A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

OUCH!

Nesta edição

Redes Sociais com Segurança

EDITOR CONVIDADO

Ted Demopoulos é o editor convidado desta edição. Ele é consultor de segurança de longa data e tem ministrado cursos SANS há uma década, incluindo SEC401/501 e MGT414/512. Saiba mais sobre o Ted em http://demop.com.

VISÃO GERAL

Sites de redes sociais como Facebook, Twitter, Google+, Pinterest e LinkedIn são poderosos, permitem a você encontrar, interagir e compartilhar com pessoas ao redor do mundo. Mas, com todos esses recursos vêm os riscos, não somente para você mas também para sua família. Nesta edição vamos ver que riscos são esses e como utilizar estes sites com mais segurança.

PRIVACIDADE

Uma preocupação comum sobre redes sociais é a privacidade, a proteção de suas informações pessoais e informações confidenciais de outros. Perigos potenciais incluem:

- **Impacto no seu futuro:** Muitas organizações vasculham sites de redes sociais ao fazerem verificação de perfil pessoal. Publicações embaraçosas ou incriminatórias, independente de quão antigas são, podem atrapalhar uma contratação ou promoção. Além disso, muitas universidades, especialmente no exterior, conduzem verificações similares em novos candidatos. Opções de privacidade podem não te proteger, pois essas empresas pedem que você "curta" ou siga suas páginas antes do processo de inscrição;
- **Ataques à sua pessoa**: Criminosos cibernéticos podem obter informações pessoais e utilizá-las para atacar você. Por exemplo, podem utilizar suas informações pessoais para adivinhar as respostas das "perguntas secretas" que liberam suas senhas de Internet, criar ataques de email chamados "Phishing" ou pedir cartões de crédito em seu nome. Além disso, esses ataques podem recair no mundo real, como ao identificar onde você vive ou trabalha;
- **Prejudicar seu funcionário:** Criminosos ou concorrentes podem utilizar qualquer informação confidencial sobre sua empresa contra seus funcionários. Além disso, suas publicações podem causar prejuízos de reputação à sua empresa. Certifique-se de verificar a política da sua empresa antes de publicar alguma coisa sobre ela.

A melhor proteção é limitar a informação que publica. Sim, opções de privacidade podem dar alguma proteção. Mas

Redes Sociais com Segurança

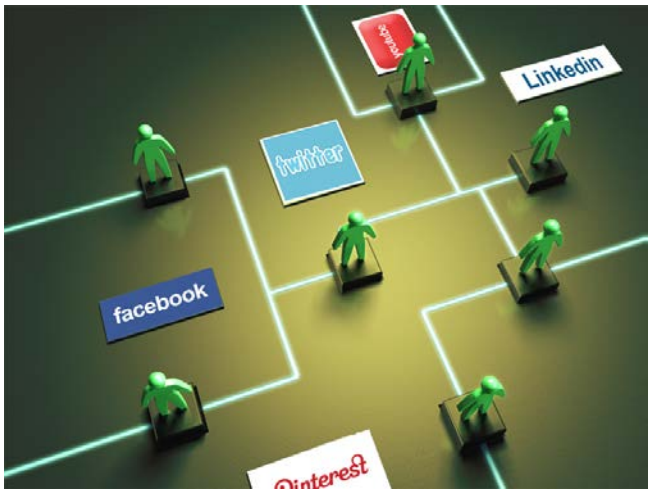
tenha em mente que opções de privacidade são muitas vezes confusas e podem mudar frequentemente sem seu conhecimento. O que você pensava ser privado pode tornar-se público por uma variedade de motivos. Além disso, a privacidade da sua informação é tão segura quanto as pessoas com quem compartilha. Quanto mais pessoas ou amigos você tem para compartilhar informações confidenciais, mais provavelmente essa informação se tornará pública. Finalmente, a melhor maneira de proteger sua privacidade é seguir essa regra: se você não quer que sua mãe ou chefe veja sua publicação, provavelmente não deveria publicá-la.

Além disso, esteja ciente de quais informações seus amigos publicam sobre você. Elas também podem ser prejudiciais ao incluírem informações privativas ou fotos embaraçosas suas. Certifique-se de que seus amigos entendam o que podem e não podem publicar sobre você. Se publicarem algo com o que não esteja confortável, peça que retirem. Da mesma forma, seja respeitoso com suas publicações sobre eles.

SEGURANÇA

Adicionalmente às questões de privacidade, sites de redes sociais podem ser utilizados por criminosos cibernéticos para atacar seus aparelhos. Aqui vão alguns passos para proteger-se:

- **Contas:** Proteja sua conta de rede social com uma senha forte e não compartilhe esta senha com ninguém ou reutilize em outros sites. Além disso, alguns sites de rede social têm a opção de autenticação forte, como verificação de dois passos. Habilite o método de autenticação forte sempre que possível;
- **Criptografia:** Muitos sites de rede social permitem que você utilize criptografia com o conhecido HTTPS para proteger sua conexão com o site. Alguns sites comoTwitter e Google+ o habilitam por padrão, enquanto outros requerem que você o habilite manualmente, na configuração da sua conta. Sempre que possível utilize HTTPS;
- **Email:** Suspeite de emails que dizem vir de sites de redes sociais. Eles podem facilmente ser ataques enviados por criminosos cibernéticos. A maneira mais segura para responder essas mensagens é entrar no site diretamente, talvez por um link armazenado como favorito no seu navegador de Internet, e verificar qualquer mensagem ou notificação utilizando o próprio site;
- **Links maliciosos / Golpes**: Seja cauteloso com links suspeitos ou golpes potenciais publicados em sites de redes sociais. Criminosos cibernéticos podem publicar



Sites de rede social são poderosos e divertidos mas tenha cuidado com o que publica e em quem você confia.

Redes Sociais com Segurança

links maliciosos e, se você clicar neles, podem levá-lo a sites que tentam infectar seu computador. Além disso, só por que uma mensagem foi publicada por um amigo não significa que é dele, pois sua conta pode ter sido comprometida. Se um parente ou amigo publicou uma mensagem estranha que você não pode verificar, (como se tenha sido roubado e precisa que envie dinheiro), ligue para ele para confirmar;

- Aplicativos: Alguns sites de redes sociais oferecem o recurso de adicionar ou instalar aplicativos de terceiros, como jogos. Tenha em mente que há pouco ou nenhum controle de qualidade ou revisão nesses aplicativos. Eles podem ter acesso completo à sua conta e informações privativas. Só instale aplicativos que conheça, que sejam de fonte conhecida e sites de Internet confiáveis. E remova-os quando não precisar mais deles.

Sites de rede social são formas poderosas e divertidas de se comunicar com o mundo. Ao seguir as dicas informadas aqui você poderá curtir uma experiência muito mais segura na Internet. Para mais informações sobre como utilizar sites de rede social de forma segura ou reportar atividade não autorizada, verifique as páginas de segurança dos próprios sites de rede social que utiliza.

RECURSOS

Alguns dos links abaixo foram abreviados para melhorar a leitura utilizando o serviço TinyURL. Para reduzir riscos de segurança, o OUCH! Sempre usa o recurso de pré visualização do TinyURL, que mostra o destino final do link e sempre pede sua permissão para prosseguir.

11 dicas de segurança para Redes Sociais (em Inglês):
http://preview.tinyurl.com/b28a525

Segurança no FB (Facebook):
https://www.facebook.com/safety

Suas configurações de segurança do FB:
https://www.facebook.com/settings?tab=security

Termos de Segurança (em Inglês):
http://preview.tinyurl.com/6wkpae5

CERT.br – Glossário de segurança:
http://cartilha.cert.br/glossario/

Dica de segurança SANS do Dia (em Inglês):
http://preview.tinyurl.com/6s2wrkp

SAIBA MAIS

Assine a publicaçãomensal OUCH! de sensibilização de segurança, acesse os arquivos OUCH! e aprenda mais sobre as soluções de sensibilização de segurança do SANS nos visitando 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

Time Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner