OUCH! | Juillet 2015

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

OUCH!

Dans ce numéro...

- Vue d'ensemble
- Vie privée
- Sécurité

Médias sociaux

Vue d'ensemble

Les sites de médias sociaux tels que Facebook, Twitter, Instagram et LinkedIn sont des ressources incroyables, vous permettant de rencontrer, d'échanger et de partager avec les gens à travers le monde. Cependant, toute cette puissance amène des risques, non seulement pour vous, mais également pour votre famille, vos amis et votre employeur. Dans ce numéro, nous expliquons ce que sont réellement ces dangers et comment utiliser ces sites en toute sécurité.

Editeur invité

Tanya Baccam est consultante en sécurité depuis de nombreuses années. Elle a été auteur et instructrice SANS plus d'une décennie y compris pour les cours SEC502, SEC542, SEC401, MGT414, AUD507 et encore pour de nombreux autres cours. Suivez-la sur Twitter à **@tbaccam**.

Vie privée

Une préoccupation commune avec les médias sociaux est de protéger vos renseignements personnels. Les dangers potentiels incluent:

- **Impact sur votre avenir** : Dans le cadre de la vérification d'antécédents, certaines entreprises effectuent des recherches au travers de sites de médias sociaux. Des photos ou des messages embarrassants ou incriminants, peu importe leur ancienneté, pourraient vous empêcher de vous faire embaucher ou d'être promu. En outre, de nombreuses universités procèdent à des contrôles similaires pour les nouvelles demandes des étudiants. Les options de confidentialité ne peuvent pas vous protéger tant que ces organismes peuvent vous demander de "Liker" ou rejoindre leurs pages ou que certains postes peuvent être archivés sur plusieurs sites.
- **Attaques contre vous** : Les cybers attaquants peuvent analyser vos messages et les utiliser pour accéder à vos informations ou à celles de votre organisation. Par exemple, ils peuvent utiliser les informations que vous partagez pour deviner les réponses à vos « questions secrètes » pour réinitialiser votre mot de passe en ligne, créer des attaques ciblées à l'encontre de messagerie appelées spearfishing, ou encore, appelez quelqu'un dans votre organisation se faisant passer pour vous. En outre, ces attaques peuvent se répandre dans le monde physique, comme l'identification de l'endroit où vous habitez ou travaillez.
- **Nuire accidentellement à votre employeur** : Des criminels ou concurrents peuvent utiliser toutes les informations sensibles que vous postez sur votre organisation contre votre employeur. En outre, vos messages peuvent potentiellement causer des dommages à la réputation de votre organisation. Soyez sûr de vérifier les politiques de votre organisation avant de poster quoi que ce soit à propos de votre travail. De plus, certains de vos messages de médias sociaux peuvent être surveillés.

La meilleure protection est de limiter ce que vous publiez. Certes, les options de confidentialité peuvent fournir une certaine protection, mais elles sont souvent source de confusion et changent souvent à votre insu. Ce que vous pensiez être privé peut rapidement devenir public pour diverses raisons. En outre, la confidentialité de vos messages est aussi sûre que les gens avec

Médias sociaux

lesquels vous partagez. Plus vous avez d'amis ou de contacts avec lesquels vous partagez des informations, plus il est probable que ces informations seront rendues publiques. Vous devez partir du principe que tout ce que vous postez peut ou deviendra public et fera partie intégrante d'Internet.

Enfin, soyez conscient de ce que vos amis affichent sur vous. S'ils affichent quelque chose avec lequel vous n'êtes pas à l'aise, demandez-leur de le supprimer. S'ils refusent ou vous ignorent, contactez le site de médias sociaux et demandez-lui de supprimer le contenu pour vous. De la même manière, soyez respectueux avec ce que vous publiez sur les autres.



Les sites de médias sociaux sont amusants et puissants, mais attention à ce que vous partagez et avec qui vous le faites.

Sécurité

En plus des problèmes de confidentialité, voici quelques mesures pour vous aider à protéger vos comptes de médias sociaux et vos activités en ligne.

- **Connexion** : Protéger chacun de vos comptes avec un mot de passe fort et unique et ne le partager pas avec quelqu'un d'autre. En outre, de nombreux sites de médias sociaux permettent l'authentification forte, comme la vérification en deux étapes. Activer toujours ces méthodes d'authentification fortes chaque fois que possible. Enfin, n'utilisez pas votre compte de médias sociaux pour vous connecter à d'autres sites car s'il est piraté alors tous vos comptes sont vulnérables.
- **Paramètres de confidentialité** : Si vous utilisez les paramètres de confidentialité, assurez-vous de les revoir et de les tester régulièrement. Les sites de médias sociaux changent souvent les paramètres de confidentialité et il est facile de faire une erreur. En outre, de nombreuses applications et services vous permettent de marquer votre position au contenu que vous publiez (appelé geotagging). Vérifiez régulièrement ces paramètres si vous souhaitez garder votre localisation privée.
- **Cryptage** : sites de médias sociaux utilisent le cryptage appelé HTTPS pour sécuriser vos connexions en ligne sur le site. Certains sites comme Twitter et Google+ permettent cela par défaut, tandis que d'autres exigent que vous activer manuellement le protocole HTTPS. Vérifiez vos paramètres de compte de médias sociaux et activer HTTPS comme la connexion par défaut chaque fois que possible.
- **Email** : Méfiez-vous des courriels qui prétendent provenir de sites de médias sociaux, ceux-ci peuvent facilement être falsifiés attaques envoyés par les cyber-criminels. La meilleure façon de répondre à ces messages est de vous connecter à votre site Web de médias sociaux directement, peut-être à partir d'un signet enregistré, puis lire et répondre à un message ou une notification sur le site.
- **malveillants Liens / Escroqueries** : Soyez prudent de liens suspects ou les escroqueries potentielles affichées sur les sites de médias sociaux. Les méchants utilisent les médias sociaux pour diffuser leurs propres attaques. Juste parce qu'un message est envoyé par un ami ne veut pas dire que ce message est vraiment d'eux, leur compte peut avoir été compromise. Si un membre de la famille ou un ami a posté un message étrange que vous ne pouvez pas vérifier (tels qu'ils ont été volés et ont besoin d'envoyer de l'argent), les appeler sur leur téléphone mobile ou d'autres moyens pour confirmer le message est vraiment d'eux.

Médias sociaux

- **Applications mobiles** : La plupart des sites de médias sociaux offrent des applications mobiles pour accéder à vos comptes en ligne. Assurez-vous de télécharger ces applications mobiles à partir d'un site de confiance et que votre smartphone est protégé par un mot de passe fort. Si votre smartphone est déverrouillé lorsque vous perdez, tout le monde peut accéder à vos sites de médias sociaux grâce à votre smartphone et commencer à poster que vous.

Sites de médias sociaux sont une merveilleuse façon de communiquer et de rester en contact avec le monde. Si vous suivez les conseils décrits ici, vous devriez être en mesure de profiter d'une expérience en ligne plus sûr. Pour en savoir plus sur la façon d'utiliser vos sites de médias sociaux en toute sécurité ou pour signaler toute activité non autorisée, consultez la fiche de sécurité de votre site de média social.

Ressources publiques

N'utilisez jamais les ordinateurs publics, tels que ceux que l'on trouve dans les halls d'hôtels, les librairies ou les cybers cafés. Vous n'avez aucune idée de qui a pu utiliser cet ordinateur avant vous, il se peut que cette personne ait, volontairement ou involontairement, infecté cet ordinateur. Lorsque cela est possible, n'utilisez que des appareils que vous contrôlez et auxquels vous faîtes confiance pour vos activités en ligne. Si vous n'avez d'autre choix que d'utiliser un ordinateur public, n'utilisez aucun service qui vous demande de vous identifier ou d'entrer un mot de passe.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients.
Pour en savoir plus, veuillez vous référer aux liens suivants :
http://www.answersolutions.ch et http://answersecurity.com/

Sources

Phrases de passe : http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_fr.pdf

La vérification en deux étapes : http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_fr.pdf

Utiliser les applications mobiles de manière sécurisée :

http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201501_fr.pdf

Eduquer les enfants à la sécurité informatique : http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201506_fr.pdf

La sécurité pour tous (Facebook) : https://www.facebook.com/safety

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet