Fiche 5

Nos conseils pour se protéger des pièges sur Internet

L'hameçonnage ou le « phishing » est une technique de piège sur Internet

Ces e-mails non désirés ont pour objectif de récupérer : vos informations personnelles.

- adresse de connexion ;
- mots de passe ;
- coordonnées postales ou bancaires.

Dans la majorité des cas, les e-mails d'hameçonnage invitent le destinataire à cliquer sur un lien pour :

- compléter un formulaire ;
- contacter un centre d'appel ;
- envoyer à une adresse e-mail inconnue des informations personnelles.

Ces e-mails ont souvent un lien vers un site sécurisé, mais qui redirige vers un site dangereux.

Comment reconnaître les mauvais e-mails ?

- Les mauvais e-mails ont parfois des fautes d'orthographe ou de grammaire ;
- Les mauvais e-mails sont souvent écrits en anglais ;
- L'objet de l'e-mail est souvent lié à une perte de données clients, de coordonnées bancaires, remboursement ou facture à payer ;
- L'adresse e-mail de l'expéditeur ou l'adresse de la page sur laquelle on vous demande de vous rendre ne correspond pas au bon site.

Plus de conseils sur le site de l'ANSSI :
les 5 réflexes à avoir lors de l'arrivée d'un e-mail :
http://bit.ly/ANSSI5réflexes

Si vous recevez un e-mail douteux d'un expéditeur inconnu :

1. ne répondez pas ;
2. ne cliquez sur aucun lien contenu dans l'e-mail et n'ouvrez pas les documents ;
3. signalez l'e-mail douteux sur le site du Gouvernement :
   https://signalants.signal-spam.fr/login
4. Supprimez ensuite l'e-mail de votre messagerie.

Les 10 règles pour bien utiliser son téléphone mobile

1	Dès l'achat du téléphone mobile, je note et garde le numéro IMEI de mon mobile. Le numéro IMEI est le véritable « antivol » du téléphone mobile ;
2	J'utilise un kit oreillette quand je téléphone ;
3	Je rapporte mon « vieux » téléphone portable en magasin ;
4	Je maîtrise ma consommation et ses coûts en choisissant un forfait adapté ;
5	Je parle doucement dans les lieux et transports publics ;
6	En deux-roues ou en voiture je laisse la messagerie répondre ;
7	En classe, j'éteins mon téléphone portable ;
8	Je préviens mes parents ou mes amis si j'ai un doute sur un message ou un e-mail ;
9	Je reste prudent avec mon téléphone portable quand je l'utilise ;
10	Je respecte les autres personnes, en particulier pour les photos et vidéos sur les réseaux sociaux.

Si l'expéditeur vous semble digne de confiance (service public, opérateur, banque...):

1. Méfiez-vous des questionnaires avec de l'argent à gagner, des remboursements ou des livraisons ;
2. Vérifiez l'adresse e-mail de l'expéditeur ou l'adresse de la page sur laquelle on vous demande de vous rendre. Vérifiez les adresses habituellement utilisées ;
3. Ne donnez jamais vos coordonnées bancaires ou votre mot de passe, ni par e-mail ni par téléphone ;
4. En cas de doute, contactez le service client de l'organisme concerné et vérifiez avec lui d'où vient l'e-mail ;
5. Signalez l'e-mail sur le site du Gouvernement dédié: **https://signalants.signal-spam.fr/login**
6. Supprimez ensuite l'e-mail de votre messagerie.

Si vous avez été victime d'un piège sur Internet et si vous avez donné des informations personnelles :

- changez-le(s) mot(s) de passe(s) des sites ;
- vérifiez les réglages de vos boîtes mails ;
- mettez à jour l'antivirus et enregistrer le disque dur.

Cette fiche a été transcrite par l'atelier FALC de l'ESAT La roseraie
27, rue du général Leclerc 78420 Carrières-sur-Seine.

Avec la participation de Pierre Barreau, Richard Escat, Delphine Grellier et Bruno Kopaczynski.

Fédération Française des Télécoms
11-17 rue de l'Amiral Hamelin
75 116 Paris
www.fftelecoms.org

Tél. : **01 47 27 72 69**
Retrouvez-nous sur les réseaux sociaux

FÉDÉRATION FRANÇAISE DES TÉLÉCOMS