Garantindo Mais Segurança

A UBS Brasil CCTVM procura fornecer aos seus clientes produtos e serviços inovadores, e para isso, busca sempre os mais recentes desenvolvimentos tecnológicos para manter o nível de proteção em relação a dados e informações pessoais. Entretanto, a UBS Brasil CCTVM reconhece que a rede mundial de computadores é um ambiente de transmissão de dados eletrônicos que pode apresentar riscos aos usuários finais que dela se utilizam.

Ciente desses riscos, e buscando auxiliar nosso cliente, elencamos abaixo algumas recomendações de práticas e condutas que podem auxiliar na redução dos riscos do uso de recursos conectados à rede mundial de computadores.

1. Sempre mantenha seus softwares atualizados.
Nem sempre os códigos dos softwares estão isentos de falhas, e justamente por isso seus fornecedores disponibilizam periodicamente atualizações para corrigir eventuais bugs e falhas de funcionamento. Uma das maneiras mais eficazes de se proteger é manter os softwares que você utiliza sempre atualizados, principalmente seu sistema operacional e seu navegador de internet.

Em alguns softwares, essa atualização está programada para ser feita automaticamente – caso contrário, é possível habilitar essa opção nas configurações da maioria dos softwares. Existem ainda recursos próprios de segurança e privacidade nos sistemas operacionais e navegadores, que podem ser explorados e configurados em menus de "Opções", "Ferramentas" e similares, dependendo do programa utilizado.

2 .Tenha um pacote de segurança instalado em seu computador pessoal.
É muito importante manter seu computador seguro com a instalação e atualização de software de antivírus e com a habilitação de um programa de firewall, dentre outros programas que compõem um pacote de segurança, como softwares de backup, e antimalwares.

O software de antivírus ajuda a rastrear vírus que podem roubar informações, portanto recomendamos realizar periodicamente sua atualização e uma varredura em seu computador, e se algum arquivo estiver infectado, o ideal é apagá-lo. O firewall, por sua vez, bloqueia a comunicação e o acesso de fontes externas não autorizadas pelo usuário do computador, protegendo seus dados de possíveis hackers.

3. Crie e utilize senhas de maneira segura.
Além das recomendações básicas de segurança (não informar sua senha a terceiros e não utilizar senhas "fáceis" como datas de aniversário e números de telefone), sugerimos que as senhas criadas sejam razoavelmente longas (recomenda-se que tenha no mínimo 8 caracteres) e contenha letras, números e símbolos intercalados. Não se esqueça de alterar sua senha periodicamente, e tome o cuidado de não anotá-la em papéis ou arquivos que possam estar expostos a falhas de segurança. Além disso, sempre atente às páginas que possuem a opção de armazenar informações digitadas, e se não estiver em uma conexão segura, evite acessar sua conta na corretora.

4. Tenha cuidado com links e anexos suspeitos em seu e-mail e seja cauteloso ao instalar softwares e aplicativos.
É muito comum o envio de spams por e-mail, contendo anexos, links ou imagens que, quando o usuário clica ou os abre, podem instalar softwares ocultos. Por isso, recomendamos que não abra anexos ou clique em links a não ser que você saiba identificar seu conteúdo, mesmo que seja proveniente de remetentes conhecidos, porque eles podem ter sido infectados.

Mensagens de spam são mensagens maliciosas disfarçadas muitas vezes de ofertas, correntes, fotos e notícias que despertam a curiosidade do usuário, e podem roubar dados particulares. Recomendamos todo cuidado com anexos que

contenham arquivos e extensões desconhecidas ou estranhas. Outras maneiras comuns de fraude são sites falsos, inclusive de redes sociais, que podem roubar informações e senhas, deixando o usuário vulnerável. São abordagens comuns: envio de cobranças de serviços não solicitados e comunicações do SPC e Serasa, cartões virtuais, promoções duvidosas, comunicados falsos de órgãos públicos, links falsos de bancos, entre outros.

Métodos mais elaborados de roubo de dados também circulam pela rede. Dentre eles, é importante mencionar o phishing, golpe muito comum para roubo de informações financeiras. Para evita-lo, jamais responda e-mails que você julgue suspeitos, e tenha em mente que instituições financeiras não solicitam informações como senhas e dados pessoais por e-mail. Caso surjam dúvidas sobre a solicitação ou o seu teor, confirme os dados do solicitante antes de prosseguir com o envio.

Vírus e programas maliciosos também podem estar escondidos em softwares e aplicativos aparentemente inofensivos. Portanto, apenas faça o download de softwares gratuitos em sites confiáveis, e não instale softwares sem saber exatamente do que ele se trata. Programas de compartilhamento de arquivos ou barras de ferramentas personalizadas podem trazer outros softwares inclusos, podendo ser malwares.

5. Precauções para descartar seu computador.
Com tantas novidades tecnológicas, é normal que as pessoas busquem o que há de mais moderno no mercado. No entanto, o descarte de um computador não pode ser feito sem que seu disco rígido seja completamente apagado, porque ele contém inúmeros dados, inclusive senhas, números de contas, chaves de licença, endereços e números de telefones, entre outros, e pode se tornar um alvo para ladrões de informação e dados pessoais.

Seja qual for a maneira de descarte (reciclagem, revenda ou doação são as opções mais sustentáveis), não se esqueça de utilizar um software para limpar seu disco rígido.