Ciências & Cognição 2007; Vol 10: 46-53 <http://www.cienciasecognicao.org> **© Ciências & Cognição**
Submetido em 08/12/2006 | Revisado em 07/03/2007 | Aceito em 12/03/2007 | ISSN 1806-5821 – Publicado *on line* em 31 de março de 2007

Artigo Científico

Segurança da informação: uma reflexão sobre o componente humano

Information security: a reflection on the human component

Denise Ranghetti Pilar da Silva[✐] **e Lilian Milnitsky Stein**

Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Porto Alegre, Rio Grande do Sul, Brasil

Resumo

Na sociedade informatizada em que vivemos, o papel da segurança da informação é fundamental. A proteção a informações privilegiadas é essencial, e a abordagem mais usada para autenticação de usuários legítimos consiste de sistemas de senhas. Contudo, os requisitos para uma senha segura esbarram nas capacidades cognitivas de seus usuários, dando origem a inúmeros problemas. Este artigo discute esses dois mundos muito diferentes e que precisam interagir: o mundo da tecnologia e o mundo dos seres humanos; questionando a validade e a eficácia do tratamento desses problemas, ao longo da história, pelas pessoas encarregadas. © Ciências & Cognição 2007; Vol. 10: 46-53.

Palavras-chave: senhas; segurança da informação; autenticação; memória humana; capacidades cognitivas.

Abstract

In the networked society of today, the role of information security is fundamental. Protecting privileged information is crucial, and the most used approach for authentication of legitimate users is through password systems. However, the requirements for a secure password conflict directly with the cognitive abilities of their users, what generates countless problems. This paper discusses these two very different worlds that need to interact: the world of technology and the world of human beings. We also question the validity and efficacy of the ways in which these problems were addressed over time. © Ciências & Cognição 2007; Vol. 10: 46-53.

Keywords*: passwords; information security; authentication; human memory; cognitive abilities.*

1. Introdução

Quem sabe dizer, num piscar de olhos, onde seu passaporte está nesse momento? E sua certidão de nascimento? As baterias extras para sua câmera? Esses são apenas alguns exemplos de pequenos incômodos que podem ocorrer no dia-a-dia em conseqüência de lapsos de memória. O uso de senhas envolve preocupações similares. Donald Norman (1990), em seu livro "*Design of Everyday Things*", chama a atenção para a dificuldade que a maioria das pessoas encontra ao precisar lembrar de códigos

✐ **- D.R.P. da Silva** é Bacharel em Ciência da Computação (UPF, Brasil), Mestre em Informática (UCL, Bélgica) e Doutoranda no Programa de Pós Graduação em Psicologia (PUCRS) na Área de Processos Cognitivos. *E-mail* para correspondência: deniserps@gmail.com.

secretos ou senhas. Apesar disso, na Era da Informação em que vivemos, manipulamos uma quantidade de informações cada vez maior. Por essa razão, a demanda por segurança digital tem crescido em função das sérias preocupações a respeito do uso não-autorizado de informações sigilosas e das respectivas conseqüências. Na verdade, o uso de senhas, como forma mais comum de controlar o acesso a informações privilegiadas, envolve dois mundos muito diferentes - tecnológico e humano - que precisam conviver um com o outro e cuja interação tem gerado inúmeros problemas. Este trabalho se propõe a questionar a validade e a eficácia do tratamento desses problemas, ao longo da história, pelas pessoas encarregadas.

Intrusos não-autorizados que tentam burlar a segurança de uma empresa ou indivíduo, por qualquer que seja a razão, são chamados de *hackers*. Ataques de *hackers* vêm sendo noticiados com uma freqüência cada vez maior. As vítimas de tais ataques não mais se restringem a grandes companhias ou departamentos governamentais, já que hoje qualquer indivíduo pode ser alvo de um ataque. Da mesma forma, quando o número de códigos secretos que uma pessoa precisa armazenar e ser capaz de lembrar aumenta muito, a memória pode falhar. Quando a memória fica sobrecarregada, pode ser muito difícil lidar com a variedade de dados necessários diariamente. Para as atividades diárias, temos que ter disponíveis em nossa memória desde números de telefone, números de contas bancárias, números de documentos e senhas; sem falar em informações mais pessoais tais como endereços, datas de aniversário, tamanhos de roupas, e assim por diante.

Especificamente no caso de códigos secretos, ou senhas, é importante que sejam mantidos em segredo, uma vez que protegem informações confidenciais. Algumas senhas ainda devem ser periodicamente alteradas. Como pode alguém, lembrar de tantas senhas? Ao que tudo indica, não é possível. De que maneira, então, as pessoas administram a situação?

Muitas pessoas criam algum tipo de registro físico do código secreto, seja eletronicamente, seja em papel. Tal registro físico é às vezes disfarçado ou escondido, o que, por sua vez, cria outros problemas: como lembrar qual o disfarce usado ou onde o registro físico foi armazenado. Sabe-se que pessoas escondem coisas em lugares improváveis, mas, em geral, existe uma lógica envolvida na escolha desses lugares. Há evidências que amparam a hipótese de que o esquecimento do disfarce ou do esconderijo pode ocorrer quando há tanto um julgamento de que o local é altamente memorável, quanto um julgamento de que o local é improvável para o objeto (Winograd e Soloway, 1986).

O problema da segurança da informação tem sempre duas faces, que são representadas pelas características inerentes de dois mundos diferentes e por vezes conflitantes: o mundo da tecnologia e o mundo dos seres humanos.

A maioria dos profissionais de tecnologia, em algum momento, já se deparou com problemas relacionados à utilização de seus sistemas que não foram considerados na fase de projeto, ou que foram ao menos, subestimados pelos projetistas. Uma vez que o comportamento humano é complexo e envolve variáveis que não podem ser controladas, se torna difícil, para profissionais da informação, pensar no usuário humano como um componente dos sistemas com que trabalham e que abrangem não apenas máquinas e métodos organizados para coletar, processar, transmitir e disseminar dados que representam informação para o usuário. Assim, parece bem mais confortável aderir às variáveis que podem, de fato, ser controladas, tais como *hardware* e *software.*

2. O mundo tecnológico: segurança da informação

A maioria das definições de Segurança da Informação (SI) (Brostoff, 2004; Morris e Thompson, 1979; Sieberg, 2005; Smith, 2002; Wikipedia, 2005) pode ser sumarizada como a proteção contra o uso ou acesso não-autorizado à informação, bem como a

proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas. A SI não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma. É importante lembrar que a SI também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros.

Embora, na prática, não se possa erradicar completamente o risco de uso impróprio ou mal-intencionado de qualquer informação, muitos esforços já foram feitos no sentido de aprimorar os sistemas de SI. Apesar disso, durante muito tempo, houve pouca ou nenhuma preocupação com as capacidades e limitações humanas dos usuários desses sistemas.

Uma das áreas-chave em Segurança da Informação é a autenticação, ou o processo pelo qual os sistemas distinguem usuários autorizados de outros não-autorizados. A autenticação de usuário é, pois, um componente vital de sistemas com informações críticas ou serviços personalizados (Renaud e DeAngeli, 2004). À medida que a oferta de serviços online, tais como *online banking* ou comércio eletrônico, cresce exponencialmente, a demanda por proteção de informações críticas vem aumentando na mesma proporção. Além disso, a autenticação via Internet pode ser ainda mais complexa do que em outros tipos de sistemas, pois envolve fatores além do controle das equipes de segurança, como o equipamento ou o sistema operacional do usuário.

Apesar de suas falhas básicas e de causar problemas de memorabilidade para os usuários, sistemas de senhas ainda constituem a abordagem mais utilizada para autenticação. Em sistemas desse tipo, em primeiro lugar, a pessoa declara sua identidade, por exemplo, com um nome de usuário, e então revela ao sistema um código secreto ou palavra-chave, que somente o usuário deveria conhecer. As vantagens de sistemas de autenticação por senhas decorrem do fato de que estes não requerem equipamento especial, como leitores de impressões digitais. Ainda, se comprometidos por uma invasão, os objetos de identificação, isto é, nome de usuário e senha, podem ser alterados facilmente, e a um custo muito baixo.

Do ponto de vista da Segurança da Informação, uma boa senha deveria ser segura, o que foi definido por algumas diretrizes publicadas pelo Departamento de Defesa Americano (DoD), em 1985. Além de várias recomendações técnicas para a implementação e gerenciamento de senhas, o documento do DoD forneceu recomendações sobre como os indivíduos deveriam selecionar e administrar suas senhas. Essas recomendações deram origem às seguintes regras (Smith, 2002):

1. Cada senha escolhida deve ser nova e diferente, já que o uso de uma única senha para vários sistemas pode dar aos invasores uma grande vantagem ao interceptar uma só senha;
2. Senhas devem ser memorizadas. Se uma senha é registrada em papel, este deve ser armazenado em local seguro;
3. Senhas devem ser compostas de pelo menos seis caracteres, provavelmente mais, dependendo do tamanho do conjunto de caracteres usado, i.e. se contêm apenas números, números e letras, ou se contêm uma combinção de números, letras e outros caracteres do teclado como, por exemplo, "*", "%", "$", "#", "@", e outros;
4. Senhas devem ser substituídas periodicamente;
5. Senhas devem conter uma mistura de letras (tanto maiúsculas quanto minúsculas), dígitos e caracteres de pontuação.

Por outro lado, do ponto de vista do usuário, a autenticação é apenas uma tarefa obrigatória para ter acesso aos recursos necessários à realização do trabalho real. Sob

essa ótica, uma boa senha deveria ser facilmente disponível, não requerer equipamento especial nem conhecimento técnico, ser conveniente (isto é, não consumir muito tempo) e, acima de tudo, ser fácil de lembrar. Essas motivações, associadas às limitações cognitivas dos seres humanos conflitam diretamente com as recomendações do DoD.

2.1. A segurança da informação e a sociedade

Segredos e códigos secretos existem desde os primórdios da humanidade. Há registros de escrita codificada já no Egito Antigo, datando de aproximadamente 1900 a.C. (Aranha, n.d.). Da mesma forma, as tentativas de decifrar tais códigos são provavelmente tão antigas quanto eles. Pode-se então dizer que, de certa forma, a SI sempre existiu, embora sua relevância tenha crescido ao longo do tempo, especialmente nos últimos anos. Hoje a Segurança da Informação se tornou um problema importante da sociedade moderna. Desde grandes empresas a indivíduos comuns, todos têm o direito de esperar que seus dados privados sejam mantidos intactos e disponibilizados apenas a pessoas autorizadas.

As organizações estão cada vez mais cientes dos riscos de ataques a suas informações privilegiadas, porém, os indivíduos comuns e em alguns casos, até mesmo órgãos do governo tendem a acreditar que é improvável que eles sejam alvo de ataque. Em 29 de Novembro de 2005, em São Paulo, um estagiário do INSS de 18 anos foi preso e acusado de inserir dados falsos nos sistemas da previdência usando senhas de colegas. Em dois anos o jovem acumulou três milhões de reais. Ele adquiriu seis carros de luxo, equipamentos eletrônicos de alto custo e mobiliou sua casa com móveis de alta qualidade. A polícia conseguiu reaver em torno de dois milhões de reais, mas continua investigando o caso (GloboOnline, 2005). Em 2004, outro estudante brasileiro foi condenado a seis anos de prisão por invadir contas bancárias pessoais do Banco do Brasil, Bradesco, Caixa Federal e Itaú. Ele já tinha sido preso outras duas vezes anteriormente, mas foi liberado por falta de provas (FolhaOnline, 2004).

Alguns *hackers* buscam lucro financeiro, outros procuram segredos corporativos, outros ainda estão atrás do fascinante desafio de encontrar a chave para o território proibido das informações confidenciais de outros. Com a capacidade de processamento dos computadores modernos e com programas especiais para decifrar senhas, uma senha composta de seis letras minúsculas - o que significa 308 milhões de combinações - pode ser decifrada por um *hacker,* em média, em dez segundos (Garancis, 2004). O mais surpreendente é que tais programas estão disponíveis gratuitamente na *Internet*.

Um ataque de *hackers* pode ser descrito, de forma ampla, como adivinhação em alta velocidade. Assim, a força de uma senha poderia ser medida em termos do tempo necessário para decifrá-la, que pode variar de segundos a milênios. Os três métodos mais usados pelos programas que decifram senhas são ataques de dicionário (ou listas de palavras), ataques híbridos e ataques de força-bruta. Um ataque de dicionário se utiliza de listas de palavras que às vezes contêm dicionários inteiros e que podem ser altamente especializados, como por exemplo, ao atacar um hospital, além de utilizar um dicionário padrão, consultar um dicionário médico. Ataques de dicionário decifram, em média, 25% de todas as senhas e levam apenas alguns segundos. Um ataque híbrido é similar a um ataque de dicionário, mas leva um pouco mais de tempo. Ataques híbridos estendem ataques de dicionário ao acrescentar versões ligeiramente modificadas de palavras que os usuários poderiam tentar no intuito de tornar uma senha mais difícil de ser decifrada, por exemplo, substituindo números por letras visualmente similares, adicionando dígitos ao fim da senha, digitando a palavra de trás para frente, e assim por diante (por exemplo, se a senha escolhida for "salada", a letra "l" minúscula poderia ser substituída pelo número "1" e a letra "S", pelo símbolo "$", gerando então "$a1ada"). Em um ataque de força-bruta, toda e qualquer combinação

possível é testada. Esse é o método mais lento, por exemplo, decifrar uma senha de oito caracteres, com ao menos uma letra maiúscula, uma minúscula e um número, levaria em torno de 6354 horas (Brostoff, 2004). Poder-se-ia então concluir que, para o mundo da tecnologia, quanto maior e mais complexa for uma senha, mais tempo será necessário para decifrá-la, e portanto, mais robusta ela poderá ser considerada.

Ao longo dos últimos vinte anos, a abordagem tradicional à segurança tem sido tentar solucionar o problema desenvolvendo tecnologias cada vez mais complexas para proteger as informações, tais como protocolos de encriptação ou certificados de segurança. Considerando o crescente número de ataques, pode-se dizer que esse tipo de medidas não parece ser suficiente para assegurar que a informação esteja segura. Na verdade, ao que tudo indica, o Mundo Tecnológico se sente entitulado a controlar a segurança, como se indiretamente afirmasse que o Mundo Humano não o é.

3. O mundo humano

Muitas das deficiências dos sistemas de autenticação por senhas se originam das limitações da memória humana. Se não fosse necessário lembrar de senhas, elas poderiam, com certeza, ser muito seguras, isto é, totalmente aleatórias, tão longas quanto as limitações do sistema permitissem, e conter todos os tipos de caracteres.

A ironia maior no uso de senhas é que uma senha deveria ser fácil de aprender e lembrar para seu proprietário, mas difícil de ser adivinhada ou decifrada por outras pessoas. Brown e colaboradores (2004) apontam que a literatura é bastante escassa ao fornecer procedimentos claros, passo a passo, que auxiliem na geração e recordação de senhas. A maioria dos poucos artigos existentes não leva em consideração as limitações cognitivas impostas pela natureza humana. Assim, as pessoas são obrigadas a conviver com um dilema entre a segurança e a conveniência.

3.1. O componente humano em um sistema de segurança de informação

A comunidade de segurança da informação recentemente deu-se conta de que o comportamento do usuário desempenha um papel importante em incidentes de segurança. Sistemas de segurança da informação são freqüentemente comparados a uma corrente com muitos elos representando os componentes envolvidos, tais como equipamento, *software*, protocolos de comunicação de dados, e outros, incluindo o usuário humano. Na literatura sobre segurança da informação, o usuário humano é freqüentemente referenciado como o elo mais fraco (Sasse *et al.*, 2001). Entretanto, além de culpar o usuário, pouco tem sido feito para identificar os fatores que levam a comportamentos potencialmente inseguros e menos ainda para tentar resolver tais problemas. Corporações já gastaram milhões de dólares em *firewalls*, encriptação e dispositivos de acesso seguro. Recursos que talvez tenham sido desperdiçados, uma vez que os usuários desses sistemas ainda são humanos, com todas as suas limitações humanas e, portanto, ainda o elo mais fraco.

Há uma série de características que impactam o projeto e o uso de sistemas de senhas. Entre essas características, uma das principais é a memorabilidade. Existe uma vasta gama de pesquisas em Psicologia da memória, que poderia ser usada para auxiliar na melhor compreensão do que está acontecendo de fato na mente humana ao ter que lembrar várias senhas no dia-a-dia.

Os critérios para gerar senhas fortes fazem com que seja difícil para seres humanos mantê-las na memória, especialmente quando se tem várias senhas para lembrar. O que, então, as pessoas fazem? Há vários "maus hábitos", amplamente difundidos, que já foram identificados (Brown *et al.*, 2004, Yan *et al.*, 2004). Tais maus hábitos incluem escrever as senhas em papel e armazená-los em locais óbvios, como o monitor do computador ou sob o *mouse pad*, ou utilizar a mesma senha repetidamente, ou ainda, escolher palavras simples ou nomes

que são muito fáceis de adivinhar. Maus hábitos no uso de senhas significam que políticas de segurança, que foram cuidadosamente elaboradas, não estão sendo observadas. Na verdade, esses maus hábitos se materializam em vulnerabilidades de sistemas de informação, tais como senhas fracas, senhas comuns ou senhas visíveis.

Dentre os muito poucos estudos que têm investigado a criação e o uso de senhas, Brown e colaboradores (2004) entrevistaram 218 estudantes de graduação para avaliar a geração e o uso de senhas. Com base em um levantamento prévio, 19 itens foram incluídos no questionário, como conta bancária ou *e-mail*. Para cada item, os participantes deveriam descrever o tipo de informação usada para criar ou lembrar da senha. Os resultados mostraram que dois terços das senhas foram geradas em torno de características pessoais dos usuários e a maioria das senhas restantes se relacionava à família, amigos ou relacionamentos amorosos. Nomes próprios e aniversários compunham aproximadamente metade de todas as senhas levantadas. O estudo ainda encontrou suporte empírico para os maus hábitos mencionados acima. Quase todos os entrevistados reusavam senhas e mais da metade deles mantinha uma cópia escrita de suas senhas. O estudo de Brown e colegas corrobora achados de estudos anteriores, menos abrangentes, mas que também detectaram alguns maus hábitos e onde apenas um pequeno percentual de senhas foi criado de acordo com as diretrizes de segurança. Por exemplo, Carstens e colaboradores (2004) encontraram que indivíduos com oito a onze senhas corriam maior risco de não conseguir lembrá-las. Com a proliferação de websites que requerem autenticação, e-mails pessoais e profissionais, contas bancárias, etc., possuir múltiplas senhas não é incomum nos dias de hoje.

Entretanto, fora do mundo tecnológico, pouca atenção tem sido dada a problemas especificamente relacionados ao uso de senhas. Embora periódicos de tecnologia e administração (*e.g.* Ives *et al.*, 2004; Sasse *et al.*, 2001; Sieberg, 2005; Smith, 2002) tenham tratado de alguns aspectos pragmáticos da segurança de senhas, tais como maus hábitos e perdas de produtividade associadas ao esquecimento de senhas, na literatura psicológica ou da área de Interação Humano-Computador pouco foi dito sobre os aspectos cognitivos da criação, uso e esquecimento de senhas.

Todos os maus hábitos mencionados acima, bem como as falhas de memória no uso de senhas, acontecem simplesmente porque, na impossibilidade de memorizar suas senhas, as pessoas desenvolvem estratégias não seguras. Os estudos da Psicologia Cognitiva, que têm estudado o funcionamento da memória, têm mostrado consistentemente que:

- guardar informações literais, ou detalhes superficiais como a exata ordem em que os caracteres aparecem em uma senha, é uma coisa difícil (Reyna e Brainerd, 1995);
- as pessoas tendem a ter facilidade de lembrar de coisas que têm significado (Tulving e Craik, 2000) - o que geralmente não é o caso das senhas aleatórias ou geradas pelo sistema;
- com a falta de uso e a passagem do tempo, traços literais, como a estrutura da senha ou a fonte, tendem a se perder;
- o fato de processar informações de natureza semelhante interfere no registro mnemônico dessas informações (Teoria da Interferência, Pergher e Stein, 2003; Dempster e Brainerd, 1995), acarretando perda de parte ou de toda a informação.

Assim sendo, a indústria da segurança da informação, em seus esforços para tornar a autenticação por meio de senhas um mecanismo mais viável, poderia considerar o vasto arcabouço de conhecimento que a Psicologia da memória possui.

4. Considerações finais

Será possível obter senhas seguras que possam realmente ser lembradas? De acordo com Sasse e colaboradores (2001), especialis-

tas, tanto de segurança quanto de usabilidade, já afirmaram que lembrar de senhas fortes é uma tarefa impossível para seres humanos, uma vez que senhas fortes consistem de itens sem sentido e assim são inerentemente difíceis de lembrar. Por outro lado, poderia ser viável criar senhas que são combinações pseudo-aleatórias de letras, números e símbolos, significativas para seus donos, mas sem sentido para outras pessoas. Instruir usuários a criar esse tipo de senhas pode ser muito útil, embora a efetividade desta abordagem ainda não tenha sido extensivamente testada. Nielsen (2004) diz que é indispensável treinar os usuários, embora essa medida, isoladamente, não seja suficiente para erradicar os problemas relacionados ao uso de senhas.

Quais são os fatores que mais afetam o desempenho humano, em relação ao uso de senhas? Esta questão parece ainda não ter resposta. Poderia ser qualquer combinação de fatores como sobrecarga de informações, fadiga, estresse, idade, tamanho das senhas, complexidade, número de senhas diferentes, freqüência de alteração, ou objetivos incompatíveis entre si. No que diz respeito a senhas, a interferência parece sem dúvida muito plausível, especialmente quando um usuário precisa de lembrar de várias senhas. Também nos parece claro que senhas são um caso muito especial de memória literal, já que detalhes, como a ordem dos caracteres, devem ser lembrados precisamente. O esquecimento de um único caractere ou a falha em lembrar a ordem exata em que estes aparecem invariavelmente implica acesso negado.

Todos possuímos informações valiosas que gostaríamos de manter confidenciais, por razões financeiras ou emocionais. Para que possamos atingir esse objetivo, é urgente buscarmos algumas respostas, no sentido de usar nossa capacidade de memória em nosso favor. Se as limitações da memória humana forem levadas em consideração, uma ponte ligando o Mundo Humano e o Mundo Tecnológico poderia ser construída e a cadeia de segurança, como um todo, poderia se beneficiar. Já estamos começando muito tarde.

Agradecimentos

Gostaríamos de agradecer ao nosso Auxiliar de Pesquisa, Carlos F. A. Gomes, pela sua valiosa ajuda nas buscas de literatura.

5. Referências bibliográficas

Aranha, A. C. (n.d.) *A sociedade e a segurança da informação*. MicrosoftTechNet. Disponível em: http://www.microsoft.com/brasil/technet/Colunas/AnnaCarolinaAranha/Seguranca.mspx, acessado em 11/11/05.

Brostoff, S. (2004). *Improving password system effectiveness*. Tese de Doutorado. University College London.

Brown, A.S.; Bracken, E., Zoccoli, S. e Douglas, K. (2004). Generating and remembering passwords. *Appl. Cogn. Psychol.*, 18, 641-651.

Carstens, D. S.; McCauley-Bell, P.; Malone. L. C. e DeMara, R.F. (2004). Evaluation of the human impact of password authentication practices on Information Security. *Inform. Sci. J.,* 7, 67-85.

Dempster, F.N. e Brainerd, C.J. (1995). *Interference and Inhibition in Cognition*. San Diego, CA: Academmic Press.

FolhaOnline. (2004). Brasileiro é condenado à prisão por invasão de sites de bancos. *Folha Online Informática*. Publicado em 5 de Janeiro de 2004. Disponível em: http://www1.folha.uol.com.br/folha/informatica/ult124u14866.shtml, acessado em 20/10/05.

Garancis, P. (2004). My gate is locked, is yours? A look at implementing a strong password policy. *Technical Report*. Publicado em fevereiro de 2004. Disponível em: http://www.giac.org/Practical/GSEC/Peter_Garancis_GSEC.pdf, acessado em 20/10/05.

GloboOnline. (2005). Estagiário desvia R$ 3 milhões do INSS. *Globo Online*. Publicado em 29 de novembro de 2005. Disponível em: http://oglobo.globo.com/online/sp/189451733.asp, acessado em 25/10/05.

Ives, B.; Walsh, K.R. e Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, 47, 76-78.

Morris, R. & Thompson, K. (1979). Password security: a case history. *Communications of*

the ACM, 22, 594-597.
Nielsen, J. (2004). *User education is not the answer to security problems*. Disponível em: http://www.useit.com/alertbox/20041025.html, acessado em 26/01/05.
Norman, D.A. (1990). *The Design of Everyday Things*. New York: Doubeday.
Pergher, G.K. e Stein, L.M. (2003). Comprendendo o Esquecimento: Teorias clássicas e seus fundamentos experimentais. *Rev. Est. Psicol.*, 14, 129-155.
Renaud, K. e De Angeli, A. (2004). My password is here! An investigation into visuo-spatial authentication mechanisms. *Interacting with Computers*, 16, 1017-1041.
Reyna, V.F. e Brainerd, C.J. (1995). Fuzzy-trace theory: An interim synthesis. *Learning and Individual Differences*, 7, 1-75.
Sasse, M.A., Brostoff, S. e Weirich, D. (2001). Transforming the "weakest link" — a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19, 122-131.
Sieberg, D. (2005). Hackers shift focus to financial gain. *CNN.com - Special Reports - Online Security*. Publicado em 26 de setembro de 2005. Disponível em: http://www.cnn.com/2005/TECH/internet/09/26/identity.hacker/index.html.
Smith, R.E. (2002). The strong password dilemma. *Authentication: From Passwords to Public Keys*. Chapter 6. Addison-Wesley.
Tulving, E. e Craik, F. (2000). *The Oxford Handbook of Memory*. New York. Oxford University Press US.
Wikipedia. (2005) *Wikipédia, a enciclopédia livre.* Disponível em: http://pt.wikipedia.org/wiki/Segurança_da_informação, acessado em 10/10/05.
Winograd, E. e Soloway, R.M. (1986). On forgetting the locations of things stored on special places. *J. Exp. Psychol.,* 115, 366-372.
Yan, J.; Blackwell, A.; Anderson, R. e Grant, A. (2004). Password memorability and securety: empirical results. Security e Privacy, *IEEE Computer Society*, 25-31.