Vous avez un email ! COVID-19 et Cybersécurité : le cas du phishing

Les pirates informatiques ont su tirer parti de la pandémie actuelle de coronavirus pour tenter d'infecter des ordinateurs et appareils mobiles avec des logiciels malveillants ou d'escroquer les utilisateurs. Dans une période où la majorité des administrations françaises fonctionnent en télétravail, la vulnérabilité des agents de la fonction publique, non avertis et parfois isolés, est accrue et le risque de cyberattaque se voit amplifié. La crise sanitaire véhiculant de l'anxiété face à la recherche d'informations sur les coronavirus révèle des vulnérabilités inhérentes qui font des salariés en télétravail des cibles faciles pour la cybercriminalité. L'art de recueillir intelligemment des informations sensibles et confidentielles auprès d'une personne en exploitant les faiblesses humaines est connu sous le nom d'ingénierie sociale (Lohani, 2019). Les méthodes d'ingénierie sociale utilisent des astuces psychologiques pour créer la tromperie, qui à son tour pousse les gens à accomplir des actions ou à divulguer des informations confidentielles personnelles et d'entreprise (Choudhary, Kumar, et Kumar, 2016) en toute innocence. En conséquence, tout message ayant la connotation du coronavirus reçoit une attention particulière, y compris les courriers électroniques non sollicités, les faux sites web et les pièces jointes malveillantes que les fraudeurs sur internet utilisent pour voler des informations par la tromperie et le mensonge.

L'Agence américaine de cyber sécurité et de sécurité des infrastructures et le Centre national de cyber sécurité du Royaume-Uni ont publié un avis commun sur les faux SMS provenant d'expéditeurs tels que « COVID » et « UKGOV » qui contiennent un lien vers des sites de *phishing*. Le terme *phishing* peut être défini comme « un acte de tromperie modulable par lequel l'usurpation d'identité est utilisée pour obtenir des informations de la cible » (Lastdrager, 2014, p. 8). Tout comme des pêcheurs, ces escrocs utilisent des appâts pour augmenter les chances que leur cible « morde ». Cette pêche consiste le plus souvent à envoyer des messages (courriels, SMS…) venant apparemment d'une entité de confiance, par exemple une banque (Wright et Marett, 2010) ou une institution gouvernementale. Ces messages informent le destinataire qu'un problème est survenu et qu'il ne peut être résolu que si le destinataire du courriel confirme des informations personnelles (Wright et Marett, 2010), ou ils promettent des offres alléchantes qui leur permettent de récupérer des identifiants et des mots de passes (Hinde, 2004). Habituellement, les courriels de *phishing* ne demandent pas de réponse directe, mais contiennent un lien vers un site web frauduleux, ce qui est « l'hameçon » dans la métaphore de la pêche. Ce site web est très similaire, dans son aspect et sa convivialité, au site officiel qu'il personnifie (Purkait et al., 2014). Les facteurs déterminant le fait que l'utilisateur tombe (ou non) dans le piège peuvent à la fois dépendre de caractéristiques liées aux mails et à l'utilisateur.

Les caractéristiques du mail et du profil utilisateur

Les e-mails proposant un prix monétaire ou demandant un mot de passe sont plus facilement considérés comme « *phishy*« , tandis que les messages contenant uniquement des informations (par exemple, sur une prétendue mise à jour de sécurité) sont plus susceptibles d'être perçus comme sûrs. Cela peut poser un problème, car ces messages électroniques apparemment dignes de confiance peuvent tout aussi bien contenir un lien vers un site web de phishing. En outre, les courriels contenant des fautes d'orthographe ou une conception non professionnelle ont tendance à éveiller les soupçons (Furnell, 2007 ; Jakobsson, 2007). Lorsque les pirates, qu'on pourrait appeler faussaires, parviennent à convaincre les destinataires que le courrier est authentique, l'étape suivante consiste à les persuader que le partage des informations personnelles est nécessaire. Les stratégies d'ingénierie sociale qui se sont avérées efficaces sont le « *liking* » (c'est-à-dire prétendre être une personne, une organisation ou une entreprise que le destinataire apprécie et en laquelle il a confiance) (Wright et al., 2014), la « réciprocité » (c'est-à-dire donner aux gens l'impression qu'ils doivent retourner une faveur), la « preuve sociale » (c'est-à-dire prétendant que d'autres personnes ont également partagé leurs données personnelles), la « rareté » (c'est-à-dire donner l'impression qu'une opportunité est limitée) (Wright et al., 2014)

et l'autorité » (c'est-à-dire prétendre être une figure d'autorité) (Butavicius et al., 2016). Une récente étude réalisée sur la période de mi-mars à mi-avril suggère que les trois stratégies les plus pertinentes en dans les cas de *phishing* liés au COVID-19 sont : *liking* (42 %), la preuve sociale (18 %) et la rareté (17 %) (Naidoo, 2020).

Dhamija, Tygar et Hearst (2006) ont constaté que de nombreux utilisateurs ne connaissaient pas les indices techniques des sites web sécurisés ou ne les recherchaient pas. Ce qui implique que les indicateurs de sécurité standard peuvent ne pas être utiles dans de nombreux cas, car les utilisateurs ne les comprennent pas ou négligent de les rechercher. Plusieurs études montrent que les personnes ayant une plus grande expérience d'Internet (Wright et Marett, 2010) ou des connaissances technologiques (Sheng et al., 2010) sont moins susceptibles d'être victimes de *phishing*. On peut supposer que les utilisateurs habituels d'Internet ont une plus grande expérience de la détection des incohérences dans les courriers électroniques. Cependant, une étude de Pattinson et al. (2012) indique que seules les personnes qui savaient qu'elles avaient participé à une expérience de *phishing* ont vu leur connaissance de l'ordinateur avoir un effet significatif sur la façon dont elles gèrent les courriels de *phishing*. Cela pourrait signifier que même les internautes expérimentés ont besoin d'un rappel constant des risques auxquels ils sont confrontés, et qu'ils ne sont donc pas toujours mieux armés pour faire face à un éventuel risque.

La démarche de protection : PPT (*People Process & Technologies*)

La protection contre le *phishing* peut s'appuyer sur les trois composantes structurelles de tout système numérique Schneier (1999) : *People, Process & Technology*.

– *Technology* – D'abord, les technologies sont depuis longtemps conçues de façon à limiter la propagation du *phishing*. Filets anti-spam et anti-*phishing*, détection de la menace avec des signatures, indice de réputation des expéditeurs en fonction des métadonnées des messages sont autant de techniques permettant de classifier voire de rejeter directement des messages malveillants. Or, comme les virus qui s'adaptent aux antibiotiques censés les curer, le *phishing* a également su évoluer. Il est ainsi de plus en plus utilisé en ciblant les utilisateurs de façon personnalisée (*spear phishing*). C'est pour cette raison que toutes les politiques de protection contre cette menace requièrent une sensibilisation des salariés.

– *People* – La sensibilisation aide les utilisateurs à reconnaître les courriels et les sites web frauduleux et vise à expliquer comment des informations apparemment innocentes peuvent être utilisées dans le développement d'une attaque de *phishing* ciblée. Les formations de sensibilisation des utilisateurs doivent d'abord permettre de comprendre (a) les limites des outils techniques existants, (b) pourquoi les attaquants s'intéressent à leur organisation et (c) pourquoi les utilisateurs sont des cibles (Kumaraguru et al., 2010). En permettant aux individus de mieux comprendre à la fois les conséquences de leurs actions et la manière dont ces conséquences peuvent être atténuées à chaque étape (en suivant les procédures implémentées) la menace du *phishing* peut être réduite (Tsai et al, 2016).

– *Process*. Dans le cas conjugué d'une menace de sécurité et d'une crise, les procédures doivent permettre de (a) répondre à la question des rôles : qui dirige une éventuelle cellule de crise, qui est en charge de rendre disponible les outils nécessaires aux utilisateurs ayant basculé du jour au lendemain en télétravail, qui fait l'inventaire des personnels formés et non encore formés, qui anime une séance de formation urgente à destination des personnes les plus à risque, etc., et (b) de favoriser la communication et le partage d'information entre « défenseurs » de l'organisation et « utilisateurs ». Dans le cadre de la crise sanitaire que nous traversons, la capacité à apporter de l'information fiable avec des référents disponibles semble être un atout majeur. D'une manière plus globale, la démarche PPT doit s'adapter au contexte dans lequel évoluent les salariés. La taille

de l'organisation, le secteur d'activité, les fonctions des personnes au sein de celle-ci sont autant d'éléments à prendre en considération (Naidoo, 2020).

Jeanne Le Roy et Benjamin Laubie

Références

Butavicius, M., Parsons, K., Pattinson, M., et McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv preprint arXiv:1606.00887*.

Choudhary, M., Kumar, A., et Kumar, N. (2016). Social Engineering in Social Networking Sites: A Survey. *International Journal of Engineering Research et Management Technology (IJERMT)*, *3*(1), 123-129.

Dhamija, R., Tygar, J. D., et Hearst, M. (2006, April). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590).Furnell, 2007

Hinde, S. (2004). All you need to be a phisherman is patience and a worm. *Computer Fraud et Security*, *2004*(3), 4-6.Jakobsson, 2007

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., et Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, *10*(2), 1-31.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 9.Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, 1-16.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., et Butavicius, M. (2012). Why do some people manage phishing e-mails better than others?. *Information Management et Computer Security*, *20*(1), 18-28.

Purkait, S., De, S. K., et Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. *Information Management et Computer Security*.

Schneier, B. (1999). Security in the real world: How to evaluate security technology. *Computer security journal*, *15*, 1-14.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., et Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382).

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., et Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers et Security*, *59*, 138-150.

Wright, R. T., et Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273-303.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., et Marett, K. (2014). Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research*, *25*(2), 385-400.Lohani, 2019