Comitê Gestor da Internet no Brasil

Cartilha de Segurança para Internet

Parte III: Privacidade

Versão 3.1
2006

CERT.br – Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Parte III: Privacidade

Esta parte da Cartilha discute questões relacionadas à privacidade do usuário ao utilizar a Internet. São abordados temas relacionados à privacidade dos *e-mails*, à privacidade no acesso e disponibilização de páginas *Web*, bem como alguns cuidados que o usuário deve ter com seus dados pessoais e ao armazenar dados em um disco rígido.

Versão 3.1 – Outubro de 2006
http://cartilha.cert.br/

Sumário

1 Privacidade dos *E-mails*

O serviço de *e-mails* foi projetado para ter como uma de suas principais características a simplicidade. O problema deste serviço é que foi comparado com o correio convencional, dando a falsa idéia de que os *e-mails* são cartas fechadas. Mas eles são, na verdade, como cartões postais, cujo conteúdo pode ser lido por quem tiver acesso a eles.

1.1 É possível alguém ler *e-mails* de outro usuário?

As mensagens que chegam à caixa postal do usuário ficam normalmente armazenadas em um arquivo no servidor de *e-mails* do provedor, até o usuário se conectar na Internet e obter os *e-mails* através do seu programa leitor de *e-mails*.

Portanto, enquanto os *e-mails* estiverem no servidor, poderão ser lidos por pessoas que tenham acesso a este servidor[1]. E enquanto estiverem em trânsito, existe a possibilidade de serem lidos por alguma pessoa conectada à Internet.

1.2 Como é possível assegurar a privacidade dos *e-mails*?

Se a informação que se deseja enviar por *e-mail* for confidencial, a solução é utilizar programas que permitam criptografar o *e-mail* através de chaves (senhas ou frases), de modo que ele possa ser lido apenas por quem possuir a chave certa para decodificar a mensagem. Maiores informações sobre criptografia podem ser encontradas na Parte I: Conceitos de Segurança.

Alguns *softwares* de criptografia podem estar embutidos nos programas leitores de *e-mails*, outros podem ser adquiridos separadamente e integrados aos programas leitores de *e-mails*.

Devem ser usados, preferencialmente, programas de criptografia que trabalhem com pares de chaves, como o GnuPG, que pode ser obtido no site `http://www.gnupg.org/`.

Estes programas, apesar de serem muito utilizados na criptografia de mensagens de *e-mail*, também podem ser utilizados na criptografia de qualquer tipo de informação, como por exemplo, um arquivo sigiloso a ser armazenado em uma cópia de segurança (vide Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção).

1.3 A utilização de programas de criptografia é suficiente para assegurar a privacidade dos *e-mails*?

Os programas de criptografia são utilizados, dentre outras finalidades, para decodificar mensagens criptografadas, recebidas por um usuário, no momento em que este desejar lê-las.

Ao utilizar um programa de criptografia para decodificar uma mensagem, é possível que o programa leitor de *e-mails* permita salvar a mensagem no formato decodificado, ou seja, em texto claro. No caso da utilização de programas leitores de *e-mails* com esta característica, a privacidade do

[1] Normalmente existe um consenso ético entre administradores de redes e provedores de nunca lerem a caixa postal de um usuário sem o seu consentimento.

conteúdo da mensagem é garantida durante a transmissão da mensagem, mas não necessariamente no seu armazenamento.

Portanto, é extremamente importante o usuário estar atento para este fato, e também certificar-se sobre o modo como suas mensagens estão sendo armazenadas. Como uma mensagem pode ser decodificada sempre que o usuário desejar lê-la, é aconselhável que ela seja armazenada de forma criptografada e não em texto claro.

2 Privacidade no Acesso e Disponibilização de Páginas *Web*

Existem cuidados que devem ser tomados por um usuário ao acessar ou disponibilizar páginas na Internet. Muitas vezes o usuário pode expor informações pessoais e permitir que seu *browser* receba ou envie dados sobre suas preferências e sobre o seu computador. Isto pode afetar a privacidade de um usuário, a segurança de seu computador e até mesmo sua própria segurança.

2.1 Que cuidados devo ter ao acessar páginas *Web* e ao receber *cookies*?

Cookies são muito utilizados para rastrear e manter as preferências de um usuário ao navegar pela Internet. Estas preferências podem ser compartilhadas entre diversos *sites* na Internet, afetando assim a privacidade de um usuário. Não é incomum acessar pela primeira vez um *site* de música, por exemplo, e observar que todas as ofertas de CDs para o seu gênero musical preferido já estão disponíveis, sem que você tenha feito qualquer tipo de escolha.

Além disso, ao acessar uma página na Internet, o seu *browser* disponibiliza uma série de informações, de modo que os *cookies* podem ser utilizados para manter referências contendo informações de seu computador, como o *hardware*, o sistema operacional, *softwares* instalados e, em alguns casos, até o seu endereço de *e-mail*.

Estas informações podem ser utilizadas por alguém mal intencionado, por exemplo, para tentar explorar uma possível vulnerabilidade em seu computador, como visto na Parte I: Conceitos de Segurança e Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

Portanto, é aconselhável que você desabilite o recebimento de *cookies*, exceto para *sites* confiáveis, onde sejam realmente necessários.

As versões recentes dos *browsers* normalmente permitem que o usuário desabilite o recebimento, confirme se quer ou não receber e até mesmo visualize o conteúdo dos *cookies*.

Também existem *softwares* que permitem controlar o recebimento e envio de informações entre um *browser* e os *sites* visitados. Dentre outras funções, estes podem permitir que *cookies* sejam recebidos apenas de *sites* específicos[2].

Uma outra forma de manter sua privacidade ao acessar páginas na Internet é utilizar *sites* que permitem que você fique anônimo. Estes são conhecidos como *anonymizers*[3] e intermediam o envio e recebimento de informações entre o seu *browser* e o *site* que se deseja visitar. Desta forma, o seu

[2] Um exemplo deste tipo de *software* pode ser encontrado em http://internet.junkbuster.com/.

[3] Exemplos desse tipo de *site* podem ser encontrados em http://anonymouse.org/ (serviço gratuito) e http://www.anonymizer.com/ (serviço pago).

browser não receberá *cookies* e as informações por ele fornecidas não serão repassadas para o *site* visitado.

Neste caso, é importante ressaltar que você deve certificar-se que o *anonymizer* é confiável. Além disso, você não deve utilizar este serviço para realizar transações via *Web*.

2.2 Que cuidados devo ter ao disponibilizar uma página na Internet, como por exemplo um *blog*?

Um usuário, ao disponibilizar uma página na Internet, precisa ter alguns cuidados, visando proteger os dados contidos em sua página.

Um tipo específico de página *Web* que vem sendo muito utilizado por usuários de Internet é o *blog*. Este serviço é usado para manter um registro freqüente de informações, e tem como principal vantagem permitir que o usuário publique seu conteúdo sem necessitar de conhecimento técnico sobre a construção de páginas na Internet.

Apesar de terem diversas finalidades, os *blogs* têm sido muito utilizados como diários pessoais. Em seu *blog*, um usuário poderia disponibilizar informações, tais como:

- seus dados pessoais (*e-mail*, telefone, endereço, etc);
- informações sobre seus familiares e amigos (como árvores genealógicas, datas de aniversário, telefones, etc);
- dados sobre o seu computador (dizendo, por exemplo, "...comprei um computador da marca X e instalei o sistema operacional Y...");
- dados sobre os *softwares* que utiliza (dizendo, por exemplo, "...instalei o programa Z, que acabei de obter do *site* W...");
- informações sobre o seu cotidiano (como, por exemplo, hora que saiu e voltou para casa, data de uma viagem programada, horário que foi ao caixa eletrônico, etc);

É extremamente importante estar atento e avaliar com cuidado que informações serão disponibilizadas em uma página *Web*. Estas informações podem não só ser utilizadas por alguém mal-intencionado, por exemplo, em um ataque de engenharia social (vide Parte I: Conceitos de Segurança), mas também para atentar contra a segurança de um computador, ou até mesmo contra a segurança física do próprio usuário.

3 Cuidados com seus Dados Pessoais

Procure não fornecer seus dados pessoais (como nome, *e-mail*, endereço e números de documentos) para terceiros. Também **nunca** forneça informações sensíveis (como senhas e números de cartão de crédito), a menos que esteja sendo realizada uma transação (comercial ou financeira) e se tenha certeza da idoneidade da instituição que mantém o *site*.

Estas informações geralmente são armazenadas em servidores das instituições que mantêm os *sites*. Com isso, corre-se o risco destas informações serem repassadas sem sua autorização para outras instituições ou de um atacante comprometer este servidor e obter acesso a todas as informações.

Fique atento aos ataques de engenharia social, vistos na Parte I: Conceitos de Segurança. Ao ter acesso a seus dados pessoais, um atacante poderia, por exemplo, utilizar seu *e-mail* em alguma lista de distribuição de *spams* (vide Parte VI: *Spam*) ou se fazer passar por você na Internet (através do uso de uma de suas senhas).

3.1 Que cuidados devo ter em *sites* de redes de relacionamentos, como por exemplo o orkut?

Os *sites* de redes de relacionamentos, como o orkut, tiveram uma ampla aceitação e inserção de usuários da Internet, por proporcionarem o encontro de pessoas (amigos) e permitirem a criação e participação em comunidades com interesses em comum.

Um *site* de redes de relacionamento normalmente permite que o usuário cadastre informações pessoais (como nome, endereços residencial e comercial, telefones, endereços de *e-mail*, data de nascimento, etc), além de outros dados que irão compor o seu perfil. Se o usuário não limitar o acesso aos seus dados para apenas aqueles de interesse, todas as suas informações poderão ser visualizadas por qualquer um que utilize este *site*. Além disso, é recomendável que o usuário evite fornecer muita informação a seu respeito, pois nenhum *site* está isento do risco de ser invadido e de ter suas informações furtadas por um invasor.

A participação de um usuário em determinados tipos de comunidades também pode fornecer muita informação para terceiros. Por exemplo, a comunidade de donos de um determinado veículo, ou dos freqüentadores do estabelecimento X, pode dizer qual é a classe social de um usuário, que locais ele gosta de freqüentar, etc.

Desta forma, é extremamente importante estar atento e avaliar com cuidado que informações você disponibilizará nos *sites* de redes de relacionamentos, principalmente aquelas que poderão ser vistas por todos, e em que comunidades você participará. Estas informações podem não só ser utilizadas por alguém mal-intencionado, por exemplo, em um ataque de engenharia social (vide Parte I: Conceitos de Segurança), mas também para atentar contra a segurança física do próprio usuário.

4 Cuidados com os Dados Armazenados em um Disco Rígido

É importante ter certos cuidados no armazenamento de dados em um computador. Caso você mantenha informações sensíveis ou pessoais que você não deseja que sejam vistas por terceiros (como números de cartões de crédito, declaração de Imposto de Renda, senhas, etc), estas devem ser armazenadas em algum formato criptografado.

Estes cuidados são extremamente importantes no caso de *notebooks*, pois são mais visados e, portanto, mais suscetíveis a roubos, furtos, etc.

Caso as informações não estejam criptografadas, se você necessitar levar o computador a alguma assistência técnica, por exemplo, seus dados poderão ser lidos ou copiados por uma pessoa não autorizada.

Para criptografar estes dados, como visto na seção 1.2, existem programas que, além de serem utilizados para a criptografia de *e-mails*, também podem ser utilizados para criptografar arquivos.

Um exemplo seria utilizar um programa que implemente criptografia de chaves pública e privada[4], como o GnuPG. O arquivo sensível seria criptografado com a sua chave pública e, então, decodificado com a sua chave privada, sempre que fosse necessário.

É importante ressaltar que a segurança deste método de criptografia depende do sigilo da chave privada. A idéia, então, é manter a chave privada em um CD ou outra mídia (como *pen drive*, disco rígido removível ou externo) e que este não acompanhe o computador, caso seja necessário enviá-lo, por exemplo, para a assistência técnica.

Também deve-se ter um cuidado especial ao trocar ou vender um computador. Apenas apagar ou formatar um disco rígido não é suficiente para evitar que informações antes armazenadas possam ser recuperadas. Portanto, é importante **sobrescrever** todos os dados do disco rígido (vide seção 4.1).

4.1 Como posso sobrescrever todos os dados de um disco rígido?

Para assegurar que informações não possam ser recuperadas de um disco rígido é preciso sobrescrevê-las com outras informações. Um exemplo seria gravar o caracter 0 (zero), ou algum caracter escolhido aleatoriamente, em todos os espaços de armazenamento do disco.

É importante ressaltar que é preciso repetir algumas vezes a operação de sobrescrever os dados de um disco rígido, para minimizar a chance de recuperação de informações anteriormente armazenadas.

Existem *softwares* gratuitos e comerciais que permitem sobrescrever dados de um disco rígido e que podem ser executados em diversos sistemas operacionais, como o Windows (95/98, 2000, XP, etc), Unix (Linux, FreeBSD, etc), Mac OS, entre outros.

5 Cuidados com Telefones Celulares, PDAs e Outros Aparelhos com *Bluetooth*

Telefones celulares deixaram de ser meramente aparelhos utilizados para fazer ligações telefônicas e passaram a incorporar diversas funcionalidades, tais como: calendário, despertador, agenda telefônica e de compromissos, câmera fotográfica, envio e recebimento de texto e imagens, etc.

A tecnologia *bluetooth*[5] tem sido introduzida em diversos tipos de telefones celulares para permitir a transmissão de dados entre eles (por exemplo, contatos da agenda telefônica, agenda de compromissos, texto, imagens, etc), bem como conectar um telefone a outros tipos de dispositivo (por exemplo, fones de ouvido, sistema viva-voz de automóveis, etc). Outros exemplos de aparelhos que podem fornecer esta tecnologia são PDAs e *notebooks*.

O fato é que a inclusão da tecnologia *bluetooth* em aparelhos como telefones celulares e PDAs, entre outros, trouxe alguns riscos que podem afetar a privacidade de seus usuários.

[4] Detalhes sobre criptografia de chaves pública e privada estão disponíveis na Parte I: Conceitos de Segurança.
[5] A definição deste termo pode ser encontrada no Glossário.

5.1 Que riscos estão associados ao uso de aparelhos com *bluetooth*?

Muitas vezes, um aparelho que fornece a tecnologia *bluetooth* vem configurado de fábrica, ou é posteriormente configurado, de modo que qualquer outro aparelho possa se conectar a ele, indiscriminadamente. Esta configuração normalmente permite que dados sejam obtidos do aparelho sem qualquer tipo de controle.

O problema não reside no fato do aparelho disponibilizar a tecnologia, mas sim na má configuração das opções de *bluetooth*, que podem permitir que terceiros obtenham diversas informações de um aparelho. Estas informações podem incluir: agenda telefônica, agenda de compromissos, arquivos, imagens, entre outras.

Pode-se citar como exemplos os casos de algumas celebridades que tiveram todos os contatos telefônicos armazenados em seus aparelhos furtados e disponibilizados na Internet.

5.2 Que cuidados devo ter para evitar a exposição de informações de um aparelho com *bluetooth*?

É preciso tomar alguns cuidados para evitar a exposição de informações de um aparelho que fornece a tecnologia *bluetooth*. Alguns dos principais cuidados são:

- mantenha o *bluetooth* do seu aparelho desabilitado e somente habilite-o quando for necessário. Caso isto não seja possível, consulte o manual do seu aparelho e configure-o para que não seja identificado (ou "descoberto") por outros aparelhos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível");
- fique atento às notícias, principalmente àquelas sobre segurança, veiculadas no *site* do fabricante do seu aparelho;
- aplique todas as correções de segurança (*patches*) que forem disponibilizadas pelo fabricante do seu aparelho, para evitar que possua vulnerabilidades;
- caso você tenha comprado uma aparelho usado, restaure as opções de fábrica (em muitos aparelhos esta opção aparece como "Restaurar Configuração de Fábrica" ou "Restaurar Configuração Original") e configure-o como no primeiro item, antes de inserir quaisquer dados.

Como Obter este Documento

Este documento pode ser obtido em http://cartilha.cert.br/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@cert.br.

Licença de Uso da Cartilha

Agradecimentos

O CERT.br agradece a todos que contribuíram para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.