

OUCH!

NESTA EDIÇÃO...

- Visão Geral
- Cinco Passos Simples
- Protegendo as Crianças em Visitas

Ajudando Outros a se Proteger

Visão Geral

Muitos de nós ficam à vontade com a tecnologia, inclusive em como utilizá-la de forma segura. Contudo outros membros da família ou amigos podem não se sentir tão confortáveis. De fato, eles podem estar confusos, intimidados ou até assustados com ela. Isso os torna muito vulneráveis aos ataques cibernéticos de hoje. Segurança cibernética não tem que ser assustadora. Na verdade, ela é bem simples, uma vez que entenda o básico. E eles provavelmente precisam de um guia como você para entender o básico.

Editor Convidado

Randy Marchany (Twitter: [@randymarchany](https://twitter.com/randymarchany)) é o CISO na empresa Virginia Tech e é instrutor SANS certificado.

Cinco Passos Simples

Aqui vão cinco passos simples que você pode seguir para ajudar outras pessoas a superarem seus medos e aproveitar o máximo da tecnologia atual. Para mais informações sobre cada um desses pontos veja a seção de Referências no final desta edição.

1. **Engenharia Social:** É uma técnica usada por atacantes cibernéticos para enganar pessoas e conduzi-las a fazer algo que não deveriam, como compartilhar sua senha, infectar seu computador ou compartilhar informação sensível. Não é nenhuma novidade pois golpes e trapaceiros existem há milhares de anos. A única diferença agora é que os vigaristas estão usando os mesmos conceitos na Internet. Você pode ajudar outras pessoas explicando as pistas mais comuns de um ataque de engenharia social, como quando alguém cria um tremendo senso de urgência, quando algo é muito bom para ser verdade ou quando o atacante finge ser alguém que você conhece, mas suas mensagens não parecem ser do seu amigo. Compartilhe exemplos de ataques comuns de engenharia social, como e-mails de phishing ou as ligações de suporte técnico da Microsoft. Ao final, certifique-se de que os membros da família entendam que nunca devem dar suas senhas para ninguém, nem permitir acesso remoto ao seu computador;
2. **Senhas:** Senhas fortes são chave para proteger tanto equipamentos quanto contas online. Demonstre aos membros da sua família como criar senhas fortes. Nós recomendamos frases de acesso por serem fáceis de digitar e lembrar. Frases de acesso são nada mais que senhas compostas de várias palavras. Adicionalmente, ajude-os a instalar e usar gerenciadores de senha. É importante ter uma senha única para cada dispositivo e conta de acesso. Se um gerenciador de senha for estressante, ajude-os talvez a anotar suas senhas e armazená-las em um local seguro. Finalmente, para

Ajudando Outros a se Proteger

contas importantes ajude-os a habilitar a verificação em duas etapas (também chamada autenticação de dois fatores). Verificação de duas etapas é um dos passos mais efetivos que você pode seguir para proteger qualquer conta;

3. **Atualizações de Segurança:** Manter sistemas atualizados é um passo chave que qualquer um pode seguir para proteger seus dispositivos. Isso vale não somente para seus computadores e dispositivos móveis, mas para qualquer coisa conectada na Internet, como consoles de jogos, termômetros ou até luzes ou alto falantes. A forma mais simples de garantir que todos os dispositivos estejam atualizados é habilitar a atualização automática sempre que possível;
4. **Antivírus:** As pessoas cometem erros. Às vezes nós clicamos em algo ou instalamos coisas que provavelmente não devêssemos e que infectam nossos sistemas. Os antivírus foram feitos para nos proteger desses erros. Mesmo não sendo capazes de parar todos os malwares, eles ajudam a detectar e parar os ataques mais comuns. Por isso, certifique-se de que qualquer computador de sua casa tenha um antivírus instalado, que esteja atualizado e ativo. Adicionalmente, muitas das soluções de antivírus de hoje em dia incluem outras tecnologias de segurança como firewall e proteção de navegadores de Internet;
5. **Backups:** Quando tudo falhar, os backups são frequentemente a única forma de se recuperar de erros como apagar arquivos errados ou ataques como Ransomware. Certifique-se de que sua família e amigos tenham implementado um backup automático de arquivos. Frequentemente as soluções mais simples são aquelas baseadas em Nuvem, que copiam os arquivos dos seus dispositivos de hora em hora, ou quando você alterar um arquivo. Essas soluções tornam simples não somente o processo de backup, mas também de restauração.



Protegendo as Crianças em Visitas

Se você se sente confortável com a tecnologia, provavelmente você não só se protegeu, mas também os seus filhos. Contudo, quando as crianças visitam um parente que não está confortável com a tecnologia, como os avós, esses parentes ou amigos podem não estar cientes sobre como melhor proteger as crianças ou sobre as suas expectativas. Aqui vão alguns passos que você pode seguir para ajudar a proteger seus filhos enquanto eles estiverem em visita, especialmente em família:

- **Regras:** Certifique-se de que, se houver regras ou expectativas definidas para a segurança dos seus filhos, as pessoas visitadas as conheçam. Por exemplo, há alguma regra sobre quanto tempo seus filhos podem permanecer online, com quem podem falar ou quais jogos podem ou não jogar? Confie em nós, não conte com a explicação

Ajudando Outros a se Proteger

dos seus filhos aos outros membros da família. Outra ideia é criar uma “folha de regras” e compartilhá-la com os parentes visitados frequentemente pelos seus filhos;

- **Controle:** Se uma criança entende de tecnologia melhor que seus guardiões, ela pode tirar vantagem disso. Por exemplo, uma criança pode pedir ou obter acesso administrativo ao computador dos seus avós e então fazer o que quiser, como instalar um jogo que você não queira que ela jogue. Certifique-se de que os parentes entendam que não devem dar acessos adicionais às crianças além do que estiver estabelecido.

Finalmente, sugira às pessoas que assinem publicações periódicas como o OUCH!, para que continuem aprendendo por conta própria. Este boletim de notícias é publicado mensalmente e gratuitamente em mais de 20 línguas. Assine em <https://securingthehuman.sans.org/ouch>.

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

Marta Visser – Tradutora autônoma

Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigogularte

Recursos

Engenharia Social:	https://securingthehuman.sans.org/ouch/2017#january2017
Frases de Acesso:	https://securingthehuman.sans.org/ouch/2017#april2017
Gerenciamento de Senha:	https://securingthehuman.sans.org/ouch/2017#september2017
Verificação em Duas Etapas:	https://securingthehuman.sans.org/ouch/2015#september2015
Backup e Restauração:	https://securingthehuman.sans.org/ouch/2017#august2017
Tornando seguras as Crianças Online de hoje:	https://securingthehuman.sans.org/ouch/2017#may2017

OUCH! é publicado pelo “SANS Securing the Human” e distribuído sob o licenciamento [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). A distribuição ou utilização desta publicação em programas de treinamento é permitida desde que seu conteúdo não seja modificado. Para traduções ou mais informações entre em contato pelo ouch@securingthehuman.org

Board Editorial: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley

Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus