FORTRA

# Terranova Security®

## Qu’est-ce que la mystification ?

La mystification ou spoofing survient lorsqu’un cybercriminel usurpe l’identité d’un individu ou d’une organisation en utilisant des techniques d’ingénierie sociale pour commettre des actes malveillants. Des adresses courriel, des sites Web et également des numéros de téléphone peuvent être falsifiées pour convaincre les victimes de partager des informations confidentielles.

### Exemples de différents types de spoofing

**01 — SPOOFING PAR COURRIEL**

Le spoofing par courriel survient lorsqu’un pirate utilise une fausse adresse courriel pour mener une attaque. Selon la tactique utilisée, l’expéditeur peut falsifier l’adresse courriel, le nom d’expéditeur, ou les deux. Les cybercriminels peuvent également utiliser le spoofing par courriel pour endosser des identités multiples.

**02 — SPOOFING DE SITE WEB**

Le spoofing de site Web, qui consiste à présenter à la victime un faux site Web qui semble légitime, est une tactique communément utilisée dans le cadre de cyberattaques. Le site Web falsifié est en tous points identique à l’original. Le logo, l’image de marque, les couleurs, la disposition, le nom de domaine et les coordonnées sont exactement les mêmes pour tromper les visiteurs.

**03 — SPOOFING DE L’IDENTITÉ DE L’APPELANT**

Ce type de tactique de spoofing survient lorsqu’un faux numéro de téléphone contient votre indicatif régional. Comme les victimes sont toujours plus susceptibles de répondre à un numéro local, les cybercriminels utilisent cette tactique pour les amener à répondre au téléphone ou au message texte.

**04 — SPOOFING WI-FI**

Les cybercriminels créent de faux réseaux sans fil auxquels les utilisateurs peuvent se connecter lorsqu’ils cherchent un point d’accès Wi-Fi. Les menaces et les risques sont réels lorsque les utilisateurs voyagent, travaillent à distance, participent à des conférences ou sont en déplacement.

**05 — SPOOFING DE L’EXTENSION DE FICHIER**

Le spoofing de l’extension de fichier survient lorsqu’un fichier possède une double extension pour dissimuler sa nature réelle. Par exemple, file.txt.exe est un fichier exécutable, mais il peut apparaître comme un simple fichier texte si l’extension est dissimulée. L’ouverture de ce type de fichier entraîne l’ouverture et l’installation de programmes malveillants.

## Qui peut être la cible de spoofing ?

**Tout type d’organisation ou d’individu peut être la cible d’une attaque de spoofing.** Le spoofing permet aux fraudeurs d’adopter une identité qui peut sembler crédible. À l’aide de faux sites Web, adresses courriels, points d’accès Wi-Fi ou numéros de téléphone, les cybercriminels peuvent facilement amener leurs victimes à penser que leurs communications et requêtes sont légitimes.