

La faille humaine, talon d'Achille de la cybersécurité

Le phishing exploite la confiance

Le mot «phishing» vient de l'anglais et constitue la contraction des mots «password» (mot de passe) et «fishing» (pêcher). En français, phishing se traduit généralement par «hameçonnage». Ce terme désigne une technique pour obtenir des renseignements personnels dans le but de les utiliser à l'insu et sans le consentement de la personne concernée.



Martina Guillod

La collecte des données peut se faire via des sites internet, e-mails ou notifications falsifiés, qui feront croire à la victime qu'elle s'adresse à un tiers de confiance (banque, autorité, employeur) et la pousseront ainsi à dévoiler des renseignements personnels comme un mot de passe ou un numéro de carte de crédit. Les escrocs peuvent ensuite réaliser des affaires au nom de leur victime et s'enrichir à ses dépens. Le phishing repose sur la faille humaine, car il exploite la confiance et la crédulité des victimes.

D'un point de vue juridique, il est difficile d'appréhender le phishing. La création et l'envoi d'e-mails de phishing ne sont punissables que si les conditions du faux dans

les titres (art. 251 du Code pénal) sont remplies. Tel peut par exemple être le cas si l'e-mail envoyé par l'escroc demande au destinataire de divulguer l'identifiant et le mot de passe afin d'éviter que le compte ne soit fermé. Les conditions peuvent également être remplies si un site web falsifié ouvre une fausse session e-banking au visuel quasi identique à celui du site authentique. L'auteur doit agir intentionnellement dans le but de nuire à autrui ou d'améliorer sa situation personnelle, par exemple en vendant les données obtenues. Le faux dans les titres est puni par une peine privative de liberté de cinq ans ou une peine pécuniaire.

Un escroc ne se contente que rarement d'envoyer des e-mails de phishing sans utiliser les données obtenues. Dès qu'il fait usage des informations recueillies par le

phishing, par exemple en se connectant à e-banking et en effectuant un transfert d'argent en ligne, il est susceptible de se rendre coupable d'utilisation frauduleuse d'un ordinateur (art. 147 Code pénal). Il faut pour cela qu'il ait agi intentionnellement dans le but de s'enrichir de manière illégitime. L'auteur risque une peine privative de liberté de cinq ans au plus ou une peine pécuniaire. Si l'auteur fait métier de tels actes, la peine sera constituée d'une peine privative de dix ans au plus ou de 90 jours-amendes au moins. L'utilisation frauduleuse d'un ordinateur peut être poursuivie dans notre pays si les escrocs utilisent les données obtenues illégalement pour se connecter à l'e-banking d'un institut financier helvétique, même si les auteurs ne sont pas physiquement en Suisse.