https://www.dane.ac-versailles.fr/spip.php?article675

ACADÉMIE
DE VERSAILLES
Liberté
Égalité
Fraternité

Sécurité numérique : l'affaire de tous !

Comprendre et contrer les techniques de l'ingénierie sociale

- Mes enjeux - Sécurité numérique -

Date de mise en ligne : mardi 10 octobre 2023

En tant qu'enseignant, vous avez probablement déjà entendu parler des pirates informatiques (hackers) et de leurs méthodes pour compromettre la sécurité de services en ligne. L'une des techniques les plus redoutables utilisée est l'ingénierie sociale. Dans cet article, nous allons explorer les bases de ce qu'est l'ingénierie sociale, comment elle fonctionne, et surtout, comment vous pouvez protéger vos données personnelles et sensibles contre cette menace élaborée.

Qu'est-ce que l'ingénierie sociale ?

L'ingénierie sociale est une méthode basée sur la manipulation des gens par les assaillants afin d'obtenir des informations confidentielles. Au lieu de cibler directement les systèmes informatiques, ils ciblent les individus. Les pirates utilisent diverses techniques psychologiques pour tromper leurs victimes, les incitant à divulguer des informations confidentielles, telles que des mots de passe, des numéros de sécurité sociale ou des informations bancaires.

[Illustration de la sÃ©curitÃ© des donnÃ©es bancaires : un cadenas posÃ© sur deux cartes bancaires.]

Les pirates informatiques cherchent à obtenir des informations confidentielles, comme les coordonnées bancaires

Voir la transcription

Photographie d'un clavier d'ordinateur, sur lequel sont déposées deux cartes bancaires. Un cadenas fermé est posé sur elles.

Quelles sont les techniques les plus courantes d'ingénierie sociale ?

- **Le phishing ou le smishing :** les hackers envoient des e-mails ou des messages SMS prétendant provenir de sources légitimes pour inciter les victimes à cliquer sur des liens malveillants ou à divulguer des informations personnelles.
- **Usurpation d'identité :** les attaquants se font passer, au téléphone par exemple, pour quelqu'un d'autre, comme un employé de votre banque, pour obtenir des informations sensibles.
- **Influence psychologique :** les assaillants manipulent les émotions de leurs victimes, les incitant à agir rapidement sans réfléchir, afin de partager des informations confidentielles ou effectuer des paiements.
- **Ingénierie sociale physique :** les pirates se présentent en personne pour accéder à des locaux restreints ou pour voler des informations physiques.

L'ingénierie sociale sur les réseaux sociaux

L'ingénierie sociale sur les réseaux sociaux est une technique très populaire chez les cybercriminels. Ils l'utilisent pour manipuler les utilisateurs et obtenir des informations personnelles ou sensibles. Voici comment, d'une manière simplifiée elle fonctionne.

[Photographie des mains d'une personne tenant un smartphone, sur lequel s'affichent les icÃ´nes de diffÃ©rents rÃ©seaux sociaux.]

Les cybercriminels utilisent les réseaux sociaux pour manipuler les utilisateurs et obtenir des informations personnelles

Voir la transcription

Photographie des mains d'une personne tenant un smartphone, sur lequel s'affichent les icônes de différents réseaux sociaux.

Création de profils faux ou usurpation d'identité

Les pirates informatiques créent souvent de faux profils sur les réseaux sociaux en utilisant de fausses identités ou en usurpant l'identité de quelqu'un d'autre. Ces profils peuvent sembler authentiques, avec des photos, des informations de profil et des publications pour renforcer leur crédibilité. Les IA permettent par exemple de générer facilement et automatiquement du texte ou des photos de profil plus vraies que nature.

Établissement de la confiance

Une fois ces faux profils créés, les attaquants cherchent à établir la confiance avec d'autres utilisateurs. Ils peuvent le faire en suivant, en aimant (*like*) et en commentant régulièrement les publications de leurs cibles. Ils peuvent également prétendre avoir des intérêts ou des amis en commun pour renforcer leur crédibilité.

Phishing et hameçonnage

Une fois qu'ils ont gagné la confiance de leurs cibles, les pirates passent à l'étape suivante, qui consiste à envoyer des messages privés ou des liens malveillants. Ces messages peuvent sembler provenir d'amis ou de contacts de confiance de leur victime. Ils incitent les cibles à cliquer sur des liens qui conduisent souvent à des sites web de phishing, conçus pour voler des informations sensibles telles que des mots de passe ou des informations financières.

Collecte d'informations

En continuant à interagir avec leurs cibles, les pirates peuvent poser des questions subtiles pour recueillir des informations personnelles. Ils peuvent demander des détails sur la vie personnelle, les habitudes en ligne, les informations de compte ou d'autres données sensibles. Ces informations sont d'ailleurs souvent disponibles en mode public sur certains profils non correctement sécurisés par les victimes.

Chantage et extorsion

Une fois que les attaquants ont recueilli suffisamment d'informations, ils peuvent les utiliser pour exercer un chantage sur leurs cibles. Ils menacent de divulguer des informations embarrassantes ou sensibles, à moins que la cible ne coopère (rançon) ou ne fournisse plus d'informations.

Comment se protéger de l'ingénierie sociale ?

- Soyez prudent avec les demandes d'amis et de suivi : n'acceptez que les demandes d'amis ou de suivi de personnes que vous connaissez personnellement ou en qui vous avez confiance.
- Vérifiez l'authenticité des profils : si un nouveau contact semble suspect, vérifiez son profil, ses amis et ses activités en ligne ; méfiez-vous des profils avec peu d'activité ou d'amis.
- Soyez conscient des informations que vous partagez : évitez de divulguer des informations personnelles sensibles sur les réseaux sociaux, même à des amis présumés.
- Veillez à séparer vie professionnelle et vie privée.
- Utilisez la vérification en deux étapes : activez-la pour renforcer la sécurité de vos comptes de médias sociaux.
- Signalez tout comportement suspect : si vous êtes contacté par quelqu'un de suspect ou si vous remarquez une activité inhabituelle sur votre compte, signalez-le immédiatement aux administrateurs du réseau social et remplacez votre mot de passe par un qui est robuste.

En restant vigilant et en prenant des mesures simples et de bon sens pour protéger vos informations personnelles en ligne, vous pouvez réduire considérablement le risque de devenir une victime de l'ingénierie sociale sur les réseaux sociaux.

Pour aller plus loin

Les techniques d'attaques les plus répandues
Le phishing (hameçonnage), Le smishing (hameçonnage)
Des podcasts sur la sécurité numérique