10

Méfiez-vous du Phishing

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

Méfiez-vous du Phishing

Le phishing ou hameçonnage est une technique d'ingénierie sociale, qui consiste à exploiter non pas une faille informatique mais la « faille humaine ». Cette technique d'escroquerie consiste à vous subtiliser des données personnelles (mots de passe de connexion à un service, numéro de compte en banque ou de carte bancaire...) en vous piégeant avec un faux courrier électronique qui reprend le logo, la mise en page, l'adresse de votre banque, de votre fournisseur d'accès à Internet, d'un service de messagerie …etc. Le message prétexte un problème lié à votre compte et vous invite à cliquer sur un lien pour donner vos coordonnées. Vous basculez en réalité sur un faux site et ainsi l'attaquant récupère les informations saisies. Les conséquences sont diverses selon le type de renseignements que vous avez fournis. Cela va du pillage de votre compte en banque, en passant par des achats effectués avec votre numéro de carte bancaire. Autre arnaque très en vogue, l'usurpation de votre identité sur des sites de réseaux sociaux comme Facebook ou MySpace.

Quelques règles pour éviter le Phishing

- Ne cliquez pas directement sur le lien contenu dans le mail, ouvrez plutôt votre navigateur et saisissez vous-même l'URL d'accès au service.

- Méfiez-vous des formulaires demandant des informations bancaires. Il est en effet rare (voire impossible) qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute contactez directement votre agence par téléphone !

- N'envoyez jamais vos mots de passe, identifiants de connexion ou toutes autres informations personnelles par courrier électronique. Méfiez-vous toujours des messages vous invitant à saisir des informations personnelles, même si la demande semble légitime. Si vous pensez avoir été victime de phishing en donnant vos identifiants de connexion et/ou vos mots de passe, changez vos données d'authentification au plus vite.

- Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par https et qu'un petit cadenas est affiché dans la barre d'état au bas de votre navigateur.

- Lorsque vous cliquez sur le lien d'un courriel, vérifiez, une fois le navigateur ouvert, que l'adresse du site est bien orthographiée. Les attaquants utilisent parfois la même charte graphique d'un site légitime et modifient un ou plusieurs caractères dans l'url afin de faire croire à la victime qu'elle est bien sur le site sollicité.