A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

Fui Hackeado?

Visão Geral

Independente de quanto seguro você estiver, assim como ao dirigir um carro, mais cedo ou mais tarde você pode sofrer um acidente. Colocamos abaixo algumas pistas para ajudá-lo a identificar se você foi hackeado e, caso tenha acontecido, o que fazer. Quanto antes você identificar algo ruim acontecendo, mais provavelmente você poderá resolver o problema.

Pistas para identificar se você foi hackeado

- **Seu programa de antivírus gera um alerta informando que seu sistema está infectado. Certifique-se de que é o seu software antivírus que está gerando o alerta e não uma mensagem em uma janela vindo de um site de internet, tentando conduzi-lo a ligar para um telefone ou instalar alguma coisa. Não tem certeza? Abra seu software antivírus;**
- **Uma janela se abre dizendo que seu computador foi criptografado e você tem que pagar um resgate para recuperar seus arquivos;**
- **Seu navegador de Internet está abrindo páginas variadas de internet que você não pediu para visitar;**
- **Seu computador ou aplicações estão falhando constantemente, há ícones de aplicações desconhecidas ou janelas estranhas aparecem na tela;**
- **Sua senha não está mais funcionando mesmo que tenha certeza de que está correta;**
- **Amigos perguntam a você por que está enviando e-mails estranhos, que você sabe que nunca mandou;**
- **Aparecem contas no seu cartão de crédito ou saques da sua conta corrente que você nunca fez.**

Como responder

Se você desconfia que foi hackeado, quanto antes você agir, melhor. Se o incidente foi em ambiente de trabalho, não tente resolve-lo sozinho, ao invés disso, relate imediatamente. Se é relativo a um sistema ou conta pessoal, aqui vão alguns passos que você pode seguir:

Mude suas Senhas: Isso inclui não apenas as senhas no seu computador e dispositivos móveis mas também das suas contas online. Não utilize um computador hackeado para mudar suas senhas, use um sistema diferente que você saiba que é seguro. Se você tem muitas contas, comece pelas mais importantes. Se não consegue guardar todas as suas senhas, use um gerenciador de senhas;

Financeiro: Para problemas com seu cartão de crédito ou contas financeiras, ligue direto para seu banco ou administrador de cartão. Utilize um número de telefone confiável para ligar para eles, como o que consta no verso do seu cartão do banco, o que consta no seu extrato mensal ou visite seu website de um computador seguro. Adicionalmente, considere a possibilidade de congelar a disponibilidade das suas informações de crédito, temporariamente. Esse é um recurso chamado credit freeze, disponível nos Estados Unidos;

Antivirus. Se o seu software antivírus informa sobre um arquivo infectado, siga os passos recomendados. A maioria dos softwares antivírus terá links para sites onde você poderá aprender mais sobre a infecção específica;

Reinstalação. Se você não consegue corrigir um computador infectado ou quer ter certeza de que seu sistema está seguro, reinstale o sistema operacional. Não reinstale a partir de backups, pois eles devem ser utilizados apenas para recuperar seus arquivos pessoais. Se você não se sente confortável para reinstalar, considere a possibilidade de contratar um serviço profissional para lhe ajudar. Ou se o seu computador ou dispositivo for antigo, pode ser mais fácil adquirir um novo. Finalmente, uma vez reconstruído o sistema ou adquirido um novo, certifique-se de que ele está atualizado e habilite as atualizações automáticas sempre que possível;

Backups. Um passo chave para se proteger é manter antecipadamente backups (cópias de segurança) regulares. Muitas soluções vão fazer backup automaticamente dos seus arquivos, diariamente ou mesmo de hora em hora. Independente de qual solução você utilizar, verifique periodicamente que consegue restaurar esses arquivos. Muitas vezes, restaurar dados de um backup é a única forma de se recuperar de uma invasão;

Aplicação da Lei: Se você se sentir de qualquer forma ameaçado, relate o incidente para aplicação da lei. Se você for vítima de roubo de identidade e estiver baseado nos Estados Unidos, visite: https://www.identitytheft.gov.

Editor Convidado

Dr. Johannes Ullrich *(@johullrich) é o reitor de pesquisa do Instituto de Tecnologia SANS, diretor do SANS Internet Storm Center e um SANS "Fellow". Ele criou a rede de sensores colaborativos DShield e publica diariamente o podcast de notícias do Internet Storm Center.*

Recursos

Backups:	https://www.sans.org/u/JGP
Frases de Acesso:	https://www.sans.org/u/JGU
Gerenciadores de Senha:	https://www.sans.org/u/JGZ
O que é um Malware:	https://www.sans.org/u/JH4
Credit Freeze:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/