OUCH! | Junho de 2016

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Criptografia

O que é Criptografia?

Você pode ouvir pessoas mencionando “criptografia” e como você deve utilizá-la para proteger suas informações e você mesmo. Contudo criptografia pode ser confuso e você deve entender suas limitações. Nesta edição nós explicamos em termos simples o que é criptografia, como ela te protege e como implementá-la corretamente.

Editor Convidado

Francesca Bosco (**@francibosco**) é pesquisadora e responsável por projetos, especificamente os relacionados a crimes cibernéticos, segurança cibernética e mau uso de tecnologia. Trabalha no Instituto de Pesquisa de Crime e Justiça Inter-regional das Nações Unidas (United Nations Interregional Crime and Justice Research Institute) e foi cofundadora do Centro de Tecnologia e Lei.

Você tem uma quantidade tremenda de informações sensíveis nos seus dispositivos, como documentos, fotografias e e-mails pessoais. Se você tivesse um dos seus dispositivos roubado ou perdido, todas as suas informações sensíveis poderiam ser acessadas por quem tivesse posse do aparelho. Além disso, você pode utilizá-lo para fazer transações online como compras ou acesso a bancos. Se alguém estiver monitorando essas atividades ele pode roubar suas informações, como seus números de conta ou de cartão de crédito. A criptografia protege você nessas situações ao ajudá-lo a garantir que pessoas não autorizadas não consigam acessar ou modificar suas informações.

A criptografia existe há milhares de anos. Hoje em dia ela é bem mais sofisticada, mas serve ao mesmo propósito: passar uma mensagem secreta de um lugar para outro garantindo que somente a pessoa autorizada poderá acessá-la. Quando a informação não está encriptada, ela está em texto claro. Significa que qualquer um pode lê-la ou acessá-la facilmente. A criptografia converte essa informação para um formato não legível, chamado texto cifrado ou criptografado. A criptografia de hoje em dia funciona com operações matemáticas complexas e uma chave única para converter sua informação em texto cifrado. A chave é o que trava e destrava sua informação. Em muitos casos, sua chave é uma senha ou código de acesso.

O que você pode encriptar?

Geralmente há dois tipos de dado para encriptar: o dato parado (como aquele armazenado no seu dispositivo móvel, um celular ou tablet) e o dado em movimento (como o e-mail sendo acessado ou uma mensagem para um amigo).

Criptografar dados parados é vital para proteger a informação no caso de perda ou roubo do seu computador ou dispositivo móvel. Os equipamentos de hoje em dia são extremamente poderosos e armazenam uma quantidade tremenda de informações, mas também são muito fáceis de perder. Adicionalmente outros tipos de meio de armazenamento (mídias)

Criptografia

podem guardar informações sensíveis, como discos USB (pendrives) ou discos externos. A criptografia de disco inteiro (FDE – Full Disk Encryption) é uma técnica de criptografia amplamente utilizada que criptografa o disco inteiro do seu sistema. Significa que tudo que estiver no seu dispositivo é automaticamente encriptado para você, ou seja, você não tem que decidir sobre o que encriptar e o que não encriptar. Hoje em dia muitos computadores já vem com FDE mas você tem que habilitar o recurso manualmente. Nos Macs ele é chamado FileVault e nos computadores com Windows, dependendo da versão, pode ser chamado Bitlocker ou Criptografia de Dispositivo (Device Encryption, na versão em Inglês). Muitos dispositivos móveis também suportam FDE. O sistema operacional iOS dos iPhones e iPads habilitam automaticamente o FDE uma vez que um código de acesso (passcode) seja definido. E nas versões acima da 6.0 (Marshmallow) do Android, o Google sugere a habilitação do FDE por padrão, desde que o dispositivo atenda certos requerimentos mínimos de recursos.

Criptografia é uma forma poderosa de proteger sua informação, mas ela só é tão forte quanto for sua chave.

A informação também está vulnerável quando está em trânsito. Se o dado não estiver encriptado, ele pode ser monitorado, modificado e capturado online. Por isso é importante garantir que qualquer transação ou comunicação sensível online esteja encriptada. Uma forma comum de criptografia online é o HTTPS. Significa que todo o tráfego entre seu navegador de Internet e o site de Internet está encriptado. Procure por https:// no endereço URL, ou um ícone de cadeado no navegador, ou a barra de endereços URL do navegador se mostrando em verde, ao acessar o site. Um outro exemplo é quando você envia ou recebe um e-mail. Muitos clientes de e-mail têm capacidade de criptografia que você pode ter que habilitar. E um terceiro exemplo de criptografia de dados em trânsito é quando dois usuários conversam entre si com aplicativos como Whatsapp, Telegram, iMessage, Wicker ou Signal. Aplicativos como esses utilizam criptografia fim a fim, que previne terceiros de acessar os dados enquanto estiverem sendo transferidos de um dispositivo para outro. Significa que somente você e a pessoa com quem está se comunicando podem ler o que foi enviado.

Fazendo da forma certa

Para certificar-se de que você está protegido ao utilizar criptografia, é fundamental que você a utilize da forma correta.

- Sua criptografia é tão forte quanto sua chave. Se alguém puder adivinhar ou ter acesso à sua chave, ele terá acesso aos seus dados. Proteja sua chave. Se você está usando um código de acesso ou uma senha, certifique-se de que ela é forte e única. Quanto maior sua senha, mais difícil de um atacante adivinhá-la ou descobri-la. Não esqueça a sua

Criptografia

senha, pois sem ela você não poderá mais decriptar suas informações. Se não puder lembrar de todas as suas senhas, recomendamos utilizar um gerenciador de senhas;

- Sua criptografia é tão segura quanto a segurança dos seus dispositivos. Se o seu dispositivo foi comprometido ou infectado por um malware, atacantes cibernéticos poderão evitar sua criptografia. É por isso que é tão importante tomar outras medidas para proteger seu dispositivo como utilizar antivírus, senhas fortes e mantê-lo atualizado;
- Muitos aplicativos para dispositivos móveis, bem como programas de computador, agora oferecem criptografia forte para proteger seus dados e comunicações. Se o app ou aplicação que estiver pensando em utilizar não suportar criptografia, considere utilizar outro como alternativa.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em securingthehuman.sans.org/ouch/archives.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

Criptografia Explicada (em Inglês):	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Cartilha do Cert.br – Criptografia:	https://securingthehuman.sans.org/ouch/2015#october2015
Frases Secretas:	https://securingthehuman.sans.org/ouch/2015#october2015
Gerenciadores de Senhas:	https://securingthehuman.sans.org/ouch/2015#october2015
O que é um Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Tornando Seguro Seu Novo Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser

