# Attaques en filoutage (*phishing*) & OTP RSA

Fiche synthèse d'informations et d'actualités

## Attaques en filoutage et en ingénierie sociale

### Pour quoi faire ?

**L'objectif de l'attaquant est de vous faire révéler des secrets** utilisables dans des actions malveillantes et cela au moyen de fausses demandes ou fausses promesses...
*Ex : Votre numéro de carte bancaire pour faire des achats*
*Ex : Vos identifiants pour demander une mutation malgré vous*

### Quels sont les moyens utilisés ?

Ces attaques ne nécessitent aucun moyen technique particulier, **tous les moyens de communication peuvent être utilisés**, que cela soit le mèl, les réseaux sociaux, les SMS ou même un simple appel téléphonique.

### Comment ça marche ?

Le principe est celui d'une arnaque classique. Il s'agit de **provoquer une réaction spontanée et irréfléchie**. Cela est possible, entre autre, en usurpant une relation de confiance ou en provoquant une réaction naturelle.

**Les relations de confiance** peuvent être vis-à-vis d'un service, d'une personne ou d'une autorité...
*Ex : « Bonjour, ici le support technique », « ... ici l'Inspection Académique », « Ce courrier est de l'HADOPI »*
**Les réactions naturelles** sont nombreuses, de la crainte jusqu'à l'appât du gain.
*Ex : « Pour éviter la destruction de votre compte, fournissez votre identifiant et mot de passe dans les 6 heures »*

### Comment s'en protéger ?

**En réfléchissant :** vous devez savoir que cela existe pour **éviter les réactions *à chaud*** et déjouer les arnaques.
*Ex : Le support m'appelle → Qui me demande cette information ? Est-ce bien lui ? En a-t-il besoin ?*
*Ex : J'ai gagné à une loterie à laquelle je n'ai pas participé → Est-ce-crédible ?*
**En préservant vos secrets** : vous devez avoir conscience de détenir des secrets pour y porter une attention particulière. Parmi ceux-ci, il y a bien sûr vos identifiants, vos mots de passe et codes PIN, mais aussi beaucoup d'autres informations de nature personnnelle telles que vos coordonnées bancaires ou votre NUMEN.

***Les urgences à la minute sont rares et les offres trop intéressantes sont souvent des supercheries.***
***Elles doivent vous inciter à en parler à quelqu'un de confiance autour de vous***

## Le cas des clés OTP RSA

### A quoi servent-ils ?

**Ils apportent de la robustesse en introduisant un nouveau secret**, le code régénéré chaque minute.
L'utilisation de cette clé OTP implique aussi l'utilisation des secrets déjà vus : l'identifiant et le mot de passe.
Le renouvellement très rapide du code rend les attaques en filoutage caduques car, si ce secret est dérobé, il n'est réutilisable que durant la minute où il a été généré et les codes suivants sont impossibles à prévoir.

### L'actualité

La société RSA, suite à l'attaque informatique qu'elle a subie en mars 2011, rappelle que **votre code PIN, les codes générées et le numéro de série de votre clé OTP sont des informations de nature personnelle** pouvant être la cible d'attaque en filoutage.

### Comment s'en protéger ?

La protection est la même que pour les autres informations de nature personnelle, il faut faire attention à qui vous les divulguez et à leur confidentialité. Pour cela, il est recommandé de :

**Ne pas noter votre code PIN à proximité de la clé OTP**
**Valider l'identité de celui qui vous demande des informations**
**Ne pas suivre de liens vous entrainant à saisir des informations**
**Ne pas laisser vos clés sans surveillance**
**Ne pas communiquer votre code PIN**
**Prendre le temps d'agir**