"I’ve been tricked again!": Threat perceptions, compensatory strategy and acceptability of cybersecurity’s "best practices”

Contenu sous forme de paragraphes

Projet accompagné dans le cadre de l'appel à manifestation d'intérêt "Collecte et analyse de données sur les interactions humaines"

Résumé

Lorsque les individus perçoivent une situation comme étant menaçante, leur sentiment de sécurité physique et psychologique diminue. Afin de réduire cet inconfort, les individus adoptent des stratégies de compensation. Appliqué au domaine de la cybersécurité, face à une menace de type phishing (c.-à-d., méthode cybercriminelle poussant les usagers à partager leurs informations personnelles en usurpant l’identité d’une personne ou un organisme de confiance), une des stratégies de compensation adoptée par les personnes, serait l’augmentation de leur adhésion à des politiques de cybersécurité dites restrictives (c.-à-d., limitent la liberté personnelle) et de surveillance (c.-à-d., limitent la vie privée). Cela leur permet de croire que « tout est sous contrôle ». En d’autres termes, dans certaines conditions, les individus seraient prêts à renoncer à une partie de leur liberté personnelle et leur vie privée pour plus de sécurité. Le projet CYBER-Threat a pour premier objectif d’examiner cet effet de compensation – face à la cybermenace, les individus adhèrent davantage aux politiques restrictives et de surveillance en matière de cybersécurité. Cela étant, la mise en oeuvre de telles politiques pourrait engendrer chez les individus des réactions négatives. La réactance pourrait s’illustrer par une faible adhésion à ces politiques de cybersécurité ainsi qu’une faible acceptabilité envers les recommandations gouvernementales en matière de cybersécurité (c.-à-d., faible utilité perçue de ces recommandations, faible facilité perçue de leur mise en place, attitudes défavorables envers ces recommandations), et par conséquent, peu d’intention d’adopter des comportements sécuritaires (p. ex., faible intention d’appliquer les recommandations). Le projet CYBER-Threat a pour second objectif d’examiner les réactions des personnes face à l’application de ces politiques de cybersécurité restrictives et de surveillance et leurs conséquences sur l’acceptabilité des recommandations en matière de cybersécurité et l’intention d’adopter des comportements sécuritaires. Dans ce contexte, les politiques de cybersécurité restrictives et de surveillance pourraient être tout à la fois attractives (c.-à-d., réduction de l’inconfort psychologique face à la menace) et potentiellement contre-productives (p. ex., réactance). En parallèle, le projet CYBER-Threat a un troisième objectif qui est de clarifier les liens entre la perception de (cyber)menace et les performances des individus quant à la détection de mails frauduleux. En effet, certains auteurs (p. ex., Vishwanath et al., 2018) montrent que percevoir une menace améliore les performances de détection, lorsque d’autres auteurs (p. ex., Wang et al., 2017) montrent que l’anxiété qui découle de la perception de menace conduit à de moins bonnes performances de détection de mails frauduleux. Afin de répondre à ces objectifs, trois études seront réalisées. La présente demande concerne deux des trois études.

Equipe

Laurent Guillet
Psychologie
Lab-STICC
Université Bretagne Sud

Nicolas Spatola
Psychologie sociale et cognitive
Artimon Perspectives

Axe de recherche
Démocratie, expérimentations et transformations
Responsables
Dayle David
Psychologie
LP3C
Université Rennes 2
Discipline(s)
Psychologie
Mots clés thématiques
Perception de menace, acceptabilité, cybersécurité, phishing
Dates du projet
1 mars 2026 - 28 février 2027
Dispositifs de soutien
PACIHM