



CASES articles

Les voyages sans Internet appartiennent au passé

Le temps des vacances et des voyages : le temps des arnaques – également sur Internet

Pour plus de sécurité, adoptez les réflexes CASES !

Les vacanciers sont des proies faciles pour les cybercriminels

Qui n'a jamais connu de déboires au cours de ses vacances ? Pickpockets et escrocs en tout genre, cambriolage de voiture, prix exorbitants affichés par les restaurants – De ce fait, les vacanciers se doivent de rester prudents et méfiants. Pourtant lorsqu'il s'agit d'escroqueries et de dangers liés à Internet, leur vigilance est bien plus faible. Que ce soit pour des vacances à la mer, en montagne ou par-delà les océans, Internet est souvent mis à contribution dès la préparation et la réservation du voyage. Une fois en vacances et loin de chez soi, des photos sont mises en ligne sur Internet, des virements bancaires sont effectués ou des e-mails sont consultés. Le phishing, les spywares, les offres d'appel sur Internet, les cybercafés douteux ou les hotspots dans les aéroports sont autant de risques négligés. Les vacances constituent pourtant une période faste pour les cybercriminels. Même la photo prise au cours d'une fête insouciante et postée sans réfléchir sur une page Internet peut avoir un épilogue fâcheux.

Nombreux sont ceux pour qui les vacances commencent sur Internet. Une étude allemande (« Reiseanalyse 2008 »), réalisée en collaboration avec le « Verband Internet Reisevertrieb », a permis de déterminer que quinze millions d'Allemands réservaient leurs vacances en ligne.

Dans les aéroports, les cybercafés, les centres-villes, les restaurants et dans de nombreuses chambres d'hôtel, accéder à Internet est devenu simple comme bonjour. Ceci est ren-



du possible grâce à des ordinateurs à usage public ou au Wifi, une technologie permettant l'accès sans fil au net. De nombreux vacanciers sont ainsi en mesure de consulter leurs messageries professionnelles et privées ; les e-mails envoyés de vacances atteignent leurs destinataires en l'espace de quelques minutes, voire quelques secondes. Même les opérations bancaires peuvent être exécutées rapidement et aisément entre la chambre d'hôtel et la piscine. Des photos prises lors de la dernière fête organisée sur la plage peuvent immédiatement être mises en ligne et sont accessibles au téléchargement. L'utilisation très répandue des moyens de communication modernes pendant les vacances témoigne de leur popularité et de leurs avantages.

Afin d'éviter les mauvaises surprises, les vacanciers doivent être conscients du fait que les mêmes principes sont applicables et pour le monde virtuel,

et pour le monde réel. Il est important de connaître les risques et de les détecter dès leur apparition. Vigilance, une bonne dose de méfiance et un certain nombre de réflexes de sécurité, tels sont les moyens de protection à appliquer.

Titre intermédiaire : **Réservation sur internet**

Il est possible de devenir la victime d'une escroquerie dès la réservation d'un voyage. L'offre la plus intéressante est, par exemple, imbattable, presque trop belle pour être vraie. Mais ce que promet la page Internet ne correspond pas forcément à la réalité : le piège peut très bien se cacher dans les clauses en petits caractères et le voyage se révéler beaucoup plus onéreux que prévu. Il peut également s'agir d'un site malhonnête – le client réserve, paie et ne reçoit jamais la prestation correspon-

dante. La page Internet incriminée disparaît alors du web aussi vite qu'elle est apparue. Il peut également s'agir d'un site web contrefait : des cybercriminels ont réussi, par le biais d'une attaque de phishing, à attirer le client d'un prestataire honnête sur une fausse page Internet. Un leurre peut être utilisé à cette fin, par exemple une offre très avantageuse dans une publicité envoyée par e-mail. Ce ne sont pas seulement les informations liées à la réservation que le pirate cherche alors à obtenir, mais également celles relatives aux cartes de crédit, mots de passe et autres données bancaires.

Pour ne pas devenir la victime d'attaques de phishing, méfiance et vigilance sont de mise lorsqu'il s'agit d'étudier des offres de voyages particulièrement alléchantes. Ceci est particulièrement vrai pour les offres exigeant une décision rapide. La même prudence est de rigueur face à des offres entrant dans la catégorie des « trop beau pour être vrai ». Il est recommandé aux clients de comparer les prix avant toute décision. Cela permet de mieux évaluer si le prix d'une offre correspond effectivement aux prestations promises. Avant toute réservation, il convient de vérifier le sérieux du prestataire et le contenu des clauses en petits caractères.

Titre intermédiaire : **Accès à Internet au cours du voyage**

Aéroports, restaurants, hôtels, cybercafés ou centres-villes, le nombre d'accès à Internet mis à la disposition des voyageurs ne cesse d'augmenter. Qu'ils soient gratuits ou payants, ces accès ne sont pas toujours sans danger. Ces points d'accès sans fil peuvent en effet être des pièges, placés par des cybercriminels. L'on peut également se poser la question de savoir si ce genre de point d'accès répond aux exigences minimales en matière de sécurité. Si tel n'est pas le cas, un pirate peut très aisément en prendre le contrôle. Les voyageurs confiants qui se connectent à Internet par le biais de ces liaisons sans fil tombent ainsi entre les mains des pirates. Les cybercriminels cherchent alors notamment à obtenir des numéros de cartes de crédit, des mots de

passes et d'autres informations et données bancaires exploitables.

Même un point d'accès protégé ne permet pas d'éliminer tous les risques ; de nombreux cybercriminels sont en effet passés maîtres dans l'art de recueillir des informations directement à l'écran. À cette fin, ils utilisent une caméra ou se placent directement derrière le voyageur, de manière à pouvoir suivre ce qui se passe sur l'écran. Chaque vacancier devrait être conscient de la valeur que représentent des appareils tels que les PC portables, les PDA ou les téléphones mobiles et de l'importance des données personnelles ou professionnelles qu'ils contiennent. Un bref moment d'inattention suffit au voleur pour subtiliser l'appareil et disparaître dans la foule.

Les ordinateurs mis à disposition par les hôtels et cybercafés constituent une alternative à l'utilisation des points d'accès sans fil. Les voyageurs ignorent toutefois ce qui est installé sur ces machines, et il est tout à fait possible que celles-ci soient infectées par des logiciels d'espionnage. Ces derniers sont alors, entre autres, en mesure d'enregistrer un mot de passe en surveillant l'activité du clavier. Des données bancaires ou commerciales, ou d'autres informations personnelles, peuvent ainsi tomber entre les mains de personnes malintentionnées. Mais le comportement même des voyageurs constitue un risque. Saisir des mots de passe, utiliser MSN pour chatter brièvement avec ses amis, consulter des pages Internet et ne pas fermer correctement une application – une application bancaire par exemple – autant de manipulations laissant des traces sur l'ordinateur public utilisé. Les cybercriminels utilisant ensuite le même ordinateur peuvent découvrir des applications ouvertes, des mots de passe ou encore les préférences de la personne.

Il est généralement déconseillé aux voyageurs d'utiliser des points d'accès publics à Internet afin d'accéder à des données bancaires ou commerciales, ou à d'autres informations importantes. Il convient de plus de toujours bien fermer les applications en utilisant les boutons « Exit », « Déconnexion », « Logout » ou boutons similaires.

Les voyageurs devraient également veiller à ce que personne ne les observe lorsqu'ils introduisent des informations confidentielles. Les appareils tels que les PC portables représentent une prise de choix, chaque voyageur doit en être conscient et tout mettre en œuvre afin de les protéger du vol. Les données importantes doivent être sécurisées par un mot de passe adéquat et par un mécanisme de cryptage. Les données resteront ainsi protégées, même en cas de vol de l'appareil.

Avant le départ, le voyageur devrait déterminer à quelles applications Internet il souhaite avoir accès au cours de ses vacances. Pour ces applications, il devra mémoriser les actions à effectuer afin d'éliminer toute trace sur l'ordinateur étranger. Le voyageur peut ainsi effectuer les réglages nécessaires avant même de lancer l'application sur l'ordinateur de l'hôtel ou du cybercafé.

Titre intermédiaire : **Photos de vacances**

Se détendre, faire la fête et s'amuser, prendre des photos, tout cela fait partie des vacances. Que ce soit en bikini sur le pont d'un voilier sous le soleil ou en s'amusant en soirée : les téléphones mobiles et les appareils photo numériques permettent de prendre rapidement et facilement une photo dans n'importe quelle situation. Des applications telles que Facebook ou Hi5 permettent de mettre en ligne rapidement photos et vidéos. Que ce soit voulu ou non, les souvenirs de vacances se retrouvent ainsi sur le web. Ces souvenirs sont alors souvent accessibles à un public important et l'accès est d'autant plus grand que les utilisateurs de ces applications ne maîtrisent que très rarement les réglages de sécurité élémentaires de ces outils. Rares sont les vacanciers conscients des conséquences possibles de ce genre de publication. Souhaite-t-on vraiment montrer ces photographies à son supérieur, à ses collègues ou lors d'un entretien d'embauche ? Les moteurs de recherche tels que Google permettent de découvrir rapidement les photos, les entrées dans les forums ou d'autres informations relatives à une personne. Les bureaux du personnel

et les employeurs utilisent de plus en plus souvent ce genre d'outils avant d'attribuer un poste ou d'accorder une promotion. Les photos où figurent, par exemple, un épisode où l'on a bu plus que de raison ou un bain de soleil un peu trop dénudé ne sont pas toujours de nature à favoriser l'embauche ou la carrière. Il est important de noter qu'Internet a la mémoire très longue. Les photographies, une fois publiées, peuvent encore y être consultées pendant de nombreuses années.

Les cambrioleurs ont également accès à ces photos et à ces chats et peuvent les utiliser à leurs fins. Ils apprennent ainsi que tel propriétaire d'une maison ou d'un appartement est en voyage et le cambriolage peut ensuite se faire tranquillement.

De nombreux voyageurs utilisent également des supports de données afin de mettre en ligne des photos, de les stocker ou d'aller les faire développer dans un magasin spécialisé. Un support de données de faibles dimensions, comme une clé USB par exemple, est facile à égarer dans un cyber-café. Si les photos n'ont pas été sauvegardées quelque part, les souvenirs de vacances sont définitivement perdus. Si, outre les photos, d'autres informations importantes sont stockées sur ce support de données, il ne peut être exclu que celles-ci soient utilisées par un tiers.

Ces supports de données et autres cartes mémoire pour appareils photo peuvent, de plus, être infectés par des malwares. Cela peut, par exemple, arriver dans un magasin photos utilisant des ordinateurs non protégés. Une mauvaise surprise attend ensuite le voyageur lors de la prochaine utilisation.

Avant toute publication de photos, les voyageurs devraient porter une attention particulière au choix des clichés qu'ils vont rendre accessibles par le biais d'applications internet et à qui elles seront accessibles. Les réglages

Conseil de sécurité :

CASES fournit un certain nombre d'informations supplémentaires relatives à l'utilisation d'un ordinateur public, aux réflexes de sécurité indispensables et aux méthodes à appliquer pour éviter de laisser trop de traces après son passage. Une fiche thématique est disponible sur le site www.cases.lu sous la rubrique Publications / Fiches thématiques « Postes Publics ». Sous la rubrique Pratique / Solutions, figure également un guide quant aux bons réglages de sécurité de l'application Facebook. L'édition estivale 2008 de la newsletter CASES « CASESmag » est en outre consacrée au thème de la sécurité pendant les vacances.

Définition : phishing

Le phishing représente la tentative d'un cybercriminel d'obtenir les données d'un utilisateur par le biais de pages Internet falsifiées.

Définition : navigateur

Un navigateur est un programme spécifique utilisé pour consulter les pages Internet sur le « World Wide Web ».

Définition : point d'accès Internet / hotspot

Un point d'accès Internet, également appelé hotspot, est un point d'accès public et sans fil au net. La technologie employée repose sur l'utilisation d'une antenne et d'ondes radio. Il est alors possible, dans la zone d'émission de l'antenne et à l'aide d'un PC portable ou d'un téléphone mobile prévu à cet effet, d'accéder sans fil à Internet. Les points d'accès publics sont habituellement indiqués par un marquage au sol ou par un panneau.

Définition : WiFi

Le terme WiFi est un nom de marque protégé par une licence. Il désigne une technologie de réseau local sans fil par liaison radio.

Définition : PDA

PDA est l'abréviation de « Personal Digital Assistant » (assistant numérique personnel). Il s'agit d'un petit ordinateur compact et portable, principalement utilisé en tant qu'agenda personnel et outil de gestion des adresses et des tâches.

de sécurité des différentes applications internet doivent de plus être maîtrisés par l'utilisateur. La publication de photos de tiers est légalement soumise à autorisation de ceux-ci. Lorsqu'il s'agit de mineurs, l'autorisation des parents doit de plus être demandée.

Les informations privées ou commerciales se trouvant sur un support de données devraient être effacées

avant toute utilisation de ce dernier en vacances. Ces supports étant de très faibles dimensions, les voyageurs devraient particulièrement veiller à ne pas les perdre. Ces supports devraient en outre subir une analyse de virus avant toute utilisation.

Les mesures et réflexes de sécurité mentionnés ci-dessus permettent de préserver les souvenirs de vacances pour de nombreuses années.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu