"Ano novo, senhas novas" - Por Lindinaldo Marinho

Neste artigo, o magistrado destaca a importância da escolha de senhas mais seguras.

Estamos na primeira semana de um novo ano, bem apropriado darmos um pouco mais de importância às boas práticas de segurança em tecnologia de informação e comunicação (TIC). Destacaremos neste texto apenas uma das práticas mais básicas por entendermos que esta ainda merece alguns cuidados - ao menos para alguns usuários de TIC.

As estatísticas mencionam que aproximadamente 90% dos usuários da Internet escolhem senhas simples. Pode até parecer um pouco exagerado, mas, conforme análise da SplashData[1], entre as senhas mais utilizadas no mundo, no ano de 2017, destacam-se as senhas “123456” e a “Password”. Vejamos abaixo a relação das 20 “senhas” preferidas no ano de 2017, combinações fáceis e inseguras:

1. 123456 (Sem mudança)	11. admin (Subiu 4)
2. Password (Sem mudança)	12. welcome (Sem mudança)
3. 12345678 (Subiu 1)	13. monkey (Nova)
4. qwerty (Subiu 2)	14. login (Caiu 3)
5. 12345 (Caiu 2)	15. abc123 (Caiu 1)
6. 123456789 (Nova)	16. starwars (Nova)
7. letmein (Nova)	17. 123123 (Nova)
8. 1234567 (Sem mudança)	18. dragon (Subiu 1)
9. football (Caiu 4)	19. passw0rd (Caiu 1)
10. iloveyou (Nova)	20. master (Subiu 1)

* a informação ao lado de cada “senha” refere-se à posição desta no ranking referente ao ano de 2016

Relevante mencionar que as análises de fragilidade de senhas, geralmente, são efetuadas com base nas senhas que se tornaram públicas mediante violações de dados. Para

relembrarmos um pouco deste tema, informamos a seguir as 5 maiores violações da história, conforme notícia divulgada pelo Wall Street Journal[2]:

1. Yahoo! (1 bilhão de vítimas, em 2016-2017)

2. Yahoo! (500 milhões de vítimas, em 2016)

3. Equifax (143 milhões de vítimas, em 2017)

4. Heartland Payment Systems (130 milhões de vítimas, em 2009)

5. LinkedIn (117 milhões de vítimas, em 2016)

Curiosamente, as 20 “senhas” acima listadas representam quase 50% das senhas publicizadas ao longo do ano de 2017.

Esperando haver conseguido atrair a atenção para a importância de utilização de senhas menos óbvias, também queremos chamar a atenção dos usuários de TIC para outros fatores:

- troca periódica das senhas;
- utilização de caracteres minúsculos (a, b, c, ...), maiúsculos (A, B, C, ...), números (0, 1,2, ...) e símbolos (!, @, #, $, ...).

É bem verdade que a alteração periódica de senhas ainda é objeto de alguma controvérsia. Há alguns anos, a Federal Trade Comission, ente que regula as práticas comerciais nos Estados Unidos, chegou a divulgar que a troca periódica de senhas pode, na verdade, enfraquecer a segurança, conclusão baseada em pesquisa que detectou o procedimento dos usuários, de modo geral, em alterar a senha efetuando uma minúscula reciclagem da senha anterior.

De qualquer forma, não vislumbramos necessidade de maior ênfase quanto à alteração periódica de senhas já que o TRT da 13ª Região normatizou a utilização de senhas no âmbito do Tribunal (ATO TRT GP Nº 511/2014), estabelecendo uma periodicidade mínima para a alteração das senhas. E nessa trilha, reputamos um importante passo implementarmos esta prática de procedermos a alteração semestral nas principais senhas utilizadas: e-mail, internet banking, redes sociais, serviços de armazenamento em nuvem.

Mas o que fazer para criar uma senha menos insegura? Vale reportar aqui as dicas contidas na “Cartilha de Segurança de Informação” elaborada pela unidade gestora de TIC do TRT da 13ª Região[3]:

- evitar senhas baseadas em informações pessoais, como nomes, sobrenomes, número de documentos, placas de carros, telefones e datas;
- evitar senhas baseadas em palavras que constem no dicionário de qualquer idioma;
- evitar senhas com caracteres repetidos ou sequenciais (Ex.: aa22, abcde, ab123);
- evitar senhas com caracteres sequenciais no teclado do computador (Ex.: qwer, zxcv);
- elaborar senhas inspiradas em frases, assim, basta lembrar a frase para lembrar a senha (Ex.: a partir da frase “quem ri por último ri melhor” é possível criar a senha “qrpurm”).

Às dicas acima, acrescentamos as seguintes:

- utilizar senhas com pelo menos 8 caracteres;

- conter, no mínimo, 2 letras minúsculas;
- conter, no mínimo, 2 letras maiúsculas;
- conter, no mínimo, 2 caracteres numéricos;
- conter, no mínimo, 2 caracteres símbolos;
- utilizar linguagem “leet” (ou código MUNGE), consistente em substituir letras por números e símbolos que se parecem com as letras (Ex.: a=@, B=8, c=(, D=), E=&, f=ph, ...).

A ideia central é proteger a senha contra ataques de força bruta, onde um criminoso virtual utiliza um código para testar inúmeras senhas sequencialmente, até acertar a correta, com programas facilmente encontrados na internet.

Também é importante termos em mente que não devemos utilizar senhas iguais para todas as suas contas. Até pode ser melhor para a nossa memória, mas certamente também será muito bom para pessoas mal-intencionadas, afinal, basta descobrir uma senha para possibilitar o acesso a todas as demais informações.

E como saber se minha senha é fraca? Há diversas aplicações disponíveis na Internet destinadas a avaliar a complexidade de uma senha e assim ajudar ao usuário a perceber os pontos fortes e eventuais pontos a serem aperfeiçoados na escolha e formulação de senhas.

Vamos apresentar, por ora, a aplicação disponível em: https://password.kaspersky.com/br/ (https://password.kaspersky.com/br/)

Por segurança, lógico, **jamais** digitaremos a senha escolhida em alguma aplicação disponível na Internet, mas usaremos a aplicação para testarmos alguma senha com pontos de similaridade.

Como exemplo, testaremos as senhas "123456" e "Password":

Vejamos o teste da senha inspirada na frase “quem ri por último ri melhor”, acrescida do ano atual (2018), substituindo o “0” e o “8” por seus símbolos equivalentes no teclado do computador “)” e “*”, gerando "qRpUrm2)1*":

As senhas “123456” e “Password” seriam conhecidas instantaneamente por algum programa de computador dedicado a “descobrir senhas”, enquanto a senha “qRpUrm2)1*” seria conhecida somente após 4 anos.

Em síntese, práticas básicas de segurança da informação podem fazer a diferença na redução dos riscos de violação de dados. Os usuários de TIC do Poder Judiciário, especialmente na Justiça do Trabalho onde o índice de processos eletrônicos novos já chegou ao patamar de 100%, necessitam permanente conscientização acerca da relevância de se proteger as informações, importante ativo para a instituição, cuja adulteração pode afetar a tramitação dos processos, além da imagem perante a sociedade.

Por que cometer erros antigos se há tantos erros novos para escolher? (Bertrand Russel)

LINDINALDO SILVA MARINHO

Juiz do Trabalho Substituto

Presidente do Comitê Gestor de Segurança da Informação do TRT da 13ª Região

_____

1 A SplashData é uma das principais empresas fornecedoras de aplicativos e serviços de segurança, em atuação há mais de 10 anos

2 https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804 acessado em 02/01/2018

3 https://www.trt13.jus.br/institucional/seguranca-da-informacao/estrutura-normativa/normas