Laboratório – Descobrir os seus comportamentos online de risco

Objetivos

Explore ações realizadas online que podem comprometer a sua segurança ou privacidade.

Contexto/cenário

A Internet é um ambiente hostil e deve manter-se atento para garantir que os seus dados não ficam comprometidos. Os atacantes são criativos e tentarão muitas técnicas diferentes para ludibriar os utilizadores. Este laboratório ajuda-o a identificar comportamentos online de risco e apresenta sugestões para aumentar a segurança online.

Parte 1: Explorar a política de Termos de Serviço

Responda honestamente às perguntas abaixo e tome nota dos pontos obtidos em cada resposta. Some todos os pontos até obter uma pontuação total e avance para a Parte 2 para uma análise do seu comportamento online.

a. Que tipo de informação partilha nos sites de redes sociais?

1) Tudo; utilizo as redes sociais para me manter em contacto com amigos e familiares. (3 pontos)
2) Artigos e notícias que encontro ou leio (2 pontos)
3) Depende; filtro o conteúdo que partilho e com quem partilho. (1 ponto)
4) Nada; não utilizo as redes sociais. (0 pontos)

b. Quando cria uma nova conta num serviço online:

1) Reutiliza a mesma palavra-passe utilizada noutros serviços para que seja mais fácil lembrar-se. (3 pontos)
2) Cria uma palavra-passe tão simples quanto possível para que consiga lembrar-se. (3 pontos)
3) Cria uma palavra-passe muito complexa e armazena-a num serviço de gestão de palavras-passe. (1 ponto)
4) Cria uma nova palavra-passe semelhante a uma palavra-passe utilizada noutro serviço, mas diferente. (1 ponto)
5) Cria uma palavra-passe forte totalmente nova. (0 pontos)

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

1) Não clica na ligação porque nunca segue ligações que lhe são enviadas por e-mail. (0 pontos)
2) Clica nas ligações porque o servidor de e-mail já analisou o e-mail. (3 pontos)
3) Clica em todas as ligações se o e-mail tiver sido enviado por uma pessoa que conhece. (2 pontos)
4) Passa o ponteiro do rato sobre as ligações para verificar o URL de destino antes de clicar. (1 ponto)

d. Quando visita um Web site, é apresentada uma janela de pop-up. Esta indica que o seu computador está em risco e que deve transferir e instalar um programa de diagnóstico para torná-lo seguro:

1) Clica, transfere e instala o programa para manter o seu computador seguro. (3 pontos)
2) Inspeciona as janelas de pop-up e passa o ponteiro do rato sobre a ligação para verificar a respetiva validade. (3 pontos)
3) Ignora a mensagem, certificando-se de que não clica na mesma nem transfere o programa e fecha o Web site. (0 pontos)

e. Quando necessita de iniciar sessão no Web site da sua instituição financeira:

   1) Introduz imediatamente as suas informações de início de sessão. (3 pontos)

   2) Antes de introduzir quaisquer informações, verifica o URL para se assegurar de que se trata da instituição que procurava. (0 pontos)

   3) Não utiliza serviços bancários ou quaisquer outros serviços financeiros online. (0 pontos)

f. Lê acerca de um programa e decide experimentá-lo. Depois de pesquisar na Internet e encontrar uma versão experimental num site desconhecido:

   1) Transfere e instala imediatamente o programa. (3 pontos)

   2) Pesquisa mais informações acerca do criador do programa antes de transferi-lo. (1 pontos)

   3) Não transfere nem instala o programa. (0 pontos)

g. Encontra uma memória USB a caminho do trabalho:

   1) Guarda-a e liga-a ao seu computador para ver o conteúdo da mesma. (3 pontos)

   2) Guarda-a e liga-a ao seu computador para apagar todo o conteúdo da mesma antes de reutilizá-la. (3 pontos)

   3) Guarda-a e liga-a ao seu computador para executar uma análise antivírus antes de reutilizá-la para os seus próprios ficheiros (3 pontos)

   4) Não a guarda. (0 pontos)

h. Necessita de estabelecer ligação à Internet e encontra um hotspot de Wi-Fi aberto. Como procede:

   1) Estabelece ligação ao mesmo e utiliza a Internet. (3 pontos)

   2) Não estabelece ligação ao mesmo e aguarda até ter disponível uma ligação fidedigna. (0 pontos)

   3) Estabelece ligação ao mesmo e estabelece uma VPN num servidor fiável antes de enviar quaisquer informações. (0 pontos)

Parte 2: Analisar o seu comportamento online

Quanto mais alta for a sua pontuação, menos seguros são os seus comportamentos online. O objetivo consiste em ser 100 % seguro, prestando atenção a todas as suas interações online. Isto é muito importante, já que basta um erro para que o seu computador e os seus dados fiquem comprometidos.

Some os pontos obtidos na Parte 1. Registe a sua pontuação.

0: o seu comportamento online é muito seguro.

0 – 3: o seu comportamento online é relativamente seguro; contudo, para ser completamente seguro, deverá introduzir algumas alterações.

3 – 17: o seu comportamento online não é seguro e está em alto risco de comprometer a sua segurança.

18 ou mais: o seu comportamento online é muito inseguro e a sua segurança estará comprometida.

Seguem-se algumas sugestões de segurança online muito importantes.

a. Quanto mais informações partilhar nas redes sociais, mais estará a permitir que um atacante fique a conhecê-lo. Com mais conhecimento, um atacante pode criar um ataque muito mais orientado. Por exemplo, ao partilhar com o mundo que assistiu a uma corrida de automóveis, um atacante pode criar um e-mail malicioso proveniente da empresa de venda de bilhetes responsável pelo evento da corrida. Como acabou de assistir ao evento, o e-mail parece mais credível.

b. A reutilização de palavras-passe é uma prática incorreta. Se reutilizar uma palavra-passe num serviço sob controlo dos atacantes, estes poderão ser bem-sucedidos quando tentarem iniciar sessão em seu nome noutros serviços.

c. É possível forjar facilmente e-mails para que pareçam legítimos. Os e-mails forjados contêm frequentemente ligações para sites maliciosos ou software maligno. Regra geral, não clique em ligações incorporadas que tiver recebido por e-mail.

d. Não aceite software não solicitado, especialmente se for proveniente de uma página Web. É extremamente improvável que uma página Web tenha uma atualização de software legítima para si. Recomenda-se vivamente que feche o browser e utilize as ferramentas do sistema operativo para verificar a existência de tais atualizações.

e. É possível criar facilmente páginas Web maliciosas com aspeto semelhante ao do Web site de um banco ou de uma instituição financeira. Antes de clicar nas ligações ou fornecer quaisquer informações, verifique atentamente o URL para se assegurar de que se trata da página Web correta.

f. Quando permite que um programa seja executado no seu computador, está a conferir-lhe muito poder. Pense bem antes de permitir que um programa seja executado. Pesquise para se certificar de que a empresa ou o indivíduo por trás do programa é um autor sério e legítimo. Além disso, transfira o programa apenas do Web site oficial da empresa ou do indivíduo.

g. As memórias e unidades USB incluem um pequeno controlador que permite a comunicação com os computadores. É possível infetar esse controlador e dar-lhe instruções para instalar software malicioso no computador anfitrião. Uma vez que o software maligno está alojado no próprio controlador USB e não na área de dados, nenhuma eliminação ou análise antivírus irá detetar esse software maligno.

h. Muitas vezes, os atacantes irão implementar hotspots de Wi-Fi falsos para atrair os utilizadores. Uma vez que o atacante tem acesso a todas as informações trocadas através do hotspot comprometido, os utilizadores ligados a esse hotspot estão em risco. Nunca utilize hotspots de Wi-Fi desconhecidos sem encriptar o tráfego através de uma VPN. Nunca forneça dados sensíveis, tais como números de cartão de crédito, quando utilizar uma rede desconhecida (com ou sem fios).

Reflexão

Depois de analisar o seu comportamento online, que alterações faria para se proteger online?