OUCH! | Julho de 2015

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Mídias Sociais

Visão Geral

Sites de mídias sociais como Facebook, Twitter, Instagram e Linkedin são recursos incríveis que permitem encontrar, interagir e compartilhar com pessoas ao redor do mundo. Mas com todo esse poder vêm os riscos, não apenas para você mas para sua família, amigos e empregador. Nesta edição explicamos que riscos são esses e como utilizar esses sites de forma segura.

Editor Convidado

Tanya Baccam é uma consultora de segurança de longa data. Ela tem sido uma autora e instrutora SANS por mais de uma década, incluindo para os cursos SEC502, SEC542, SEC401, MGT414, AUD507 e muitos outros. Siga-a no Twitter em **@tbaccam**.

Privacidade

Uma preocupação comum com mídias sociais é proteger suas informações pessoais. Perigos pontenciais incluem:

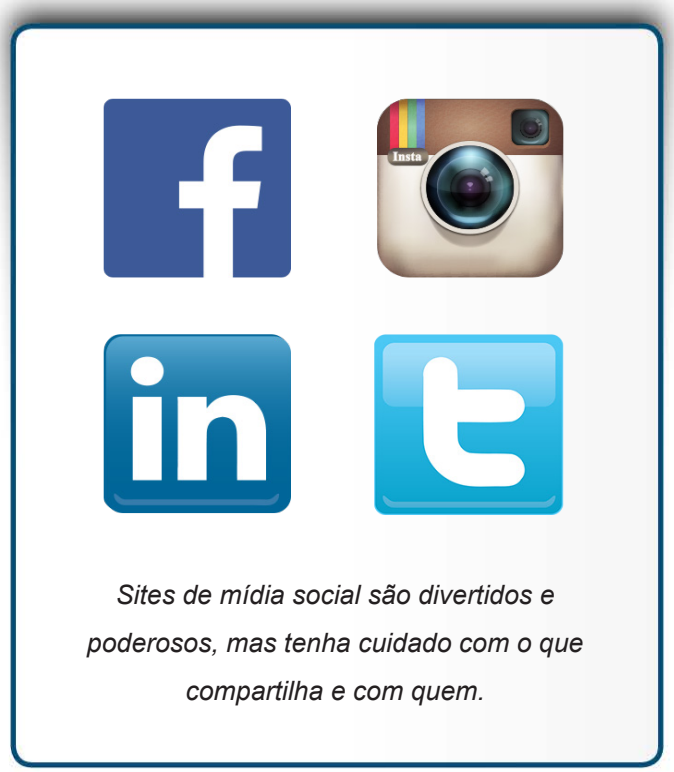
- **Impacto no seu futuro**: Algumas organizações pesquisam sites de mídias sociais como parte da investigação de perfil. Publicações ou fotos embaraçosas ou imcriminatórias, independente de quão antigas, podem impedir que seja contratado ou promovido. Adicionalmente, muitas universidades conduzem verificações parecidas com candidatos novos. Opções de privacidade podem não lhe proteger pois as empresas podem pedir que você “Curta” ou siga suas páginas. Ou algumas publicacões suas podem ser propagadas e arquivadas em múltiplos sites;
- **Ataques contra você**: Atacantes cibernéticos podem analisar suas publicações e utilizá-las para obter acesso às suas informações ou de sua organização. Por exemplo, eles podem utilizar a informação que você compartilha para adivinhar as respostas para suas “perguntas secretas” e trocar suas senhas online, criar ataques direcionados por e-mail, chamados spearphishing ou ligar para alguém na sua organização fingindo ser você. Além disso esses ataques podem vazar para o mundo real, como identificar onde você trabalha ou mora;
- **Causar danos acidentais ao seu empregador**: Criminosos ou competidores podem usar qualquer informação sigilosa que você publique sobre sua organização, contra seu empregador. Adicionalmente, suas publicações podem potencialmente causar danos de reputação para sua organização. Certifique-se de verificar as políticas da sua organização antes de publicar qualquer coisa sobre seu emprego. Além disso, algumas de suas publicações em mídias sociais podem ser monitoradas.

A melhor proteção é limitar o que você publica. Sim, opções de privacidade podem prover alguma proteção, mas elas são muitas vezes confusas e mudam frequentemente sem o seu conhecimento. Aquilo que você pensava ser privativo pode rapidamente se tornar público por várias razões. Adicionalmente, a privacidade das suas publicações é tão segura quanto as pessoas com quem compartilha. Quanto maior a quantidade de amigos ou contatos com quem compartilha, mais provavelmente essa informação se tornará pública.

Mídias Sociais

Você deve assumir que qualquer coisa que publica pode ou vai se tornar pública e parte permanente da Internet.

Finalmente, certifique-se do que seus amigos estão publicando sobre você. Se eles publicarem algo que não lhe agrade, peça que retirem. Caso se recusem ou ignorem, contacte o site de mídia social e peça que removam o conteúdo para você. Da mesma forma, seja respeitoso sobre o que você publica sobre as outras pessoas.



Sites de mídia social são divertidos e poderosos, mas tenha cuidado com o que compartilha e com quem.

Segurança

Adicionalmente às preocupações com a privacidade, seguem alguns passos de proteção para suas contas de mídia social e atividades online:

- **Login**: Proteja cada uma de suas contas com uma senha forte e única e não a compartilhe com ninguém. Além disso, muitos sites de mídias sociais suportam autenticação mais forte como as de verificação em duas etapas. Sempre que possível habilite esses métodos de autenticação mais fortes. Finalmente, não utilize sites de mídia social para se logar em outros sites pois se eles forem hackeados, sua conta estará vulnerável;
- **Opções de Privacidade**: Se você utiliza opções de privacidade, certifique-se de revisá-las e testá-las regularmente. Sites de mídias sociais mudam frequentemente suas opções de privacidade e torna-se fácil cometer um erro. Além disso, muitos aplicativos e serviços permitem a você marcar sua localização no conteúdo que publica (chamado georeferenciamento). Verifique regularmente essas opções se você deseja manter sua localização física privativa;
- **Criptografia**: Sites de mídias sociais utilizam uma criptografia chamada HTTPS para proteger suas conexões online com o site. Alguns como Twitter e Google+ habilitam isto como padrão, enquanto outros requerem que você a habilite manualmente. Verifique as configurações da sua conta de mídia social e habilite o HTTPS como conexão padrão sempre que possível;
- **Email**: Suspeite de e-mails que digam vir de sites de mídias sociais pois podem ser facilmente um ataque de spoofing (falsificação do remetente) vindo de criminosos cibernéticos. A forma mais segura de responder essas mensagens é entrar na sua conta através da página da rede social oficial na Internet, eventualmente através de um link previamente salvo como bookmark, e então ler e responder qualquer mensagem ou notificação por ali;
- **Links maliciosos/Golpes**: Seja cauteloso com links suspeitos ou golpes potenciais publicados em redes sociais. Os atacantes utilizam mídiais sociais para espalhar seus ataques. Uma mensagem publicada por um amigo não significa que ela tenha sido enviada por ele pois sua conta pode ter sido comprometida. Se um membro da família ou amigo publica uma mensagem ímpar que você não possa verificar (como contando que tenha sido roubado e precisa que lhe envie dinheiro), ligue para ele em seu telefone celular ou através de outro recurso, para confirmar que a mensagem tenha sido enviada por ele;

Mídias Sociais

- **Aplicativos Móveis**: Muitos sites de mídia social oferecem aplicativos móveis para acessar suas contas online. Certifique-se de baixar esses aplicativos de um site confiável e que seu smartphone esteja protegido com uma senha forte. Se seu smartphone estiver destravado quando perdê-lo, qualquer um poderá acessar seus sites de rede social através dele e começar a publicar em seu nome.

Sites de mídia social são um caminho maravilhoso para se comunicar e manter contato com o mundo. Se você seguir as dicas esboçadas aqui, poderá curtir uma experiência online mais segura. Para saber mais sobre como utilizar mídias sociais de forma segura ou relatar atividade não autorizada, verifique a página de segurança do site da sua rede social.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em http://www.securingthehuman.org.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte
Katia Lucia da Silva, Arquiteta de T/I, Tradutora - twitter.com/kl_silva

Fontes

Frases Secretas:	http://www.securingthehuman.org/ouch/2015#april2015
Verificação em duas etapas:	http://www.securingthehuman.org/ouch/2013#august2013
Usando aplicativos móveis de forma segura:	http://www.securingthehuman.org/ouch/2015#january2015
Educando os filhos em segurança cibernética:	http://www.securingthehuman.org/ouch/2015#june2015
Central de Segurança da Família:	https://www.facebook.com/safety

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traduzida por: Homero Palheta Michelini, Michel Girardias, Katia Lucia da Silva, Rodrigo Gularte, Marta Visser