PRAGAS

Cuidado redobrado com dados pessoais

Com a aplicação de controles de segurança, é possível proteger dados privados e não ser vítima de hackers

Não é preciso ser uma celebridade para virar alvo de hackers.

Os famosos podem até sofrer com técnicas mais sofisticadas, como o recente caso envolvendo a atriz Carolina Dieckmann, mas, para pessoas comuns, boa parte dos problemas decorre da falta de cuidados.

Com a aplicação de controles de segurança, é possível proteger dados privados, segundo Rodolfo Avelino, professor do curso de Segurança da Informação da Universidade Cidade de São Paulo.

"Hoje, estamos nos adaptando à cultura do armazenamento de documentos e mídia no formato digital. Há uma década, fotos e documentos importantes eram guardados a sete chaves. Em muitos casos, fotos sensuais nem eram registradas por máquinas fotográficas, pois, de qualquer forma, elas teriam de passar por mãos de terceiros para serem reveladas", ressalta o profissional.

Para resguardar arquivos pessoais em computadores ou dispositivos móveis, é preciso contar com alguns recursos e prevenções. Uma das sugestões do especialista é manter os arquivos pessoais em aplicativos que criptografam dados de forma amigável.

Possuir e manter atualizado um bom antivírus é primordial. Além disso, procure não executar ou clicar em links recebidos por e-mail, com exceções em casos nos quais você tenha certeza de que a origem do e-mail e o destino do link são confiáveis.

E mais: não instale programas desconhecidos antes de fazer uma breve pesquisa sobre o mesmo.

Em caso de pendrives ou HDs externos, somente enquanto a informação estiver na memória do usuário ela estará segura, garante o professor.

"A partir do momento que a transferimos para um dispositivo ou a comentamos, mesmo que em sigilo para outra pessoa, esta segurança já estará comprometida", diz.

"Como o pendrive é um periférico fácil de perder, grave somente arquivos comuns e não sensíveis. Se for necessário manter uma informação importante, ela deverá ser transferida para o desktop o mais rápido possível e, logo após, ser apagada do pendrive. Já para o HD externo, é indicado adotar a mesma postura com um sistema de criptografia", orienta Rodolfo Avelino.

Os usuários também devem tomar cuidado ao acessar computadores compartilhados em locais públicos, como lan houses e até mesmo no trabalho.

FOTOS ÍNTIMAS da atriz Carolina Dieckmann vazaram na internet

OUTRAS DICAS

Previna-se mais

Serviços como Bluetooth só podem ser habilitados quando forem utilizados e a conexão à internet deve ser feita apenas em redes conhecidas. Procure também habilitar os recursos de senhas – a mais complexa possível – e instale apenas aplicativos confiáveis.

Proteção em dispositivos móveis

Sejam smartphones, notebooks ou tablets, os cuidados para proteger os dados em dispositivos móveis devem ser redobrados. Evite manter os arquivos nestes equipamentos, portanto, sempre que existirem dados íntimos armazenados, é necessário transferi-los para o computador de mesa (desktop) de sua residência e, logo após, apagá-los do aparelho móvel.

Ao se desfazer do equipamento

Nessa hora, destine corretamente o computador ou dispositivo que não será mais utilizado, principalmente, se ele já é considerado um resíduo eletrônico, pois o conteúdo do HD permanece armazenado no disco até mesmo quando é apagado por meio do sistema operacional.

Uso de computador compartilhado

No ambiente de trabalho, lan houses, entre outros lugares com possibilidade de uso público aos computadores, é preciso evitar o acesso ao Internet banking ou realizar compras on-line, pois dados de conta bancária ou números de cartão de crédito serão requisitados.

Redes sociais

São ferramentas cada vez mais utilizadas para se comunicar, porém, é preciso ter cautela ao inseri-las em seu dia a dia. A principal recomendação é não postar informações pessoais, como endereço, número de documentos e contatos. Evite ainda falar sobre sua rotina e aceitar pessoas desconhecidas em seu perfil.

Solução antirroubo

Uma solução de segurança confiável protege os dados contidos no equipamento contra pragas virtuais, além de permitir a localização do aparelho em caso de perda ou roubo. Soluções como essa permitem ainda que a empresa possa bloquear ou mesmo apagar totalmente os conteúdos armazenados no aparelho.

Cautela

Avalie bem quais são os dados de acesso solicitados por cada aplicativo Alguns aplicativos podem requerer acesso a seus dados ou informações pessoais. Seja cauteloso com o acesso que está fora do escopo ou da proposta do aplicativo. Por exemplo, um game não precisa ter acesso a SMS, chamadas realizadas, agenda de contatos e arquivos do sistema. Caso um aplicativo como este solicite esse tipo de informação, desconfie.

Sistema atualizado

Um sistema operacional atualizado permite que você aproveite ao máximo os recursos do equipamento ao mesmo tempo que protege sua informação. Evite falhas de segurança ou vulnerabilidades mantendo sempre atualizado o software em seu dispositivo móvel.

Prevenção de problemas

Os aparelhos tecnológicos são suscetíveis a inúmeros problemas, por isso, é importante realizar periodicamente uma cópia de segurança dos dados.

Nada de invasões

Para evitar uma possível invasão de hackers, deve-se manter o sistema atualizado por meio das correções fornecidas pelo fabricante, principalmente em sistemas Microsoft.

Golpe do débito pendente ataca de novo

Criminosos da rede lançaram na internet uma enorme quantidade de uma mensagem falsa usando o nome de Mercado Livre com o título Debito Pendente, informando no corpo do e-mail que se tratava de um "último aviso" sobre a compra de um aparelho celular, acusando a falta de pagamento.

A tentativa de ameaça dos hackers foi detectada pela equipe de suporte da Nodes Tecnologia.

FATURA

Os hackers pediam também para o usuário abrir um arquivo em PDF com a suposta fatura, com ameaça de levar o nome do "comprador" ao SPC/Serasa.

Eduardo Lopes, diretor comercial da Nodes, afirma que este tipo de falso e-mail com o tal PDF na verdade direciona à abertura de um arquivo executável contendo um cavalo de troia criado para coletar informações financeiras do usuário.

"Nunca se deve acreditar nesse tipo de mensagem e orientamos que o comprador entre em contato com a loja ou site onde fez a compra para verificar a veracidade do comunicado. Caso o e-mail possua algum telefone de contato, ele deve ser desconsiderado imediatamente", alerta o executivo.

O usuário também deve manter seus sistemas, programas de computador e software antivírus sempre atualizados.

COMPRAS NA WEB: cuidado