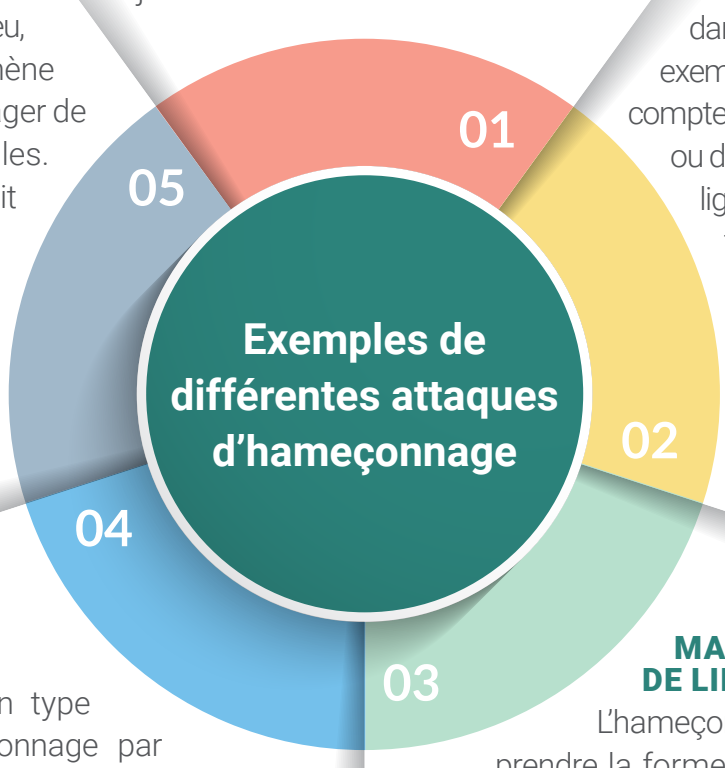
FORTRA

Terranova Security®

Co-présenté par Microsoft

Qu’est-ce que l’hameçonnage?

L’hameçonnage est un cybercrime qui consiste à utiliser des faux courriels, sites Web et messages textes pour voler des informations personnelles et corporatives confidentielles. Les cybercriminels utilisent des informations volées comme des adresses, noms et numéros d’assurance sociale pour faire des demandes de cartes de crédit ou de prêts, ouvrir des comptes bancaires et commettre d’autres activités frauduleuses.



COURRIEL

De loin la tactique la plus commune sur cette liste, un courriel d’hameçonnage peut arriver dans votre boîte courriel personnelle ou professionnelle au moment où vous vous y attendez le moins. Ce courriel peut comprendre des renseignements à suivre, un lien Web à cliquer ou une pièce jointe à ouvrir.

L’HOMME-DU-MILIEU

Dans le cas d’attaques dites de l’homme-du-milieu, le cybercriminel emmène deux personnes à partager de l’information entre elles. L’hameçonneur peut soit envoyer de fausses demandes à chacune des parties ou modifier l’information qui est transmise.

INJECTION DE CONTENU

Ce type d’attaque d’hameçonnage injecte du contenu malveillant dans un site Web connu, par exemple, la page d’accueil d’un compte de courrier électronique ou d’une institution bancaire en ligne. Ce contenu prend la forme d’un lien, d’une forme ou d’une fenêtre surgissante qui dirige les utilisateurs vers un site Web secondaire où on leur demande d’entrer leurs informations confidentielles.

HARPONNAGE

Le harponnage est un type plus avancé d’hameçonnage par courriel qui cible un individu ou une organisation spécifique. Cette technique utilise des messages personnalisés pour convaincre le destinataire de suivre les instructions. Les banques, les hôpitaux et les universités sont des cibles communes de harponnage.

MANIPULATION DE LIEN

L’hameçonnage peut parfois prendre la forme d’un lien malveillant qui semble provenir d’une source de confiance, comme Amazon ou Apple. En cliquant sur le lien, les utilisateurs sont dirigés vers un faux site Web identique au site original où ils sont incités à saisir les informations de leur compte.

Qui peut être la cible d’hameçonnage?

Tout type d’entreprise, de gouvernement, d’organisation ou d’individu peut être la cible d’une attaque d’hameçonnage. N’importe qui peut être dupé par une tactique d’hameçonnage et amené à partager des données sensibles avec un cybercriminel. Pour cette raison, il est essentiel que tous vos employés soient en mesure de détecter et rapporter toute tentative d’hameçonnage.