O boletim mensal de conscientização de segurança para você

Navegadores

Visão geral

Navegadores como Google Chrome, Microsoft Edge, Apple Safari ou Mozilla Firefox são uma das formas mais comuns de interação com a Internet. Nós os usamos para ler as notícias, ver e-mails, fazer compras online, assistir a vídeos e jogar games. Como resultado, os navegadores também são alvos de ataques cibernéticos.
Muitas pessoas assumem que navegar online é seguro se você visitar apenas sites conhecidos e confiáveis. No entanto, é muito fácil clicar ou visitar acidentalmente um site inseguro na internet, às vezes sem saber. Além disso, os próprios sites que você conhece e confia podem ser invadidos, com atacantes cibernéticos instalando software malicioso neles. Finalmente, os navegadores atuais têm muitos recursos novos, que muitas vezes podem ser confusos e, se configurados incorretamente, expõem você a ainda mais perigos.

Aproveitando seu navegador com segurança

Confira aqui os principais passos para se proteger:

Atualização: Use sempre a versão mais recente do seu navegador. Os navegadores atualizados têm os patches de segurança mais recentes e são muito mais seguros. Com os computadores de hoje, isso se tornou muito mais fácil, pois você simplesmente permite a atualização automática no seu sistema. Ou, para alguns navegadores, você só reinicia o navegador sempre que ele informa que há uma nova atualização. Após uma atualização, verifique se há novos recursos de segurança dos quais pode se beneficiar.

Alertas: os navegadores atuais normalmente reconhecem determinados sites maliciosos projetados para prejudicar você. Se o seu navegador avisar que o site que você está prestes a visitar é perigoso, feche a guia do navegador e encontre o que você precisa em um site diferente.

Sincronização: nunca sincronize seu navegador de trabalho com seu navegador pessoal ou qualquer conta pessoal. A sincronização é quando você permite que navegadores em dispositivos diferentes se comuniquem entre si e compartilhem suas informações de navegação, como histórico de navegação, favoritos e conteúdo salvo.

Senhas: Muitos navegadores suportam a opção de salvar suas senhas em sites diferentes. Em vez de armazenar suas senhas no seu navegador, recomendamos que use um gerenciador de senhas dedicado. Os gerenciadores de senhas são um aplicativo de segurança separado que possui muito mais recursos e funcionalidades de segurança.

Plug-ins: Plug-ins ou extensões são pequenos softwares adicionados aos navegadores que podem adicionar funcionalidades. No entanto, cada novo plug-in adicionado também pode adicionar mais vulnerabilidades. Para seu computador de trabalho, adicione apenas plug-ins autorizados e aprovados e, assim como seu navegador, mantenha-os atualizados. Remova os plug-ins que você não usa mais.

Modo de Privacidade: A maioria dos navegadores oferece uma opção de privacidade (também conhecida como"modo anônimo "). Isso significa que, ao abrir uma guia do navegador no modo de privacidade, limita quais informações são coletadas sobre você. Por exemplo, seu navegador não coleta cookies, não rastreia o histórico de navegação e não armazena nem distribui informações confidenciais sobre você.

Chat ao vivo: agora alguns sites oferecem um recurso de bate-papo ao vivo no qual você pode fazer perguntas. Apenas participe desses bate-papos online em sites conhecidos e confiáveis. Além disso, limite as informações que você compartilha durante uma sessão de chat ao vivo, pois você não sabe realmente quem está coletando suas informações, o que está fazendo com elas e para quem pode estar vendendo ou compartilhando.

Cuidado com o controle remoto: Sites fraudulentos tentarão invadir seu computador postando um falso aviso pop-up de segurança em seu navegador avisando que seu computador está infectado e pressionando você para uma sessão de bate-papo online para consertar seu computador. Eles solicitarão urgentemente que você permita que instalem um agente remoto a fim de permitir que eles consertem seu computador. Na realidade, seu computador está bem. Em vez disso, eles estão tentando induzi-lo a instalar software malicioso para que possam roubar suas senhas e seus dados e rastrear todas as suas atividades online.

Log Off: Quando você terminar de visitar um site, certifique-se de fazer logoff para remover informações confidenciais de login e senha antes de fechar o navegador.

Editor Convidado

Dean Parsons é o CEO da ICS Defense Force, possui mais de 20 anos de experiência em defesa cibernética de TI/ICS. Ele também é instrutor certificado de SANS para ICS515 e coautor/instrutor de ICS418, ensinando defesa cibernética ativa, resposta a incidentes, liderança e gerenciamento de riscos para sistemas de controle industrial. www.linkedin.com/in/dean-parsons-cybersecurity.

Recursos

Gerenciadores de senhas: https://www.sans.org/newsletters/ouch/password-managers/
Atualização: https://www.sans.org/newsletters/ouch/the-power-of-updating
Engenharia Social: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Protegendo sua pegada digital: https://www.sans.org/newsletters/ouch/privacy/

Traduzido para a Comunidade por: David Boldrin