Doit-on piéger ses propres employés pour les sensibiliser au risque de cyberattaques

Yvan Barel, Sandrine Frémeaux

Doit-on piéger ses propres employés pour les sensibiliser au risque de cyberattaques ?

Yvan BAREL
enseignant-chercheur en GRH, membre du laboratoire LEMNA, Université de Nantes

Sandrine FRÉMEAUX
professeur à Audencia Business School et membre du GRACE

L'entraide et le soutien, une histoire de " vivre ensemble " Le développement du télétravail lié à l'épidémie de covid-19 a augmenté le risque de cyberattaques. Comment les entreprises peuvent-elles se protéger du phishing, c'est-à-dire des courriels d'hameçonnage visant à dérober à des individus leurs identifiants de connexion et mots de passe ? La lutte contre le phishing est assurément un objectif sérieux, et elle passe par une prise de conscience des risques d'attaques externes permettant à des délinquants de se faire passer pour des employés, d'avoir accès à des renseignements confidentiels ou de perturber les systèmes.

Que les directions d'entreprise cherchent à bloquer les attaques de phishing est d'autant plus nécessaire que celles-ci se sont démultipliées ces derniers mois.

Mais une question se pose : les directions doivent-elles – avec l'aide des équipes informatiques – piéger leurs propres employés pour les sensibiliser au risque de cyberattaques ?

La question peut paraître saugrenue, mais il s'agit bien d'une nouvelle tendance sur laquelle on a encore peu de recul aujourd'hui en France, celle consistant pour les services informatiques des entreprises de tester les salariés en envoyant de faux courriels de phishing. Leur but ? Identifier les employés qui cliquent imprudemment sur le lien, qui ouvrent la pièce jointe ou qui fournissent des mots de passe à un faux site Web. Les équipes informatiques dénoncent alors les comportements des employés piégés, puis les invitent à une formation obligatoire.

L'inefficacité du dispositif

Plutôt que d'expliquer spontanément dans un format pédagogique et ludique les différents types de cyberattaques, pourquoi certains services informatiques (tels que ceux du ministère des finances ou du PMU) préfèrent-ils commencer par piéger leurs propres employés ?

Des études académiques anglosaxonnes[1] ont analysé l'impact de ces faux courriels de phishing et ont évoqué le danger du dispositif :

1/ Au lieu d'être attentifs aux règles de sécurité, les salariés concernés resteraient ou deviendraient plus vulnérables aux attaques externes.

2/ Le groupe de personnes piégées vivraient un sentiment de honte et de ressentiment qui pourraient affaiblir leur confiance, leur engagement et leur productivité.

3/ À la frustration du groupe des collaborateurs piégés s'ajoute un malaise partagé par la majorité des employés, peut-être un peu amusés, mais surtout choqués par une direction capable de réaliser ce choix.

En fait, l'ensemble des collaborateurs peuvent voir dans ce dispositif les signes d'un management par la peur qui les amène à redouter non seulement les attaques criminelles externes mais aussi les attaques internes perçues comme des atteintes à la relation de confiance. Le risque est que les salariés soient de plus en plus nombreux à se réfugier derrière une attitude de passivité ou de méfiance les amenant à ne pas (ou peu) répondre aux mails collectifs.

Le malaise est d'autant plus élevé que les faux courriels d'hameçonnage peuvent porter sur des sujets éminemment sensibles, par exemple en faisant croire aux salariés qu'ils doivent rapidement s'inscrire à une campagne de dépistage obligatoire du coronavirus. Ce malaise peut être renforcé lorsque le nom de l'expéditeur emprunté par les services informatiques est celui de la Direction des RH, dont la fonction est non pas de piéger les salariés, mais de les protéger contre les nombreux écueils et paradoxes de la vie des organisations.

Une histoire de dons mal donnés

Alors pourquoi ces directions adoptent-elles ce dispositif ? Sans doute le résultat d'une vision technique et rationnelle du risque dans un environnement marqué par la scientifisation du travail. L'idée est un peu celle de la logique de vaccination : de même qu'un virus est administré pour permettre au corps humain de s'inoculer contre des organismes, des courriels d'hameçonnage simulés sont envoyés aux employés pour les aider à s'inoculer contre de véritables cyberattaques. Comme s'il s'agissait d'une simple histoire biologique...

Mais il s'agit surtout d'une histoire humaine, d'une histoire de dons mal donnés et mal accueillis. Les services informatiques craignent vraisemblablement que la formation qu'ils souhaiteraient prodiguer ne soit pas reçue et comprise. Ils optent alors pour le coup d'éclat : piéger quelques salariés, afin

SOMMAIRE

de montrer non pas que l'erreur est humaine, mais que l'erreur est grave. Le paradoxe tient à ce que les salariés hameçonnés risquent d'être présentés comme des personnes naïves, imprudentes ou irresponsables, alors qu'ils sont le plus souvent victimes d'un manque de sensibilisation au phishing dont la responsabilité incombe précisément aux services informatiques.

En procédant ainsi, ils oublient que bien des collaborateurs avaient une soif de recevoir, d'être aidés, d'être soutenus, d'en savoir plus sur ces sujets-là et sur l'ensemble des évolutions informatiques de leur entreprise. Les employés piégés mais aussi la plupart des autres employés témoins de la division organisée sont privés de la possibilité d'accueillir les informations comme un don et condamnés à les voir comme une sanction ou comme une menace.

Restaurer la logique d'entraide dans les organisations

Les employés ont besoin d'être accompagnés par les équipes informatiques afin de protéger leur structure contre les cyberattaques et réaliser leurs objectifs de travail. Les dons de temps, d'attention, de vigilance, d'informations des services informatiques sont précieux, et ils ont d'autant plus de prix qu'ils peuvent être reçus librement. Au sein des organisations, on peut espérer que les équipes dirigeantes résistent à la tentation de stigmatiser une partie de leur staff, et entrent dans cette dynamique d'entraide et de soutien, délivrant sans crainte et sans compter les informations permettant à l'ensemble des collaborateurs de rechercher tout à la fois la sécurité, l'utilité et la qualité du travail.

YVAN BAREL
enseignant-chercheur en GRH, membre du laboratoire LEMNA, Université de Nantes

SANDRINE FRÉMEAUX
professeur à Audencia Business School et membre du GRACE.

Notes et Références

- *([1]) Jampen D. and al. (2020), " Don't click : towards an effective anti-phishing training. A comparative literature review " , Human-centric Computing and Information Sciences, vol. 10 (33), p.1-41 ; Williams E.J. and al. (2018), " Exploring susceptibility to phishing in the workplace " , International Journal of Human-Computer Studies, vol. 120, p.1-13 ; Caputo D.D. and al. (2014), " Going Spear Phishing : Exploring Embedded Training and Awareness " , IEEE Security & Privacy, vol. 12 (1), p.28-38.*