Laboratório – Descobrir seu próprio comportamento arriscado on-line

Objetivos

Conheça as ações realizadas on-line que possam comprometer sua segurança ou privacidade.

Histórico/Cenário

A Internet é um ambiente hostil, e você deve permanecer vigilante para garantir que seus dados não sejam comprometidos. Os invasores são criativos e tentarão usar várias técnicas diferentes para enganar os usuários. Este laboratório ajuda a identificar o comportamento on-line arriscado e dá dicas sobre como ter mais segurança on-line.

Parte 1: Confira os Termos da Política de Serviços

Responda às perguntas abaixo com sinceridade e tome nota de quantos pontos ganha em cada resposta. Some todos os pontos e passe para a Parte 2 para fazer uma análise de seu comportamento on-line.

a. Que tipo de informação você compartilha com sites de mídia social?

1) Tudo. Eu dependo de mídias sociais para manter contato com meus amigos e familiares. (3 pontos)
2) Artigos e notícias que eu encontro ou leio (2 pontos)
3) Depende. Filtro tudo o que compartilho e com quem compartilho. (1 ponto)
4) Nada. Eu não uso mídias sociais. (0 pontos)

b. Quando cria uma nova conta em um serviço on-line, você:

1) Reutiliza a mesma senha usada em outros serviços para torná-la mais fácil de lembrar. (3 pontos)
2) Cria a senha mais fácil possível, para conseguir lembrar-se dela. (3 pontos)
3) Cria uma senha muito complexa e a armazena em um serviço de gerenciamento de senha. (1 ponto)
4) Cria uma nova senha que é semelhante a uma senha usada em outro serviço. (1 ponto)
5) Cria uma senha forte inteiramente nova. (0 pontos)

c. Quando você recebe um e-mail com links para outros sites:

1) Não clica no link, porque você nunca segue links enviados para via e-mail. (0 pontos)
2) Clica nos links porque o servidor de e-mail já analisou o e-mail. (3 pontos)
3) Clica em todos os links, se o e-mail tiver vindo de uma pessoa que conhece. (2 pontos)
4) Passa o mouse sobre os links para verificar o URL de destino antes de clicar. (1 ponto)

d. Uma janela pop-up é exibida quando você visita um site. Ele afirma que seu computador está em risco, e você deve fazer download de um programa de diagnóstico e instalá-lo para torná-lo seguro:

1) Você clica no programa, faz download dele e o instala para manter seu computador em segurança. (3 pontos)
2) Inspeciona as janelas pop-up e passa o mouse sobre o link para verificar sua validade. (3 pontos)
3) Ignora a mensagem, certificando-se de que não clicar nele ou fazer download do programa e fechar o site. (0 pontos)

e. Quando precisa fazer login no site de seu banco para realizar uma tarefa, você: _____

   1) Insere suas informações de login imediatamente. (3 pontos)

   2) Confere a URL para garantir que é a instituição que procurava antes de inserir qualquer informação. (0 pontos)

   3) Você não usa online banking ou qualquer outro serviço financeiro on-line. (0 pontos)

f. Você leu sobre um programa e decide experimentá-lo. Procura na Internet e encontra uma versão de teste em um site desconhecido, você:

   1) Imediatamente faz download do programa e o instala. (3 pontos)

   2) Pesquisa outras informações sobre o criador do programa antes de fazer download dele. (1 pontos)

   3) Não faz download do programa em o instala. (0 pontos)

g. Você encontra uma unidade de USB enquanto caminha para o trabalho. Você:

   1) Pega e conecta em seu computador para verificar o conteúdo. (3 pontos)

   2) Pega e conecta em seu computador para apagar completamente o conteúdo antes de reutilizá-lo. (3 pontos)

   3) Pega e conecta em seu computador para executar uma verificação de antivírus antes de reutilizá-lo para os seus próprios arquivos (3 pontos)

   4) Não pega. (0 pontos)

h. Você precisa se conectar à Internet e encontra um hotspot com WiFi livre. Você:

   1) Conecta o pen drive e usa a Internet. (3 pontos)

   2) Não conecta e espera até ter uma conexão confiável. (0 pontos)

   3) Conecta e estabelece uma VPN com um servidor confiável antes de enviar qualquer informação. (0 pontos)

Parte 2: Analise seu comportamento on-line

Quanto maior sua pontuação, menos seguro é seu comportamento on-line. O objetivo é ser 100% seguro ao ter atenção a todas as suas interações on-line. Isso é muito importante porque basta um erro para comprometer seu computador e seus dados.

Some os pontos da Parte 1. Registre a pontuação.

0: Você está muito seguro on-line.

0–3: Você está razoavelmente seguro on-line mas ainda deve mudar seu comportamento para ter total segurança.

3–17: Você tem um comportamento inseguro on-line e corre alto risco de comprometer-se.

18 ou mais: Você tem muito pouca segurança on-line e será comprometido.

Veja abaixo algumas dicas importantes de segurança on-line.

a. Quanto mais informações você compartilhar na mídia social, mais fácil é para um invasor conhecê-lo. Com mais conhecimento, um invasor pode criar um ataque muito mais bem direcionado. Por exemplo, ao compartilhar com o mundo que você foi para uma corrida de carros, um invasor pode criar um e-mail malicioso da empresa de venda de ingressos responsável pelo evento de corrida. Como você acabou de ir ao evento, o e-mail parecerá mais confiável.

b. Reutilizar senhas é um péssimo hábito. Se você reutilizar uma senha em um serviço que está sob controle dos invasores, eles poderão ser bem sucedidas ao tentar conectar-se como você em outros serviços.

c. E-mails podem ser facilmente forjados para parecerem legítimos. E-mails falsos costumam ter links para sites mal-intencionados ou malware. Como regra geral, não clique em links incorporados recebidos via e-mail.

d. Não aceite nenhum software não solicitado, especialmente se vier de uma página da Web. É extremamente improvável que uma página da Web ofereça uma atualização de software legítima para você. É altamente recomendável fechar o navegador e usar as ferramentas de sistema operacional para verificar as atualizações.

e. Páginas da Web maliciosas podem facilmente ser feitas para parecerem um site de banco ou instituição financeira. Antes de clicar em links ou dar qualquer informação, verifique a URL para certificar-se de que é a página da Web correta.

f. Quando você permite que um programa seja executado em seu computador, você dá a ele muito poder. Tenha sabedoria ao permitir a execução de um programa. Faça uma pesquisa para certificar-se de que a empresa ou indivíduo por trás do programa é um autor sério e legítimo. Também, só faça download do programa do site oficial da empresa ou individual.

g. Unidade de USB e pen drives incluem um pequeno controlador para permitir que computadores se comuniquem com ele. É possível infectar esse controlador e orientá-lo a instalar software mal-intencionado no computador host. Porque o malware é hospedado no controlador USB em si e não na área de dados. Apagar ou fazer varredura antivírus não vão detectar o malware.

h. Os invasores poderão implantar hotspots de WiFi falsos para atrair os usuários. Como o invasor tem acesso a todas as informações trocadas através o hotspot comprometido, os usuários conectados a esse hotspot estão em risco. Nunca use hotspots de WiFi desconhecidos sem criptografar seu tráfego através de uma VPN. Nunca forneça dados confidenciais como números de cartão de crédito enquanto estiver usando uma rede desconhecida (com ou sem fio).

Reflexão

Depois de analisar seu comportamento on-line, que mudanças faria para proteger-se on-line?