Reconnaître un mail de phishing ou d’hameçonnage

Le phishing, cette technique frauduleuse destinée à leurrer un internaute pour l’inciter à communiquer des données personnelles en se faisant passer pour un service connu ou un proche, est très répandu. Selon une enquête CESIN OpinionWay, c’est le type d’attaque le plus couramment constaté par les entreprises en 2020 (80 %) devant l’exploitation d’une faille logiciel (52 %) et l’arnaque au président (42 %). Pour les spécialistes, le recours massif à cette technique s’explique par le fait qu’elle ne requiert aucune compétence technique et peu de moyens. Elle est donc à la portée d’un grand nombre de cybercriminels.

Se méfier des courriels inhabituels

La fiche du site www.cybermalveillance.gouv.fr rappelle quelques points de vigilance à respecter pour identifier les courriels suspects. Il est conseillé, notamment, de se méfier des courriels :

– émanant d’un service ou d’une société dont l’entreprise n’est pas cliente ;

– adressés par une entreprise partenaire ou une administration mais non signés ou signés par un expéditeur inhabituel ;

– adressés par une entreprise partenaire ou une administration mais à la mauvaise personne (par exemple, une facture adressée au mauvais service) ;

– mal rédigés (mauvaise traduction) ou utilisant un ton inadéquate (trop incitatif, menaçant…) ;
– incitant à faire quelque chose d'inhabituel comme fournir des coordonnées bancaires, prétendument perdues ;
– émanant d'un expéditeur dont la composition de l'adresse de courriel ne correspond pas à l'entreprise dans laquelle il est censé travailler.

La fiche donne également des exemples de mails frauduleux afin de nous aider à mieux les identifier.

Pour consulter la fiche : www.cybermalveillance.gouv.fr