similaires ne se reproduisent à l'avenir.
