La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

Les meilleurs conseils pour utiliser en toute sécurité les médias sociaux

Vue d'ensemble

Les sites de médias sociaux tels que Snapchat, Facebook, Twitter, Instagram et LinkedIn sont des ressources incroyables, vous permettant de rencontrer, d'interagir et de partager avec des gens du monde entier. Cependant, tout ce pouvoir amène des risques, pas seulement pour vous, mais aussi pour votre famille, vos amis et votre employeur. Dans ce numéro, nous abordons les étapes clés pour tirer le meilleur parti des médias sociaux en toute sécurité.

Publications

Soyez prudent et réfléchissez avant de publier quelque chose. Tout ce que vous publiez deviendra probablement public à un moment donné, ce qui pourrait avoir une incidence sur votre réputation et votre avenir, y compris sur les endroits où vous pouvez aller dans le cadre de vos études ou sur les emplois que vous pouvez obtenir. Si vous ne voulez pas que votre famille ou votre patron voit vos publications, vous ne devriez probablement pas publier quoique ce soit. Soyez vigilant également sur ce que les autres publient à votre sujet. Vous devrez certainement demander aux autres de retirer ce qu'ils partagent à votre sujet.

Confidentialité

Presque tous les sites de médias sociaux offrent des options de confidentialité de haut niveau, il faut les activer dès que possible. Posez-vous les bonnes questions. Par exemple, est-ce vraiment indispensable que le site suive votre localisation? De plus, les options de confidentialité peuvent être déroutantes et changer souvent. Prenez l'habitude de vérifier et de confirmer qu'elles fonctionnent comme vous le souhaitez.

Phrases de passe

Sécurisez votre compte de médias sociaux avec une longue phrase d'authentification unique. Une phrase secrète est un mot de passe composé de plusieurs mots, ce qui facilite la saisie et la mémorisation, mais reste cependant difficile à deviner pour les cyber-attaquants.

Verrouiller votre compte

Activer l'authentification à deux facteurs sur tous vos comptes. Cela ajoute un code unique avec votre mot de passe lorsque vous devez vous connecter à votre compte. C'est en fait très simple et c'est l'un des moyens les plus puissants pour sécuriser votre compte.

Escroqueries

Tout comme dans les e-mails, les malfaiteurs tenteront de vous tromper en utilisant les messages des médias sociaux. Par exemple, ils peuvent essayer de vous soutirer votre mot de passe ou votre numéro de carte de crédit. Faites attention à ce sur quoi vous cliquez: si un ami vous envoie un message qui vous semble étrange, il pourrait s'agir d'un cyber-attaquant prétendant être votre ami.

Conditions d'utilisation

Connaître les conditions d'utilisation du site. Tout ce que vous postez ou téléchargez peut devenir la propriété du site.

Travail

Si vous voulez poster quelque chose sur votre travail, vérifiez d'abord avec votre superviseur pour vous assurer que le contenu est acceptable pour pouvoir le partager publiquement.

Suivez ces conseils pour profiter d'une expérience en ligne beaucoup plus sûre. Pour en savoir plus sur l'utilisation des sites de médias sociaux en toute sécurité ou signaler des activités non autorisées, consultez la page de sécurité de votre site de média social.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Jessica Barker est leader mondial dans la dimension humaine de la cybersécurité. Elle est la co-fondatrice de Redacted Firm, où elle fournit des services de conseil à des clients à travers le monde, et est une conférencière reconnue. Suivez-la sur Twitter à @drjessicabarker.

Sources

Phrases de passe :	https://www.sans.org/u/B6E
Vérification en deux étapes :	https://www.sans.org/u/B6J
Sécuriser les enfants en ligne d'aujourd'hui :	https://www.sans.org/u/B6O
Verrouillez votre connexion :	https://www.lockdownyourlogin.org/

Licence

OUCH! est publiée par le programme SANS « sécuriser l'humain » (Securing The Human) et est distribuée sous la licence « Creative Commons BY-NC-ND 4.0 ». La distribution de cette lettre d'information est autorisée tant que vous faites référence à la source, qu'elle n'a subie aucune modification et qu'elle n'est pas utilisée à des fins commerciales. Afin d'obtenir des traductions ou plus d'informations, merci de contacter www.sans.org/security-awareness/ouch-newsletter. Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduit par : Marilyn Combet