Être vigilant avec les courriers électroniques

Le spam

On appelle spam l'envoi répété de courriers électroniques non sollicités, le plus souvent à but commercial, à des personnes dont l'adresse électronique a été captée de façon irrégulière sur des sites web, des forums de discussion, des annuaires..., et qui n'ont jamais consenti à les recevoir. L'envoi de spam est interdit par la loi.
La messagerie académique intègre un filtre de spam qui marque les messages détectés comme du spam en ajoutant l'expression [** SPAM **] dans l'objet du message.

Comment se protéger ?

Ne répondez jamais à un spam.
Ne cliquez pas sur les liens, n'ouvrez pas les pièces jointes.
N'exposez pas votre adresse.

Le phishing

Phishing est la contraction de phreaking et fishing; phreaking étant lui-même la contraction de phone et freak. Que se cache-t-il derrière ces termes anglophones ?

De quoi s'agit-t-il ?

Le phishing est le fait de piéger une personne afin d'obtenir d'elle des données confidentielles. En général il s'agit de données servant à s'authentifier sur un service en ligne, un identifiant (un numéro de compte bancaire, l'identifiant de messagerie académique, ...) et du code ou mot de passe associé, permettant l'authentification.

Comment cela se passe-t-il ?

La personne malveillante envoie de très nombreux messages dans lesquels elle demande au destinataire de communiquer des informations soit directement en répondant au message, soit par l'intermédiaire d'un formulaire sur un site web. Le message et le formulaire peuvent revêtir des formes différentes, imitant parfois parfaitement le graphisme de l'institution ciblée, ou bien sont négligés, mal orthographiés et mal présentés.
Les données envoyées par mél ou saisies dans un formulaire sont recueillies par l'escroc pour être directement utilisées ou revendues.

> Exemple de phishing imitant la direction des impôts
>
> Exemple de phishing imitant le service de messagerie

Quelle menace cela représente-t-il ?

S'il s'agit du vol de votre numéro de carte de crédit, le risque est de voir des sommes débitées sur votre compte en banque. Il s'agit généralement de sommes modestes, passant plus facilement inaperçues.

S'il s'agit de votre identifiant et mot de passe, le pirate peut accéder à une multitude de services numériques de l'éducation nationale : applications métier (ScoNet, BE1D, ...), ou outils de communication (mèl, agenda).

Le phishing constitue une menace directe pour vous mais également pour l'académie qui voit son système d'informations ouvert à des personnes malintentionnées. C'est aussi une menace pour les autres puisqu'avec votre mot de passe, le pirate peut envoyer des méls à des tiers en se faisant passer pour vous. Votre compte est utilisé pour envoyer du spam contenant de la publicité, d'autres tentatives de phishing , des escroqueries, etc.

Comment s'en protéger ? Suivez quelques règles simples

- Méfiez-vous des messages qui vous invitent à saisir votre nom d'utilisateur et votre mot de passe. Aucun service de l'éducation nationale n'est autorisé à demander ce type d'informations. Ne répondez jamais à des demandes d'informations personnelles par courrier électronique ; en cas de doute, contactez l'institution censée vous avoir envoyé le message.
- Ne saisissez jamais votre mot de passe dans un formulaire auquel vous accédez par un lien contenu dans un message, même s'il ressemble à une page de connexion de l'académie. Pour être certain que l'adresse affichée dans le lien ne vous envoie pas sur un site falsifié, retapez vous-même l'adresse dans la barre d'adresse du navigateur.
- Lors de la consultation de sites sécurisés (sites bancaires, par exemple), vérifier que l'adresse du site commence par https et non par http.
- Conservez vos informations personnelles secrètes ! Ne révélez jamais votre mot de passe ni votre NUMEN. Si vous dévoilez ces informations, modifiez-les dans les plus brefs délais.
- N'utilisez pas l'option d'enregistrement de votre mot de passe ; Il peut être capté par un virus et communiqué à un pirate.
- Effacez régulièrement les formulaires, les mots de passe, le cache et les cookies de votre navigateur, tout particulièrement si vous utilisez un ordinateur public.

Hoax

On appelle hoax (canular en français) un courrier électronique propageant une fausse information et qui incite le destinataire à la diffuser à tous ses contacts. Ce type de message suscite l'émotion (disparition d'enfant, promesse de bonheur, faits extraordinaires, alerte sur des virus, pétition, etc..) et cherche à provoquer une réaction en chaîne.
L'impact d'un hoax n'est pas négligeable ; outre la désinformation qu'il véhicule, il peut dégrader l'image d'une personne ou d'un organisme et perturber son fonctionnement, encombrer les boîtes aux lettres...

Comment réagir ?

Gardez l'esprit critique : vérifiez à l'aide d'un moteur de recherche que le message n'est pas un canular.
De façon générale, gardez-vous de faire suivre un message à tous vos contacts, surtout si on vous le demande.

Les arnaques

Beaucoup d'arnaques, également appelées scam, circulent sous la forme de courrier électronique envoyé par un inconnu qui vous propose une transaction financière. Il vous parle d'une importante somme d'argent (héritage, pot-de-vin, comptes tombés en déshérence, fonds à placer à l'étranger, etc.) et demande votre aide pour son transfert, en échange de quoi il vous offre un pourcentage sur la somme. Il finira par vous demander de lui envoyer une avance ou des frais quelconques (notaires, entreprises de sécurité, pots-de-vin...).

Comment réagir ?

Mettez ce genre de message à la corbeille. Il n'y a pas plus de miracles sur l'Internet que dans la vie courante. Si vous répondez positivement à cette sollicitation, vous ne reverrez jamais votre argent.

M.A.J. le 14/02/2018

Dans cette rubrique

- Choisir un mot de passe
- **Être vigilant avec les mèls**

- Se protéger des virus

Rectorat de Nantes
4, rue de la Houssinière
BP 72616 - 44326 Nantes CEDEX 03
Tél. 02 40 37 37 37