



# SENHA OU NÃO SENHA... EIS A QUESTÃO!

Por prof. Mauricio Andrade de Paula e Rafael Abrão Possik Jr.

Uma **senha** ou **palavra-chave** (por vezes referida no inglês como *password*) é uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento. Em sistemas computacionais (ou em nossa atual vida moderna amplamente conectada), senhas são amplamente utilizadas para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas nos diferentes sistemas e ferramentas.

Hoje em dia, a quantidade de sistemas e ferramentas (bancos, *e-mail*, Intranet, rede local, celular, banda larga, comunidades, *sites* de relacionamento, comunicadores instantâneos, etc.) que precisamos utilizar no dia-a-dia é extremamente grande, e ao mesmo tempo acaba sendo uma tarefa um tanto quanto trabalhosa devido à enorme quantidade de senhas que precisamos memorizar. E isso se torna um grande problema na vida da maior parte dos usuários.

As senhas existem para identificar e autenticar o acesso de um determinado usuário a alguma informação ou sistema. Portanto, caso você tenha permissão para acessar um determinado módulo do sistema da sua empresa, é porque você deve ter acesso àquela informação. Da mesma forma, se outro colaborador da empresa não

tem acesso é porque ele não deve ter conhecimento de tais informações, por isso você não deve “emprestar” sua senha para ele acessar o sistema sob nenhuma circunstância.

Às vezes, devido a diversos motivos, ao cadastrar uma senha sempre pensamos em algo que seja fácil de lembrar. Porém, em muitos casos esse algo é tão fácil ou óbvio, que além de você, também todos os seus colegas de trabalho, seus amigos, entre outros, saberão ou lembrarão, caso tenham oportunidade de conhecê-la.

Devido a esse fato e a outros motivos devemos ter o máximo de cuidado com nossa senha.

Estudos recentes mostram que ataques do tipo *phishing* (prática que engana usuários de Internet e os conduzem a *sites* de mentira, com visual e logomarca igual ao original, e tem o objetivo de roubar a senha e demais informações) estão se tornando um tipo de fraude comum, que as instituições financeiras e empresas devem combater.

Novos métodos de fraude *on-line* utilizam técnicas variadas, como *spyware* (*software* espião instalado na máquina do usuário que monitora suas ações), seqüestro de navegadores e ferramentas de administração remota da máquina do usuário.



Enquanto as tecnologias desenvolvidas pela indústria de *software* contra o *phishing* estão dando resultado, elas são pouco eficazes na proteção de empresas e consumidores contra *softwares* mal-intencionados nos PCs (*personal computer*), que roubam os dados sem a ciência do usuário.

Computadores pessoais estão altamente vulneráveis ao ataque desses *softwares* mal-intencionados, por isso bancos e empresas precisarão reconhecer que cada vez mais será necessário melhorar a identificação do usuário pela Internet e demais canais *on-line*. Autenticações fortes, como por exemplo, *tokens*, serão cada vez mais comuns.

Pesquisas disponíveis em *SearchSecurity.com*, citadas por Eusébio Coterillo, diretor da Actividentity da América Latina, mostram que:

- 74% dos usuários de Internet precisam lembrar muitas senhas e 63% dizem que conviver com várias políticas de senha é um problema ou um problema significativo.
- Mais de 56% dizem que tiveram que “ressetar” suas senhas.
- 79% dizem que suas organizações estão gastando o mesmo ou mais no gerenciamento de senhas este ano.

Investir em alternativas de autenticação deve ser uma constante ou aumentar em várias organizações:

- 64% estão investindo pesado em *tokens* de autenticação.
- 74% estão investindo em certificados digitais.
- 50% estão investindo em *smart-cards* (cartões inteligentes).
- 70% estão investindo sistemas de *single sign-on*, onde apenas uma autenticação dá acesso a todos os sistemas.
- 63% estão investindo em sistema *single sign-on* para uso pela Internet.

Na FAAP, um excelente exemplo de uso dessas novas tecnologias pode ser observado na forma como os usuários são verificados para ter acesso ao Cubo - pelo mapeamento das

veias da mão esquerda.

Na área de tecnologia da informação (TI), dirigida por Paulo Cesar Klein, a FAAP está testando *tokens* para autenticação nos sistemas em uso pela Fundação como Lyceum, Oracle, Intranet, Internet Alunos, Internet Professores, Internet Pós-Graduação e MBA.

Mas se você ainda não usa ferramentas de autenticação forte, aqui vão algumas dicas para minimizar os riscos de fraude:

- Combine letras, símbolos e números de que você se lembre facilmente e que sejam difíceis para os outros adivinharem.
- Crie senhas que possam ser pronunciadas (mesmo que não sejam palavras comuns), fáceis de lembrar, o que diminui a tentação de anotá-las.
- Tente usar as letras iniciais de uma frase que você goste, especialmente se ela incluir um número ou caractere especial.
- Use duas coisas familiares e combine-as com um número ou caractere especial. Como alternativa, altere a ortografia incluindo um caractere especial. Dessa forma, você obtém algo desconhecido, o que gera uma boa senha, pois é fácil para você, e somente para você, lembrar, mas difícil para qualquer outra pessoa descobrir. Aqui estão alguns exemplos: “Estou + 100 + dinheiro” = “Estou100dinheiro” ou “E\$toU100dinheir0” / “gato + \* + Rato” = “gato\*Rato” ou “gato\*R@ato”, ou ainda, “ataque + 3 + livro” = “ataque3livro” ou “@taque3livr0”

#### O que você não deve fazer:

- Não use informações pessoais, como derivados da sua identidade de usuário, nomes de membros da família, nomes de solteira, carros, placas de auto-

## Na FAAP, um excelente exemplo de uso dessas novas tecnologias pode ser observado na forma como os usuários são verificados para ter acesso ao Cubo - pelo mapeamento das veias da mão esquerda

móveis, números de telefone, animais de estimação, aniversários, números de CPF, endereços ou passatempos.

- Não use palavras em qualquer idioma, soletradas de trás para frente ou de frente para trás.
- Não junte senhas ao mês. Por exemplo, não é conveniente ter em maio a senha “Maioral”.
- Não crie senhas, substancialmente parecidas com as senhas usadas anteriormente.

Os usuários geralmente têm muitas contas de computador diferentes no trabalho, contas de telefone celular, banco, companhias de seguro, entre outras. Para facilitar a memorização das senhas, os usuários geralmente usam a mesma senha ou senhas parecidas em cada sistema e, se puderem escolher, a maioria dos usuários escolhe uma senha muito simples e fácil de lembrar, como a data de nascimento, o nome de solteira da mãe ou o nome de um parente. Senhas curtas e simples são relativamente fáceis de serem descobertas por atacantes. Alguns dos métodos comuns que os *softwares* mal-intencionados usam para descobrir a sua senha são:

- **Adivinhação** - O atacante tenta fazer *logon* usando a conta do usuário e tentando adivinhar repetidamente prováveis palavras e frases, como o nome dos seus filhos, a cidade onde nasceu e times esportivos locais.
- **Ataque de dicionário *on-line***: O atacante usa um programa automatizado que tem um arquivo de texto com palavras. O programa tenta repetidamente fazer *logon* no sistema atacado usando uma palavra diferente do arquivo de texto em cada tentativa.
- **Ataque de dicionário *off-line***: Similar ao ataque de dicionário *on-line*, o atacante obtém uma cópia do arquivo em que a cópia codificada ou criptografada das contas e senhas do usuário está armazenada e

usa um programa automatizado para determinar a senha de cada conta. Esse tipo de ataque pode ser executado muito rapidamente, uma vez que o atacante tenha conseguido obter uma cópia do arquivo de senhas.

- **Ataque de força bruta *off-line***: É uma variação dos ataques de dicionário, mas foi desenvolvido para determinar senhas que possam não estar incluídas no arquivo de texto usado nesses ataques. Embora possa haver tentativas *on-line* de ataques de força bruta, devido à largura de banda e da latência da rede, geralmente elas são executadas *off-line* com o uso de uma cópia do arquivo de senhas do sistema atacado. Em um ataque de força bruta, o atacante se vale de um programa automatizado que gera *hashes* ou valores criptografados de todas as senhas possíveis e compara-as com os valores do arquivo de senhas.

Algo bastante comum é o caso do usuário que informa a sua senha para outro usuário (pai, mãe, irmão, secretária, colega, etc.) dando acesso a ele a informações restritas que não deveria ter. Isso pode até caracterizar crime de falsidade ideológica (artigo 299 do Código Penal Brasileiro).

Cada um dos métodos de ataque apresentados anteriormente pode ser retardado significativamente, ou mesmo impedido, pelo uso de algumas medidas simples e que representam um pequeno investimento perto do risco que um incidente pode gerar. Os computadores que executam as versões recentes do *Windows*, além de outros diversos sistemas operacionais, inclusive os contidos em dispositivos móveis, dão suporte a senhas de alta segurança.