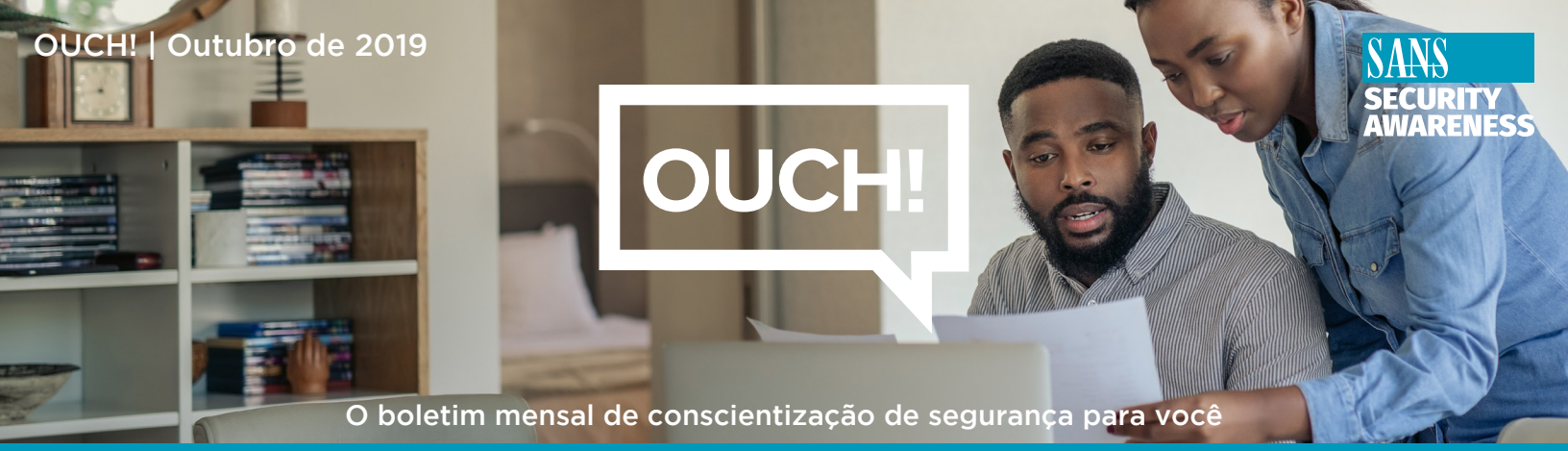

O boletim mensal de conscientização de segurança para você

Quatro etapas simples para estar protegido

Visão geral

Aproveitar ao máximo a tecnologia com segurança pode parecer desgastante e confuso. No entanto, independentemente da tecnologia que você está usando ou de como está usando, aqui estão quatro etapas simples que ajudarão você a se manter seguro.

1. Você: Em primeiro lugar, a tecnologia sozinha não pode protegê-lo completamente; você é sua melhor defesa. Os atacantes cibernéticos aprenderam que a maneira mais fácil de conseguir o que querem é direcioná-lo a você, em vez de ao seu computador ou a outros dispositivos. Se eles querem sua senha, cartão de crédito ou controlar o seu computador, tentarão induzi-lo a fornecer a eles, normalmente criando um senso de urgência. Por exemplo, eles podem ligar para você fingindo ser o suporte técnico da Microsoft e alegar que seu computador está infectado, quando na verdade são apenas atacantes cibernéticos querendo que você lhes dê acesso ao seu computador. Ou talvez eles enviem um e-mail avisando que seu pacote não pôde ser entregue e pressionando-o para clicar em um link confirmando seu endereço de correspondência, quando na verdade estão enganando você para acessar um site malicioso que invadirá seu computador. No final das contas, a melhor defesa contra atacantes é você. Usando o bom senso, você pode detectar e parar muitos ataques.

2. Frases secretas: As velocidades modernas da computação tornaram a antiga senha de 8 caracteres desatualizada e vulnerável. Quando um site solicita que você crie uma senha, crie uma senha forte e única. Uma frase secreta é um tipo de senha que usa uma série de palavras fáceis de lembrar, como “o rato roeu a roupa”. Quanto maior for a sua senha, mais forte será. Uma senha única significa usar uma diferente para cada dispositivo ou conta online. Dessa forma, se uma senha for comprometida, todas suas outras contas e dispositivos ainda estarão protegidos. Não consegue se lembrar de todas essas senhas? Use um gerenciador de senhas, que é um programa especializado que armazena com segurança todas suas senhas em um formato criptografado (e oferece muitos outros ótimos recursos também).

Por último, ative a verificação em duas etapas (também chamada de autenticação de dois ou vários fatores). Usa sua senha, mas também adiciona uma segunda etapa, como inserir um código enviado ao seu smartphone ou a partir de um aplicativo que gera o código para você. Ativar a verificação em duas etapas é provavelmente a etapa mais importante que você pode realizar para proteger suas contas online e é muito mais fácil do que imagina..

3. Atualização: verifique se cada um de seus computadores, dispositivos móveis, programas e aplicativos está executando a versão mais recente do software. Os atacantes cibernéticos estão constantemente procurando novas vulnerabilidades no software usado em seus dispositivos. Quando eles descobrem vulnerabilidades, usam programas especiais para explorá-las e invadir os dispositivos que você está usando. Enquanto isso, as empresas que criaram o software para esses dispositivos estão trabalhando arduamente para corrigi-las, lançando atualizações. Ao garantir que seus computadores e dispositivos móveis instalem essas atualizações imediatamente, você dificultará bastante a invasão de alguém. Para se manter atualizado, basta ativar a atualização automática sempre que possível. Essa regra se aplica a praticamente qualquer tecnologia conectada a uma rede, incluindo TVs conectadas à Internet, babás eletrônicas, câmeras de segurança, roteadores domésticos, consoles de videogame ou até mesmo seu carro.

4. Backups e Recuperação: Às vezes, por mais cuidadoso que seja, você ainda pode ser invadido. Se for esse o caso, normalmente a única maneira de restaurar todas as suas informações pessoais é por meio do backup. Certifique-se de fazer backups periódicos de qualquer informação importante e verifique se é possível restaurar seus dados a partir deles. A maioria dos sistemas operacionais e dispositivos móveis conta com suporte de backups automáticos, em unidades externas ou na nuvem.

Editor convidado

*O instrutor certificado do SANS **Steve Anson**;oferece orientação para equipes de segurança de TI e governos em todo o mundo para melhorar sua postura de segurança. Steve lançará em breve seu livro Applied Incident Response e também oferece recursos gratuitos para profissionais de segurança de TI no site AppliedIncidentResponse.com.*

Recursos

Engenharia Social:	https://www.sans.org/u/W3G
Golpes personalizados:	https://www.sans.org/u/W3Q
Simplificando as senhas:	https://www.sans.org/u/W3V
Tem Backups:	https://www.sans.org/u/W40