

## **A Segurança da Informação no dia-a-dia**

Segurança da informação, cada vez mais, se passa por comportamento. Aprendemos sobre segurança logo cedo na vida, quando somos instruídos a não deixar a porta de casa aberta, a não passar informação pelo telefone sem saber quem está do outro lado da linha, e qual sua intenção, a sempre desligar eletrodomésticos da tomada para evitar curto circuito, a não pegar carona com qualquer um, nem que diga que é um conhecido da família que você não está lembrado. O hábito de segurança precisa ser ensinado, incorporado na rotina. E o mesmo ocorre quando fazemos uso de tecnologias, seja o celular, o computador ou a internet.

Nosso patrimônio e nossa reputação estão em informações, por isso, a aprender a proteger as mesmas é uma questão de sobrevivência na Sociedade Digital. Sabemos o perigo de perder a chave de casa, e, portanto, mudamos a fechadura quando isso ocorre. Evitamos também emprestar a chave para outra pessoa, pois não sabemos o que ela pode fazer, isso é comum com o carro, por exemplo, já que se algo ocorrer de ruim o primeiro suspeito a vir a ser responsabilizado é o proprietário do veículo. O mesmo ocorre então com nossas senhas hoje em dia. Elas são as chaves das portas digitais, e responsabilizam seus proprietários-usuários. Emprestar a senha para alguém é o mesmo que assinar um cheque em branco.

O desafio da Segurança da Informação se passa por uma questão de falta de cultura sobre os riscos deste mundo cada vez mais real-virtual. Se alguém lhe abordar na rua, provavelmente você irá apressar o passo, mudar de lado da calçada, fechar a janela do automóvel, por reflexo, por cautela, melhor prevenir do que remediar. Mas se a abordagem ocorrer por email, através de um post no blog, uma mensagem em comunicador instantâneo, uma solicitação de convite para participar de uma comunidade, já ficamos com a guarda baixa. Por que?

Será que a magia da interface gráfica, o lado lúdico e misterioso da Internet, que tanto nos fascina, nos torna vítimas fáceis frente a ameaças cada vez mais graves disfarçadas de condutas e situações que beiram a inocência, que parecem inofensivas.

Como realmente conhecer alguém através da Internet? Como ter certeza que a informação é verdadeira. Passamos a confiar cegamente só porque está na web é verdadeiro? Será que aquela dose de “pé-atrás” não seria uma proteção necessária nesta época atual de maior violência, onde nos refugiamos atrás de máquinas, para nos sentirmos mais seguros e deixamos de ter cuidados mínimos de segurança?

O despertar para um uso sustentável das tecnologias, um uso consciente, seguro, ético, legal, deve ocorrer sem a necessidade de traumas. Não precisamos aprender pela dor, pelo incidente, pela tragédia. Todos nós estamos sujeitos sim a ter nosso computador contaminado por vírus, a receber um email falso, a ser

abordado por uma pessoa que não é quem diz ser na Internet, a acessar um site falso achando que está em um verdadeiro. Por que faz parte da vida. Mas podemos estar mais preparados, não apenas para nos protegermos disso, mas para agirmos rápido se ocorrer um problema, de modo a minimizar as conseqüências, os danos. Saber o que fazer, que prova guardar, a quem denunciar o fato é fundamental. Aprendemos a ligar para Polícia, para o Bombeiro, quando temos um incidente de mundo real, e para quem temos que ligar se o incidente é no mundo virtual?

Todos deveriam conhecer um pouco de primeiros socorros, para uma situação de ter que tomar medidas para salvar alguém que se engasgou, para aplicar uma assepsia em uma queimadura que acabou de ocorrer, estancar um sangramento, fazer uma respiração boca-a-boca, massagear o peito para evitar parada cardíaca. Nunca sabemos quando vamos precisar disso. Também precisamos conhecer os primeiros socorros para situações digitais. Por isso, segue uma tabela de dicas abaixo. Sejam usuários digitalmente corretos e preparados para usar todos os recursos que as tecnologias podem nos oferecer, sem riscos.

<b>Manual de Sobrevivência Digital</b>	
<p><b>- Evite passar senhas para terceiros (mesmo que da família ou conhecidos). Se o fizer, mudar em seguida. Sempre ao sinal de suspeita que alguém saiba a sua senha, a altere.</b></p>	<p><b>- Busque sempre estar com antivírus e antispymware atualizado, bem como faça uso de firewall e demais softwares de segurança, inclusive para criptografia das informações, para backup, há muitas opções boas e baratas e algumas também gratuitas. O importante é não ficar sem.</b></p>
<p><b>- Evite deixar o computador ligado e logado quando estiver ausente. Sempre faça bloqueio de tela ou se for se ausentar por longo período é recomendável desligar o equipamento e tirar da tomada.</b></p>	<p><b>- Busque usar apenas equipamentos que estejam com softwares de segurança atualizados, especialmente se for em local público, cybercafé, lanhouse, rede de hotel. Na dúvida pergunte para o responsável do serviço. Se possível, evite colocar sua senha de transações (bancária e cartão de crédito) nestes equipamentos. Ao encerrar a sessão, certifique-se que apagou tudo da máquina e fez log-out de todos os ambientes.</b></p>
<p><b>- Insira senha em celular, para bloqueio automático por inatividade. Também deve-se fazer backup da agenda, apagar periodicamente mensagens e emails do dispositivo (se possível 1 vez por semana) para evitar as suas informações pessoais e sigilosas caíam em mãos erradas.</b></p>	<p><b>- Evite fazer uso de fotos (imagens) de pessoas (especialmente crianças) que você não tenha autorização prévia, escrita para tanto. Na dúvida, se a pessoa vai gostar ou achar ruim, é melhor não usar. Principalmente se você tiver encontrado a mesma em um site de fotos/imagens cuja origem das mesmas é desconhecida.</b></p>
<p><b>- Evite carregar equipamentos tecnológicos que chamem a atenção quando estiver caminhando, andando de carro ou de Taxi, especialmente notebook, celular, MP3. Seja discreto e cuidadoso, se possível colocar na mala do carro e em uma mochila.</b></p>	<p><b>- Sempre leia tudo que lhe for apresentado para dar "click-ok" na Internet. Mesmo que você não possa mudar nada, deve-se sempre saber com o que se está concordando. Termos de Uso, Políticas de Privacidade, Avisos Legais de Direitos Autorais, Licenças, Garantias, Comprovante Compra-e-venda Online, tudo isso é</b></p>

	<b>documento, é prova legal. “Não assine sem ler, especialmente na Web”.</b>
<b>- Evite deixar seus pertences tecnológicos soltos, em cima da mesa de estudo, de trabalho, em uma cadeira no restaurante para se servir (especialmente quando é Buffet ou quilo, ou restaurante de hotel no horário de café da manhã que tem maior incidência de furtos). Fique de olho sempre.</b>	<b>- Seja cauteloso para quem você ira passar seus dados na Internet. Selecione bem, certifique-se. Lembre-se que na era da informação não existe almoço grátis. Todo serviço gratuito tem como preço a sua informação. Assim como ofertas mirabolantes podem significar um golpe de loja fantasma digital, bem como tenha cuidado com emails que possam ser falsos, não clique em tudo que recebe por email ou vê na internet. Na dúvida, acesse direto o site ou entre em contato pelo SAC Online.</b>
<b>- Evite ofender pessoas ou empresas na Internet. Use uma linguagem apropriada, que não seja agressiva, pois deve-se exercer a liberdade de expressão com responsabilidade. Aquele que abusa do direito, também comete ilícito e está sujeito a indenizar o outro lesado.</b>	<b>- Não faça justiça com o próprio mouse. Se algo de ruim lhe acontecer no uso de tecnologias, na internet, denuncie, busque ajuda de um especialista, comunique a autoridade. Preserve as provas digitais, evite mexer novamente na máquina. Se não for sua, peça ao proprietário que a reserve para coleta das provas.</b>

**A Dra. Patricia Peck Pinheiro**, advogada especialista em Direito Digital, sócia fundadora da Patricia Peck Pinheiro Advogados, autora do livro “Direito Digital” 3ª. Edição e co-autora do áudio livro “Direito Digital no dia-a-dia”, ambos publicados pela Editora Saraiva. ([www.pppadvogados.com.br](http://www.pppadvogados.com.br))