DICAS DE SEGURANÇA DA INTERNET

Atualizado: 21/03/2022

01) Atualize sempre o seu Sistema Operacional
Qualquer que seja o sistema operacional que usar, seja ele Windows (o mais usado no mundo e o que mais sofre ataques de vírus), Linux, Ubuntu, Macintosh, Android (em caso de celular), etc., tenha sempre a versão mais atualizada do software que é menos suscetível a invasões.

02) Atualize seus programas instalados
Pacote Office (Word, Excel, PowerPoint...), Navegadores (Google Chrome, Microsoft Edge/IE, Mozilla Firefox, Vivaldi, Opera, Safari...), Multimídias (Windows Media Player, Nero...), Complementares (Java, K-Lite Codec...), softwares de bancos, antivírus, etc., precisam ser atualizados constantemente.

03) Utilize mais de um navegador para realizar suas tarefas
Isso ajuda a confundir um pouco os softwares maliciosos, mas os mesmos precisam sempre estar atualizados e você precisa ficar atento aos alertas dos mesmos, sobre páginas maliciosas; evite também memorizar senhas nos navegadores; e mantenha o hábito de sempre digitar seus e-mails e senhas, pois pode ser um pouco cansativo, mas é para sua própria segurança.

04) Crie senhas difíceis para suas contas de internet
Senhas que contenham parte do nome pessoal/usuário, datas de nascimento ou de outros acontecimentos, detalhes da própria vida/rotina, são as mais vulneráveis. Senhas eficazes contém letras maiúsculas e minúsculas, números não sequenciais e caracteres especiais, como # * & ! $, etc.

05) Tenha sempre certeza que saiu das contas de internet, após usá-las (login/logout)
Muitas pessoas acessam redes sociais e sites, principalmente, os e-commerces, em diferentes plataformas (desktops, celulares, tablets...), em diversas redes wifi públicas (Ex: Lan houses). E muitas vezes, encerram as atividades fechando apenas os navegadores e não saem das contas (login/logout) de forma correta. Isso é um perigo! Tendo em vista que muitos usam senha única pra tudo, inclusive para contas bancárias, facilitando a vida dos golpistas que podem ter acesso ao mesmo aparelho da vítima.

06) Tenha cuidado ao baixar arquivos para os seus aparelhos
Baixe apenas arquivos de sites confiáveis e tenha bastante cuidado, principalmente, com sites de downloads de filmes, músicas e softwares. Os sites mais confiáveis para downloads são aqueles que existem também no modo físico, como sites de emissoras de TV, lojas renomadas de multimídia, instituições governamentais e ongs, empresas de tecnologia, profissionais liberais autenticados, etc., porque investem muito em segurança e você poderá reclamar por algo pessoalmente. E mesmo assim, todo cuidado é pouco!

07) Tenha muito cuidado com os e-mails que recebe
Muitas vezes, recebemos e-mails de promoções, sorteios, prêmios, serviços, produtos, pessoais, laborais, românticos, causas sociais, institucionais, parentes, emocionais, etc., que podem nos chamar a atenção e nos induzir a clicar nos links na descrição e/ou baixar seus anexos. Mas é preciso atentar-se ao cabeçalho dos mesmos e ver se os endereços de e-mails são das respectivas pessoas/empresas que enviaram e se você solicitou aquilo que está no e-mail.

08) Suspeite de todos os sites e movimentações estranhas
Memorize e guarde bem os endereços de sites que você considera confiáveis. Não aceite indicações de sites, para realizar tarefas importantes sem ao menos investiga-lo. Peça ajuda sempre a pessoas com grande domínio naquelas atividades ou de profissionais de informática. Ao suspeitar de um endereço de site que está diferente do habitual, cancele o que iria fazer e comunique a alguém que entenda mais que você ou até mesmo – em caso de percepção de fraude – vá à delegacia mais próxima de sua casa e preste queixa de provável crime cibernético.

09) Cuidado ao realizar cadastros em sites
Só realize cadastros em sites de pessoas/empresas que sejam extremamente confiáveis e verificados, principalmente, quando estes exigem para sua conclusão dados, como CPF e RG. NORMALMENTE, OS SITES MAIS CONFIÁVEIS PARA PREENCHIMENTO DE FORMULÁRIOS SÃO OS QUE TEM O ÍCONE DO CADEADO NA BARRA DE PESQUISA DO NAVEGADOR. Guarde bem os dados de acesso, se for de alguma conta que criou, tente acessar a mesma página com dados errados. Pois, se o cadastro ou login der continuidade, significa que o site é FALSO e você precisa agir logo, denunciando o golpe e protegendo seus documentos utilizados.

10) Cuidado com informações que fornece na internet
Muitas vezes, as pessoas se excedem em redes sociais e websites, falando detalhes de sua vida, rotina e atividades profissionais, etc., que podem dar pistas aos criminosos a aplicarem golpes. Essas dicas, podem ser locais de referência, nomes de parentes e animais de estimação, problemas familiares, etc. Sempre revise o que irá publicar na internet e sempre tenha cautela para não se arrepender depois!

11) Mude as senhas das suas contas de internet constantemente
Isso é muito importante! Pois dificulta a ação de softwares maliciosos e cria uma rotina de segurança. Lembre-se dos detalhes que explicamos, de como criar senhas difíceis e não confie os dados de acesso às suas contas a pessoas estranhas. Você pode criar uma rotina de segurança para as suas senhas, da seguinte forma: + Mudar a senha a cada 3, 6, 9 ou 12 meses; + Se sua senha está anotada dentro do computador, ora escreva fora, num papel; + Não identifique claramente seus dados como "usuário" e "senha"...

12) Tenha muito cuidado com as publicidades

Não seja bobo! Ninguém dá nada a ninguém de graça, principalmente, pela internet! Muitas vezes, você irá acessar sites que aparecem publicidades a torto e a direita, em vários formatos (texto, áudio, vídeo, imagem, etc.) com apelos do tipo: "Você é o usuário de nº 10.000.000! Clique aqui e receba seu prêmio!". Clique apenas em publicidades expostas em sites confiáveis e, mesmo assim, confira se vale a pena e se o link leva para o respectivo site que ele anuncia. Para ver o link, basta apenas colocar a seta do mouse em cima da respectiva publicidade. Um endereço eletrônico aparecerá e basta conferir se procede com a descrição.

13) Utilize um bom antivírus em seu aparelho

Antivírus apenas faz uma breve triagem de softwares e arquivos maliciosos, e elimina diversos tipos de vírus (não todos!), mesmo assim, precisamos ter um bom instalado em nosso aparelho. Karspersky, Avast e Norton estão entre os melhores do mercado.

14) Cuidado com os popups que aparecem em sites de transmissão de filmes, shows e futebol

Falamos há pouco sobre as publicidades que podem ser maliciosas e os pop-ups, que são aquelas telas, páginas ou arquivos que surgem, devido a alguma ação que tomamos ou espontaneamente, com diversos tipos de conteúdo, e mesmo quando estes se apresentam de sites que consideramos confiáveis, o próprio recurso do pop-up pode esconder vírus ou prejudicar as tarefas do computador. Mantenha os pop-ups sempre bloqueados em seu computador. Os navegadores de internet possuem recursos para bloqueios de pop-ups. Verifique em "Configurações" e procure pelo termo "Pop-up" para desativar ou bloquear este recurso.

15) Cuidado ao acessar redes wifi públicas

Já comentamos aqui sobre os perigos de se acessar redes com wifi públicas. Muitos criminosos são especializados nestes tipos de redes, pois as pessoas facilitam bastante a ação dos mesmos. Tipo assim: as pessoas acessam rede wifi em bares, restaurantes, eventos, shows, etc., sem se importarem e colocam seus dados de contas importantes, como as de bancos. Neste caso, quando estiver nas situações descritas acima, use os dados móveis e mesmo assim, fique atento a situações que fujam da rotina.

16) Faça cursos de informática ou procure informações com um profissional da área

A economia, avanços da tecnologia, as facilidades de compras e o aumento do poder aquisitivo das pessoas, têm facilitado a vida das mesmas em adquirir aparelhos eletrônicos cada vez mais sofisticados. No entanto, poucas pessoas costumam buscar informações de usabilidade e segurança da internet. Exemplo: as pessoas compram um computador, mas não se informam o mínimo possível para poder manuseá-lo. Por isso, é importante buscar ajuda profissional ou com alguém que possa passar o mínimo de instrução possível e evitar problemas futuros.

OBSERVAÇÕES IMPORTANTES

– As informações acima NÃO substituem a atuação e perícia de um dos nossos técnicos, servem apenas de paliativo, ou seja, procedimento provisório. Assim que possível, agende junto à Central da ITAFIBER, data e horário, para visita de nossa equipe. Ligue GRATUITAMENTE para o número 0800 095 1608 e solicite o Atendimento;

– Algumas informações acima só podem ser utilizadas por pessoa com prévio conhecimento intermediário em informática, para ação rápida sem ter que esperar por Suporte Técnico. Pois, no mundo digital, muitas vezes, ações simples conseguem sanar problemas com facilidade. No entanto, alertamos que a responsabilidade é inteiramente da pessoa que procedeu. A ITAFIBER NÃO SE RESPONSABILIZA POR DANOS MATERIAIS OU FÍSICOS causados pelo próprio Cliente/Usuário. Na dúvida, não insista e solicite o Suporte Técnico urgente, através do telefone GRATUITO: 0800 095 1608