KnowBe4

AVIS ET CONSEILS DE SÉCURITÉ

Guide pédagogique du piratage psychologique

Le piratage psychologique se produit lorsque quelqu'un essaie de vous manipuler pour vous amener à effectuer une action ou à partager des informations confidentielles. Malheureusement, les cybercriminels utilisent le piratage psychologique pour accéder aux systèmes informatiques, recueillir des informations ou gagner de l'argent. La plupart des attaques par piratage psychologique réussies sont dues à une erreur humaine. Si vous vous familiarisez avec les méthodes courantes de piratage psychologique, vous serez peut-être en mesure de reconnaître une tentative d'attaque par piratage psychologique et de vous en protéger. Dans ce guide pédagogique, vous pourrez apprendre ce qu'est le piratage psychologique et comment vous pouvez vous protéger des attaques par piratage psychologique.

Ruses du piratage psychologique

Les cybercriminels peuvent utiliser plusieurs méthodes différentes pour vous piéger avec une attaque par piratage psychologique. Passons en revue trois méthodes de piratage psychologique courantes que vous pouvez rencontrer et des exemples de chaque méthode :

Les liens malveillants : Les cybercriminels peuvent utiliser des liens malveillants pour vous inciter à télécharger un logiciel dangereux ou à ouvrir une page qui n'est pas sûre. Ils peuvent vous envoyer un courriel d'hameçonnage, c'est-à-dire un courriel qui tente de vous convaincre de partager des informations sensibles, de cliquer sur un lien qui n'est pas sûr ou de télécharger une pièce jointe malveillante. Par exemple, vous pouvez recevoir un courriel contenant un lien permettant d'accéder aux informations d'expédition d'une commande. Parce que le courriel semble légitime, vous pourriez être tenté de cliquer sur le lien. Ensuite, le lien pourrait télécharger un logiciel malveillant qui permettrait au cybercriminel de contrôler votre ordinateur.

Les fausses pages Web : Les cybercriminels peuvent créer de fausses pages pour vous inciter à vous connecter à la page ou à saisir des informations sensibles. Par exemple, vous pourriez recevoir un courriel d'hameçonnage contenant un lien pour vous connecter à LinkedIn. Parce que le courriel semble légitime, vous pourriez être tenté de cliquer sur le lien et de saisir vos identifiants de connexion. Une fois vos identifiants de connexion saisis, le cybercriminel peut se connecter à votre compte LinkedIn, consulter vos renseignements personnels et modifier votre mot de passe afin que vous ne puissiez plus accéder à votre compte.

L'usurpation d'identité : Les cybercriminels peuvent se faire passer pour une célébrité ou une personne que vous connaissez afin de vous inciter à révéler des informations sensibles, à cliquer sur un lien qui n'est pas sûr ou à télécharger une pièce jointe malveillante. Vous pourriez par exemple recevoir un appel téléphonique d'un cybercriminel se faisant passer pour votre fournisseur d'accès à Internet. Le cybercriminel pourrait vous dire que votre paiement mensuel est en retard et mentionner votre numéro de compte et votre date de naissance. Parce que l'appel semble légitime, vous pourrez être tenté de fournir vos informations de paiement. Rappelez-vous que les attaques par usurpation d'identité peuvent également se produire par courriel, par message texte ou par les médias sociaux.

KnowBe4

Conseils pour se protéger du piratage psychologique

Maintenant que vous connaissez mieux les ruses du piratage psychologique, passons en revue quelques conseils que vous pouvez utiliser pour vous protéger des attaques par piratage psychologique :

- Avant de cliquer sur un lien, passez votre souris dessus pour vous assurer que le lien est sûr et qu'il correspond au site que vous recherchez.
- Au lieu de cliquer sur un lien ou un bouton dans un courriel pour accéder à un site, accédez directement au site en saisissant son URL dans votre barre d'adresse.
- Avant de partager des informations sensibles telles que votre date de naissance ou vos informations de paiement, vérifiez que la source avec laquelle vous partagez ces informations est légitime.
- Si une personne que vous connaissez vous envoie un message pour vous demander des informations sur votre organisation ou vous envoie un lien, appelez-la ou envoyez-lui directement un SMS pour vous assurer que la demande est légitime. Si un message semble suspect, il l'est probablement.

L'équipe de sécurité KnowBe4
KnowBe4.com