# Facteur humain

Gilles Favier a fondé la société Encelis, qui utilise la psychologie cognitive pour sécuriser les systèmes informatiques. Il est convaincu que l'humain a un grand rôle à jouer dans la réduction du nombre de cyberattaques.

**Quelles sont les failles humaines exploitées par les pirates ?**

L'émotion en premier lieu, comme celle suscitée par un mail réclamant un don au profit d'une cause noble. L'appât du gain ensuite, parce que personne ne veut rater une bonne affaire.

**Pourquoi sommes-nous insouciants sur Internet ?**

L'outil informatique ne nous permet pas de constater les conséquences de nos actions dans le monde extérieur. En psychologie, cela se nomme la « perte du sentiment d'agentivité ». Lorsque l'on clique sur un lien malveillant, dans un mail ou une page web, nous ne voyons pas le virus qui s'installe. Alors on reste serein. Le psychologue Daniel Kahneman, Prix Nobel d'Économie, a théorisé le fonctionnement du cerveau sous la forme de deux « systèmes ». Le système 2 est lent, réfléchi, et nous sert pour les opérations complexes alors que le système 1 est rapide, émotionnel et incontrôlé. On l'utilise pour toutes les fonctions « automatiques », via des opérations mentales rapides pour apporter des réponses quasi-immédiates et donc plus sujettes aux erreurs. Or, l'outil informatique fait généralement appel à ce dernier.

**Comment faire pour s'en prémunir ?**

Il faut être plus vigilant. C'est compliqué car les pirates savent détourner notre attention. L'adresse mail est toujours savamment usurpée et le mail bien rédigé. Mais lorsque vous regardez bien, vous constatez que ce n'est pas le même nom de domaine ou qu'il y a des tournures mal formulées. Si votre caissier au supermarché vous demande votre numéro de téléphone ou vos clefs, cela active notre vigilance. Vous devriez réagir de la même façon face à un écran. Mais un mail qui nous demande des informations personnelles n'active pas notre vigilance car nous sommes habitués à les donner pour s'inscrire ou payer, même sur des sites inconnus. L'usage du web et des mails, à l'usure, contourne les mécanismes cognitifs de vigilance et d'autant plus facilement qu'il ne s'agit pas d'interactions réelles. C'est la vigilance humaine couplée à la technologie qui permettra de sécuriser davantage notre environnement numérique.

**Comment votre connaissance de la psychologie vous aide-t-elle dans votre approche de la cybersécurité ?**

La norme sociale est un levier comportemental très intéressant en cybersécurité. Elle est basée sur les "nudges", des incitations destinées à orienter une décision sans l'imposer. À l'instar des messages affichés sur les panneaux d'autoroute : ils ne sont pas obligatoires mais le conducteur sait qu'il a à y gagner en les respectant. Nous avons appliqué ce mécanisme dans une entreprise qui avait été victime d'une attaque par "phishing" (hameçonnage). Nous avons communiqué à tous le nombre de personnes ayant eu un comportement inadapté, puis félicité ceux qui n'avaient pas cliqué sur le lien suspect et sensibilisé les autres. Comme personne n'aime être classé dernier, ceux ayant cliqué étaient conduits à faire évoluer leur comportement et la vigilance des autres était confortée. Le regard extérieur compte beaucoup dans notre inconscient. Un autre exemple est celui que nous appelons « l'option par défaut », notamment utilisé par les services de messagerie qui placent automatiquement les mails avec des liens potentiellement malveillants dans un dossier « indésirables ». Consulter un mail placé dans un tel dossier requiert un coût cognitif supérieur à l'ouverture quasi-automatique de ce même mail placé dans la boîte de réception classique. Le biais de « statu quo » entre alors en jeu : notre propension à maintenir la situation existante plutôt que de la changer. La sécurité se voit donc renforcée.