

Fiche 1

Quelques techniques pour tromper les internautes

Vous constatez qu'un groupe de personnes qui étaient jusqu'à présent inconnues dans votre domaine d'activité gagne en popularité sur les médias sociaux. De plus en plus de comptes mentionnent leur nom, les personnes écrivent en anglais, à des heures improbables, par exemple à 4 h le matin. Vous commencez à avoir des doutes sur ces comptes...

En repérant les techniques couramment utilisées pour vous faire parvenir de l'information de façon biaisée, vous serez plus à même de les déjouer et de naviguer à travers le désordre informationnel. En voici quelques-unes.

Hameçonnage

Leurre mis en place par des personnes cybercriminelles pour s'emparer d'informations personnelles. Un courriel avec un lien cliquable reprenant les couleurs d'une institution, par exemple.

Piège à clics

Technique utilisée par certains sites Web qui consiste à utiliser des titres volontairement alarmistes pour attirer l'attention des internautes. Ces sites sont à but lucratif : plus les internautes cliquent, plus les propriétaires de ces sites gagnent de l'argent. Pour faire cliquer les internautes, les rédactrices et rédacteurs ont recours à plusieurs techniques, et font souvent appel aux émotions [Fiche 2](#).

Similitantisme (*astroturfing*)

Les campagnes de similitantisme sont créées par des groupes qui ont pour but d'influencer l'opinion publique pour une cause en utilisant une fausse impression de popularité (création de pages Web, participation aux débats publics, diffusion d'affichage, etc.), voire en simulant un mouvement populaire.

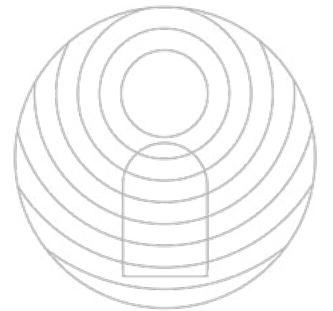
Fermes de robots

Réseau de logiciels automatisés et contrôlés par un seul opérateur pour créer et partager du contenu sur les médias sociaux, et pour interagir avec les internautes, afin de donner de la visibilité à une opinion ou à un sujet particulier, de façon artificielle.

Les robots prennent souvent la forme de profils sans photo ou avec une photo générée par l'intelligence artificielle, au nom étrange (ex. : @quebec75452578). Ils publient des messages formatés de manière identique d'un compte à l'autre, à une fréquence beaucoup plus élevée que les humains, et à des heures qui ne correspondent pas aux «heures normales».



Pour aller plus loin



Fiche 1

Quelques techniques pour tromper les internautes

Exemples de faux comptes essayant de créer de la visibilité autour d'un sujet : le modèle de message est identique, l'image et le moment auquel la publication a été effectuée également³⁵.

The image displays three separate Twitter profiles, each showing a tweet with identical content and a blurred video thumbnail. The first profile has 3,016 tweets, 754 following, 547 followers, and 47 likes. The second has 3,682 tweets, 1,651 following, 1,177 followers, 2,044 likes, 5 lists, and 1 moment. The third has 1,741 tweets, 464 following, 396 followers, and 48 likes. All three tweets read: "Despite veterans' pleas, GOP tried to cut their benefits. Democrats... Republicans won't even stand with veterans. shareblue.com". Below the tweet, each profile shows a video thumbnail of a man in a suit (Shepard Smith) on a news set. The caption under the thumbnail in the first two profiles reads: "Fox's Shepard Smith Calls Bullsh*t On Jared Kushner's Senate Testimony | Crooks and Liars". The caption under the thumbnail in the third profile reads: "Fox's Shepard Smith Calls Bullsh*t On Jared Kushner's Senate Testimony | Crooks and Liars". The video thumbnail is a blurred image of Shepard Smith speaking on a news program.