Guia de Segurança em Redes Sociais

INTRODUÇÃO

As redes sociais são parte do cotidiano de navegação dos usuários. A maioria dos internautas utiliza ao menos uma rede social e muitos deles participam ativamente de várias delas. Para muitos usuários (especialmente os mais jovens), **as redes sociais são o principal motivo para se conectar à Internet.**

Contudo, o uso dessas redes deixa os usuários expostos a um conjunto de ameaças informáticas, que podem atentar contra sua informação, a própria integridade do usuário, ou até mesmo seu dinheiro.

Com a crescente tendência dos ataques virtuais utilizarem as redes sociais como meio de propagação, é de vital importância para o usuário estar protegido e contar com um ambiente seguro no momento de utilizá-las.

Quais são os principais ataques? Quais as principais medidas de segurança a serem adotadas? Para responder a essas duas perguntas, este documento serve como um guia para o usuário ter maior segurança no uso das redes sociais

REDES SOCIAIS

Facebook

- É a rede social mais popular do mundo.
- Em 2011 superou os 600 milhões de usuários em todo o mundo.
- É a rede favorita dos jovens, utilizada para formar redes de contatos entre amigos, dentre outras finalidades.
- Também utilizada por empresas e organizações para se comunicarem com o público.

MySpace

- Permite compartilhar perfis de usuários, amigos, fotos, música, etc.
- Foi ultrapassado pelo Facebook em número de usuários, mas mantém sua importância, por exemplo, para a difusão de grupos musicais.
- Até março de 2011, possuía mais de 34 milhões de usuários.

Twitter

- Rede social de microblogging.
- Os usuários compartilham mensagens de até 140 caracteres.
- Foi uma das redes de maior crescimento em 2010.
- Possui mais de 200 milhões de usuários.

Linkedin

- Rede social para profissionais. É a mais utilizada no meio corporativo.
- Permite às pessoas tecerem redes de contatos de trabalho e publicarem seus currículos na web.
- Até março de 2011, conta com 100 milhões de usuários registrados.

Quais são os riscos nas redes sociais?

A informação e o dinheiro dos usuários são o alvo dos criminosos, pois quanto maior a quantidade de usuários, mais atraente se torna um site para um golpista. Por isso, além de todas suas vantagens, a navegação pelos sites de redes sociais implica na exposição a uma série de ameaças virtuais.

Malware

Imagem 1 - Site de propagação do Boonana

- Acrônimo em inglês das palavras ***malicious*** e ***software***, ou seja, significando "software malicioso".
- São arquivos com fins nocivos que, ao infectar um computador, executam diversas ações, como o roubo de informação, o controle do sistema ou o roubo de senhas.
- Vírus, worms e cavalos de troia são as variantes mais conhecidas neste meio.

A partir de estratégias de Engenharia Social, os desenvolvedores de malware costumam utilizar as redes sociais para propagar os códigos maliciosos.

O cavalo de troia Koobface é o mais conhecido deste tipo. Com nome acrônimo da rede social mais popular do mundo (Facebook), o cavalo de troia se caracterizou, em suas primeiras campanhas de propagação, por utilizar mensagens atrativas em redes sociais. A ameaça, cria uma botnet, uma rede de computadores zumbi que podem ser controlados remotamente pelo criminoso.

Em outubro de 2010 (a cerca de 2 anos de sua aparição), uma nova variante do Koobface (identificada como Boonana.A ou Win32/Boonana.A) tinha a particularidade de se propagar através do Java, uma tecnologia multiplataforma, que permitia infectar tanto sistemas Windows quanto Linux e Mac OS. Ao momento em que a vítima visita a página maliciosa, a ameaça identifica o sistema operacional instalado no computador do usuário e faz download do arquivo correspondente à sua plataforma.

Phishing

• Consiste no roubo de informação pessoal e financeira do usuário, através da falsificação de identidade de alguma pessoa ou empresa de confiança.

• É frequentemente realizado através de correio eletrônico e de sites duplicados, ainda que possa ser feita por outros meios.

Como identificar um site de phishing?

Nem sempre é simples identificar um site duplicado, até mesmo porque, geralmente, para chegar ali, o usuário já deva ter sido vítima de alguma técnica de Engenharia Social, ou de infecção de malware que o levou ao site malicioso.

Para o primeiro caso, é recomendável evitar clicar em links suspeitos e, no caso de alguma solicitação de informação sigilosa, acessar o site manualmente, sem utilizar nenhum tipo de link, e verificar se a informação procede.

Além disso, é recomendável verificar tanto o domínio do site, como também a encriptação para transmissão de dados (protocolo HTTPS). Esse protocolo, ainda que não garanta a legitimidade do site, é requisito indispensável e, em geral, os sites de phishing não o possuem.

Phishing

Exemplo II: phishing a través de e-mail

Asunto: Facebook Password Reset Confirmation. Customer Support.
Fecha: Tue, 8 Dec 2009 10:13:58 +0800
De: Facebook Service <customer@facebook.com>
A: [redacted]com

Hey [redacted] ,

Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.

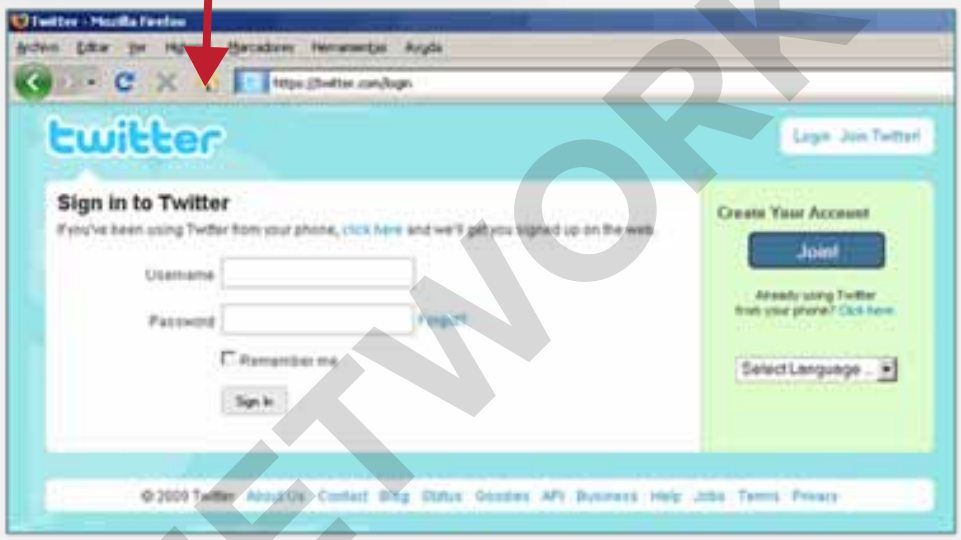
Thanks,
Your Facebook.

- - - -

Facebook_Password_833fd.zip
22 K Descargar

Exemplo I: phishing no Twitter

O site original utiliza protocolo seguro HTTPS:



O site original tem o domínio correto:

Roubo de informação

• No uso diário das redes sociais, os usuários publicam na web diversos dados pessoais, que podem ser úteis aos criminosos.

• O roubo de informação em redes sociais está relacionado diretamente ao roubo de identidade, um dos delitos virtuais que mais cresce nos últimos anos.

• Os dois fatores de ataque mais importantes no roubo de informação são:

✓ **Engenharia Social:** o contato direto com a vítima, extraindo informações através da comunicação, a "amizade" ou qualquer comunicação possível na rede social.

✓ **Informacão pública:** a má configuração das redes sociais pode permitir que informações fiquem acessíveis além do que o usuário gostaria ou lhe seria conveniente para sua segurança. Pessoas mal intencionadas poderiam acessar essas informações.

A Assédio a menores de idade

• As crianças utilizam as redes sociais desde muito cedo, ao contrário do que as próprias redes sociais recomendam como adequado (o Facebook, por exemplo, foi criado para maiors de 18 anos).

• Existe uma série de ameaças focadas especialmente nos jovens que utilizam esses serviços: abuso (cyberbullying), grooming, sexting: Estes são alguns dos riscos aos quais estão expostos ao acessar redes sociais.

• O papel dos adultos é fundamental para a proteção dos filhos: Estes não deveriam utilizar as redes sociais sem contar com o apoio, o diálogo e a educação de seus pais ou de qualquer outro adulto de referência, inclusive os próprios professores.

Formas de proteção

Diante desse cenário de ameaças, o uso de redes sociais pode parecer perigoso. Contudo, seguindo os conselhos fornecidos a seguir, é possível utilizá-las e contar com níveis de proteção adequados para um uso correto e seguro das redes sociais. Destacam-se como principais medidas: utilizar tecnologias de segurança, configurar corretamente os perfis em redes sociais e utilizar o protocolo HTTPS para a navegação. Entretanto, a educação constante do usuário e o uso cuidadoso no momento da navegação sempre permitirão minimizar de forma significativa os riscos a que se encontram expostos.

UTILIZAR TECNOLOGIAS DE SEGURANÇA

Sendo os códigos maliciosos a ameaça massiva mais importante, a utilização de um software de antivírus com capacidades proativas de detecção, e o banco de dados atualizado é um componente fundamental para prevenir o malware de se propagar pelas redes sociais.

As ferramentas antispam e firewall também otimizam a segurança do sistema perante esses riscos.

Também é fundamental não utilizar um usuário administrador no momento de navegar por essas redes, e contar com perfis de acesso para cada usuário do computador, de forma a minimizar o impacto em caso de qualquer incidente.

Finalmente, para os menores de idade, ferramentas de controle dos pais permitem bloquear sites indesejados, assim como restringir o horário ou quantidade de horas em que a criança utiliza as redes sociais.

a

CONFIGURAÇÕES DE PRIVACIDADE NAS REDES SOCIAIS

Nem sempre as configurações-padrão nas redes sociais são as melhores para a segurança do usuário. Portanto, é recomendável dedicar um tempo para criar o usuário (e periodicamente), para revisar quais são as possíveis fugas de informação devido à má configuração do sistema.

Configurações de privacidade no Facebook

• Evitar que nenhuma configuração de perfil esteja disponível de forma pública, sem limitações. De preferência, mostrar a informação somente a amigos e, sendo possível, somente a um grupo específico, caso tenha um grande número de contatos.

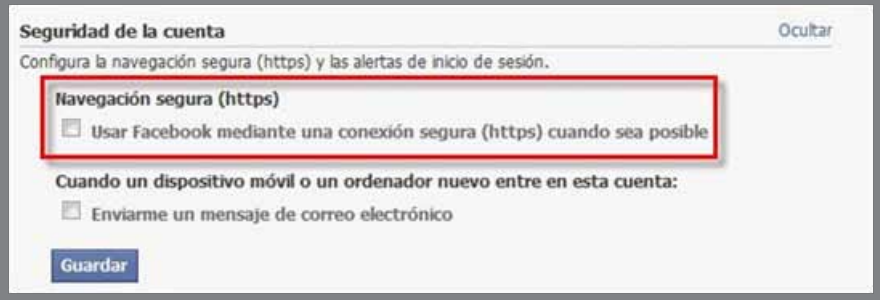
• Limitar o público que observa as fotos em que o usuário foi marcado, especialmente se for uma criança.

• Evitar que os aplicativos possam acessar informações pessoais, ou publicar no seu mural.

Mais informações: http://blog.eset.com/2011/05/25/facebook-privacy

No Facebook

Selecionar a opção "Configuração de conta" no menu "Conta" do canto superior direito. Em seguida, dirija-se à aba "Segurança da conta" e irá encontrar a possibilidade de optar pela navegação segura:



No Twitter

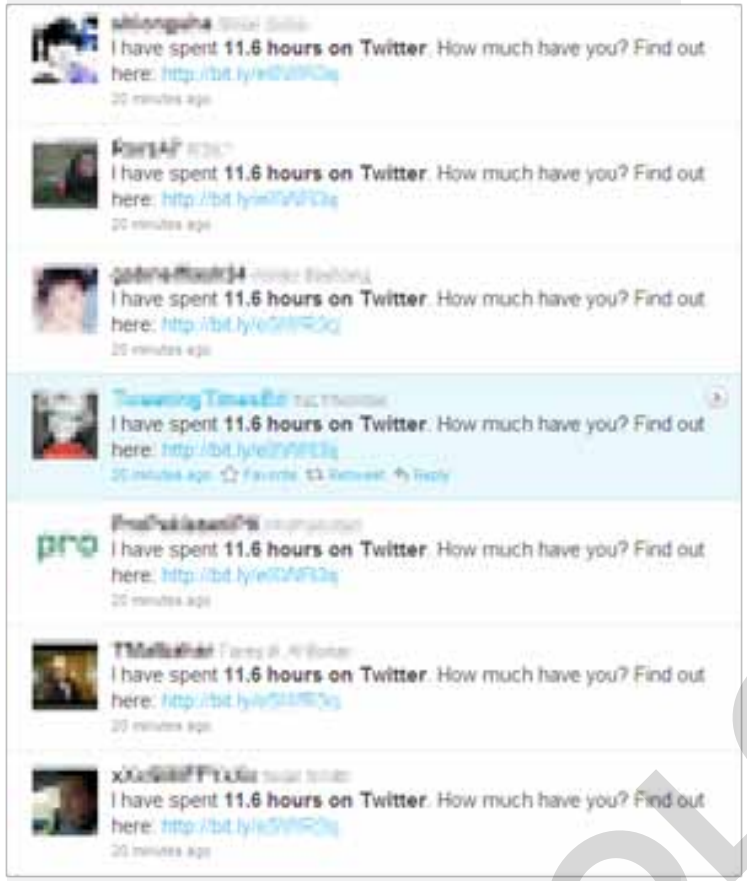
Ir à configuração de conta e marcar o campo "Usar sempre HTTPS", conforme indicado na imagem a seguir:

COMO CONFIGURAR HTTPS NO FACEBOOK E NO TWITTER

Configurar a navegação pelo protocolo HTTPS permite que todos os ataques relacionados à interceptação de informação que viaja em texto legível através das redes de computadores sejam evitados. Com o protocolo HTTPS, todos os dados – não somente usuário e senha – irão viajar codificados e serão ilegíveis para qualquer criminoso na rede.

É recomendável aplicar essas configurações, especialmente úteis ao se conectar a essas redes sociais através de redes wireless públicas.

GUIA PARA EVITAR LINKS MALICIOSOS NO TWITTER



- Somente clicar em links publicados por contatos conhecidos. Ainda assim, isso não é garantia de segurança, é uma recomendação que adquire força considerável quando somada às outras dicas a seguir.
- Evitar seguir contatos desconhecidos para diminuir a possibilidade de recepção de mensagens maliciosas.
- Caso suspeite da legitimidade de uma mensagem, é recomendável buscar partes dela ou de seu link no buscador do Twitter, e observar tanto sua repetição como as opiniões da comunidade, que, ao descobrir um golpe em redes sociais, o expõe imediatamente.
- Instalar um plugin para o navegador que revele os destinos de URLs curtas e permita ver o endereço original sem a necessidade de clicar para abri-las, como o LongURL Mobile Expander.

DEZ MANDAMENTOS DE SEGURANÇA NO CIBERESPAÇO

1. Evitar clicar em links suspeitos
2. Não acessar sites de reputação duvidosa
3. Atualizar o sistema operacional e seus aplicativos
4. Baixar aplicativos de sites oficiais
5. Utilizar tecnologias de segurança
6. Evitar inserir informações pessoais em formulários duvidosos
7. Ter precaução com os resultados conseguidos por sites de busca
8. Aceitar somente contatos conhecidos
9. Evitar abrir arquivos suspeitos
10. Utilizar senhas fortes

CONCLUSÃO

Sem dúvida, as redes sociais são um valioso recurso para os internautas. Contudo, como informado neste guia, existe uma série de ameaças que podem expor o usuário durante seu uso. É por isso que é recomendável não subestimar os criminosos virtuais. Fazendo uso correto de ferramentas de informática, configurações corretas e uma conduta adequada durante a navegação, **é possível utilizar as redes sociais de forma segura.**