Login e senha – Qual o risco para a empresa quando um colaborador não toma os devidos cuidados?

Lidar com o *login* e senha de forma correta e segura é imprescindível para qualquer empresa e colaborador, independente do cargo que ocupa, pois seu uso ou divulgação indevida, mesmo que por descuido pode gerar danos e responsabilidade para si e para a empresa.

Cabe como primeiro passo ter ciência de que *login* e senha é nossa identidade digital, ou seja, ao se logar, o usuário está informando quem é a pessoa que vai acessar aquela máquina e/ou sistema e consequentemente, as informações ali contidas, assim, se alguém se logar com seu usuário e praticar atos ilícitos, como por exemplo, desvio de verbas, lançamentos indevidos, cópia de uma informação confidencial, entre outros, o sistema apontará você como autor do ato.

Portanto, quando alguém empresta sua identidade digital, está permitindo que outra pessoa se passe por ela e na prática se essa pessoal praticar atos ilícitos ou mesmo infringir uma norma interna da empresa, o primeiro suspeito será o titular da identidade digital.

Mas e para a empresa, quais são os riscos?

O cenário mais comum, atualmente, infelizmente é de que ainda encontramos *logins* e senhas anotados em pos*t it* no monitor ou em baixo do teclado ou ainda culturalmente pessoas se *logam* nas máquinas e deixam que outras pessoas acessem em seu lugar, recentemente estive em uma Fundição em que um colaborador acessava sites pornográficos pela máquina do gestor.

Ocorre que cada perfil de acesso deve ter designado os locais e informações que aquele determinado cargo pode acessar. Imagine quando um gestor permite que um colaborador acesse o sistema utilizando seu perfil, como mencionado acima?

Com certeza o acesso a ele permitido não é o mesmo que seria permitido a outros colaboradores e se este estiver com más intenções, o risco passa a ser iminente.

Um exemplo prático, geralmente os gestores tem informações de orçamentos e clientes, imagine se um colaborador acessa tais informações e resolve “vender” ao concorrente. É certo que se trata de pratica de concorrência desleal e os dois podem responder pelo crime, quem vendeu a informação e quem comprou (pessoa física), mas ocorre que depois de praticado, por mais que seja identificado e punido o autor, o dano já ocorreu e muitas vezes até afeta a imagem da empresa no mercado.

Com certeza seu cliente busca uma fundição o qual as informações, protótipos, ferramentas e artes estejam seguras de espionagem.

É comum, colaboradores da área administrativa permitirem acesso (por seu login e senha) à internet, sem lembrar que nenhum cargo deve ser menosprezado e que o mais simples empregado pode ter conhecimentos técnicos ou básicos de informática, sendo suficiente para copiar as informações ali contidas.

Além disso, hoje com o monitoramento, é possível saber os acessos de internet e frequentemente me deparo com casos em que foi indicado acesso a sites pornográficos, mas quem estava na máquina era outra pessoa, como o exemplo utilizado no início deste artigo.

Imagine que se ao invés de sites pornográficos fossem acessados sites de pedofilia, o titular do *login* e senha seria o primeiro suspeito de tais atos e mais, se na sala não houver câmeras e a identificação não for feita na hora para que se possa verificar quem realmente está na máquina, para todos os efeitos os indícios sempre apontarão para o perfil identificado, e por que arriscar responder um processo criminal pelo ato de outra pessoa?

É preciso que as empresas trabalhem cultura de preservação de sua identidade digital, bem como criação de senhas fortes, ou seja, não óbvias e difícil descoberta.

Tecnicamente, a empresa pode forçar a alteração de senha no primeiro acesso, sendo que necessariamente o colaborador deva criar senhas fortes, constituindo-se por caracteres diversos, incluindo símbolos, números, caixa alta e baixa.

O uso responsável diz respeito ao comportamento de cada pessoa e a conscientização é uma forte aliada da prevenção.

E é claro, que não deve negligenciar na conscientização, o tema pode ser abordado tanto no termo de responsabilidade, como também em palestras e cartilhas.

Cristina Sleiman é advogada e pedagoga, mestre em Sistemas Eletrônicos pela Escola Politécnica da USP e com extensão em Direito da Tecnologia pela FGV/RJ, extensão Educador Virtual pelo Senac São Paulo em parceria com Simon Fraser University. Sócia do escritório Cristina Sleiman Sociedade de Advogados, professora de Pós Graduação na Faculdade Impacta de Tecnologia, responsável pela coordenadoria de Prevenção de Crimes de alta tecnologia no ambiente corporativo na Comissão de Crimes de Alta Tecnologia da OAB/SP. Co-autora do audiolivro e livro Direito Digital no Dia a Dia publicado pela Saraiva. www.cristinasleiman.com.br / cristina@sleiman.com.br.

Revista Abifa - 2011