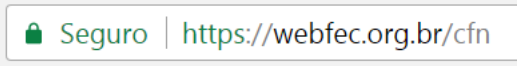
Segurança no uso da Internet

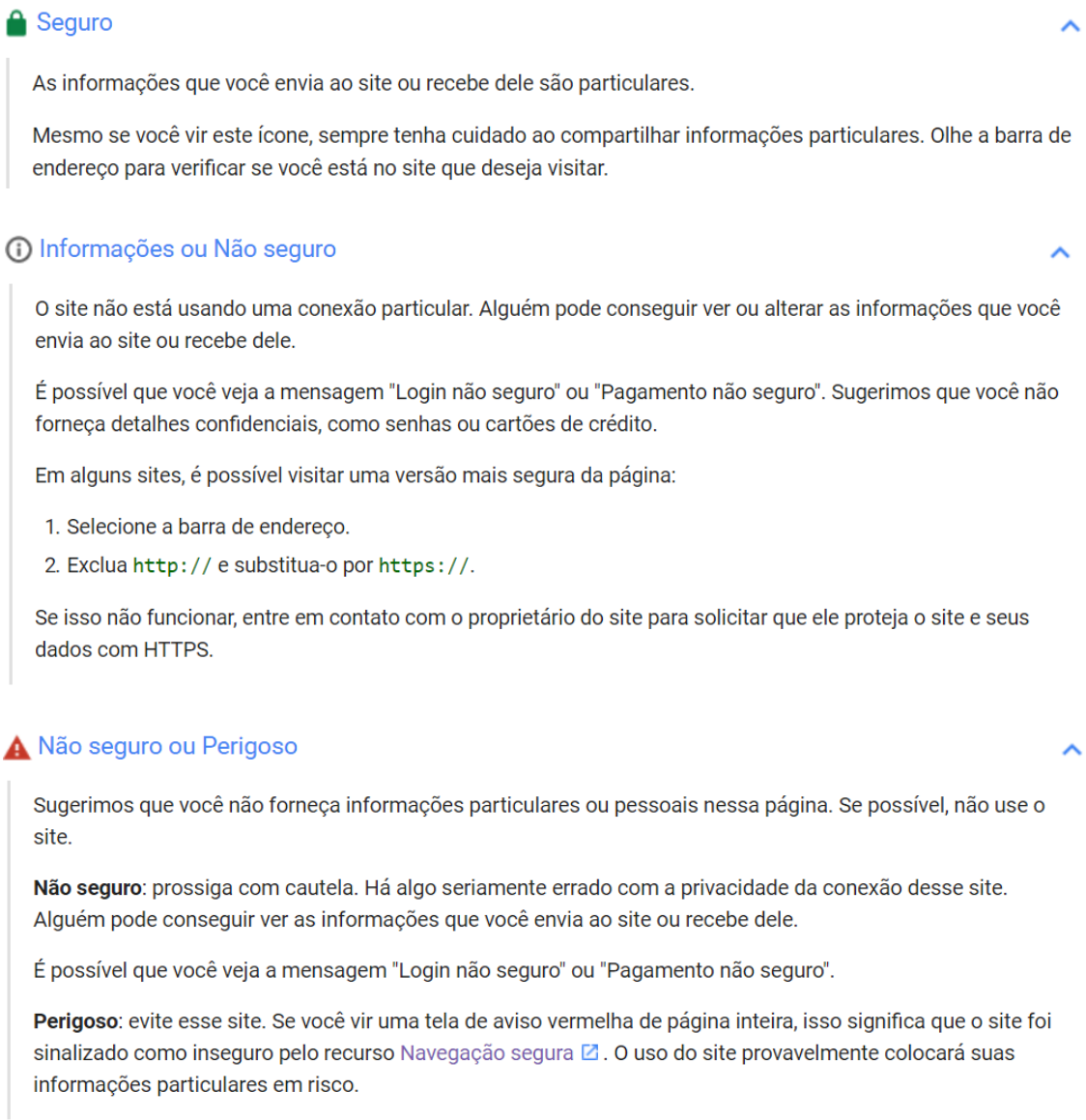
Descrevemos abaixo algumas dicas de como você poderá fazer uma navegação segura na Internet. Fique atento para tornar a internet um lugar mais seguro:

1 - Visite sites seguros

Verifique se o site que está acessando é seguro. Preste atenção no endereço do site que aparece no seu navegador. “Https” indica que você está navegando em um ambiente seguro.



Ao lado direito do endereço o navegador (Chrome) poderá apresentar as seguintes opções:



2 - Crie senhas fortes

Se você é do tipo de pessoa apegada à sua senha e usa os mesmos números e palavras há anos, você é um sério candidato a ter os dados roubados por cibercriminosos, ou seja, ladrões da internet especialistas em furtar contas de e-mails, cadastros em lojas virtuais, logins de redes sociais, entre outros serviços disponíveis na grande rede mundial de computadores.

A cada dia, milhares de usuários da web enfrentam o drama de terem suas contas invadidas, e não importa o local, idade ou tipo de computador, todos estão vulneráveis ao desprazer de ter a privacidade violada.

De acordo com os dados publicados pela campanha do Dia Mundial da Senha, 90% das pessoas que usam a internet possuem senhas fáceis de serem desvendadas. As mais comuns, e também preferidas dos ladrões na rede, são: *123456*, *senha*, *deus*, *ninja*, ou combinações como nomes ou sobrenomes e até mesmo datas de aniversário e números de documentos de identificação.
Utilize sempre letras, números e caracteres especiais como @, # ou *.

Proteger sua privacidade com senhas fortes e seguras é bem mais simples do que parece.

- Escolha uma senha longa (não precisa ser muito complicada). Quanto maior a senha, maior a dificuldade para ser decodificada.
- Não reutilize as mesmas combinações para contas diferentes.
- Misture números, letras e caracteres. Por exemplo: **S3gur4nç@, !nt3rn&t**
- Nunca envie uma senha por e-mail. Não forneça a sua senha para outras pessoas.
- Troque a senha com frequência. Alguns serviços já alertam os usuários e pedem para que se troque a senha regularmente. O ideal é uma senha a cada 3 meses.

3 - Use antivírus

Invista em um programa de segurança para seu computador ou dispositivo móvel. É importante também mantê-lo sempre atualizado. Dessa maneira, você estará protegido contra vírus e outros tipos de ameaças.

As ameaças estão por todo lado na internet, isto não há como negar. Porém, ter um bom antivírus pode te proteger bastante, também é essencial que ele esteja atualizado para te proteger de novos arquivos maliciosos que são lançados todos os dias na grande rede. Estes vírus, na melhor das hipóteses, ficam incomodando seu computador. Outros, outrora, podem roubar dados, acessar conteúdos sigilosos e muito mais.

Se seu computador for infectado por algum vírus, você pode perder arquivos e ter que, talvez, formatar seu computador. O ideal mesmo é manter o antivírus habilitado para que a execução de programas maliciosos seja bloqueada. Uma grande parte dos vírus é obtida através da internet, por isso é importante que ele esteja atualizado.

4 - Cuide bem dos seus dados pessoais

Nada de se expor demais nas redes sociais, nem compartilhar por e-mail número de documentos ou informações confidenciais.

Só utilize equipamento efetivamente confiável. Não realize operações em equipamentos públicos ou que não tenham programas antivírus atualizados nem em equipamento que não conheça. Existem programas denominados (Cavalos de Tróia) utilizados por fraudadores para capturar as informações do cliente quando digitadas no computador;

Não execute aplicações nem abra arquivos de origem desconhecida. Eles podem conter vírus e outras aplicações prejudiciais, que ficam ocultas para o usuário e permitem a ação de fraudadores sobre sua conta, a partir de informações capturadas após a digitação no teclado;

5 - Cuidado com o comércio eletrônico e internet banking

Ofertas muito arrasadoras podem ser indício de fraude. No Brasil, crimes virtuais que utilizam o **phishing** – o uso de sites e e-mails falsos para atrair vítimas e roubar informações – é bastante comum.

Faça compras em sites que tenha uma boa reputação. Fique atento também ao endereço do site. Fraudadores podem fabricar sites bastante parecidos com os mais famosos para atrair internautas desatentos.

É necessário tomar alguns cuidados com a loja em que se vai efetuar a compra, é muito importante fazer compras somente em lojas com boa reputação. Caso você esteja interessado em algum produto de uma loja desconhecida, pesquise bem sobre o site. Pesquise e veja se existem reclamações contra a empresa na internet. Um bom site para pesquisar é o **Reclame Aqui**.

Quando acessar sua conta bancária pela internet (também conhecida como *Internet Banking*), tenha bastante cuidado. Evite ao máximo possível acessar sua conta através de um computador público, sempre verifique se a URL (endereço do site) realmente pertence ao site do banco e por último, mas não menos importante, siga à risca todas as normas de segurança recomendadas pelo banco.

4 - Sempre use o botão “sair” ou “logoff”

Sempre que acessar sua conta em qualquer site, seja no e-mail, Facebook ou aqui mesmo no Oficina da Net, clique no botão ou link de nome Logout, Logoff, Sair ou Desconectar (ou qualquer outro botão/link que faça sair da sua conta).
Muita gente realiza este procedimento, simplesmente fechando a janela do navegador ou mesmo acessando outro site. Não é nem um pouco recomendado agira assim. O site que você acessou sua conta, não recebeu nenhuma informação necessária para encerrar seu acesso. Tome cuidado com isso, pois ao voltar a acessar o site, você estará logado.

Esta dica é muito importante para quem usa computadores públicos (o computador da faculdade ou de uma lan house, por exemplo). A próxima pessoa que for utilizar o mesmo equipamento terá acesso aos seus dados.

7 – Fraudes acontecem. Previna-se!

Phishing, pharming, identidade falsa, cavalos de troia, tudo isso são ameaças bastante comuns usadas por criminosos virtuais para roubar as vítimas na internet. Conhecer as práticas e saber como se proteger é essencial.

Cuidado com e-mails não solicitados ou de procedência desconhecida, especialmente se tiverem arquivos anexados. Correspondências eletrônicas também podem trazer programas desconhecidos que oferecem diversos tipos de riscos à segurança do usuário. É mais seguro apagar os e-mails não solicitados e que você não tenha absoluta certeza que procedem de fonte confiável.

Tome cuidado especialmente com arquivos e endereços obtidos em salas de bate-papo (chats). Alguns desses chats são frequentados por hackers;
Evite sites arriscados e só faça downloads (transferência de arquivos para o seu computador) de sites que conheça e saiba que são confiáveis.
Utilize sempre as versões de browsers (programas de navegação) mais atualizadas, pois geralmente incorporam melhores mecanismos de segurança.

Se você costuma receber e-mails dizendo que ganhou algum prêmio, ou que seus documentos estão em situação irregular na empresa telefônica, fique sabendo que você, pode estar recebendo e-mails com a finalidade de um golpe. É bem provável que estes e-mails sejam *scam*, ou seja, um e-mail falso com a finalidade de roubar seus dados pessoais. Se a mensagem tiver erros de português, ofertas tentadoras ou links estranhos (passe o mouse em cima do link para ver o endereço, mas cuidado, não clique nele) desconfie imediatamente. Na dúvida, entre em contato com a empresa, pessoa ou entidade que está no e-mail.

8 - Saiba mais sobre este assunto

Se você deseja saber mais sobre as questões acima, acesse a "**Cartilha de Segurança para Internet" do Comitê Gestor da Internet no Brasil**
https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

Fontes:
http://www.mundopositivo.com.br/noticias/segurancadigital
https://www.oficinadanet.com.br/artigo/1853/seguranca_no_uso_da_internet
https://cartilha.cert.br