

1. Segurança

Por meio da internet podemos ter acesso a muitas informações e diferentes formas de comunicação e entretenimento, mas é preciso que tenhamos certos cuidados, principalmente no que diz respeito à segurança.



Figura - Segurança

Segurança é uma palavra que está sempre presente em nosso cotidiano e quando falada pode fazer referência a um estado de proteção no qual podemos evitar incertezas e nos preservar de perigos ou danos futuros.

Segurança da informação refere-se ao processo de proteger a informação de ameaças externas e internas reduzindo riscos, fraudes, erros e danos. Na segurança da informação os quatro princípios centrais são: confidencialidade, autenticidade, integridade e disponibilidade.



Figura - Segurança da Informação

Neste capítulo abordaremos os conceitos básicos de segurança, como navegar de forma segura na internet e os cuidados que devemos tomar.

2. Conceitos Básicos

Quando falamos em segurança da informação alguns termos tornam-se cada vez mais comuns. Abaixo será descrito os conceitos básicos e principais que dizem respeito a segurança.

- **Vulnerabilidade:** refere-se a uma ou mais fragilidades ou falhas que podem servir de entrada para ameaças.
- **Risco:** evento ou situação que quando ocorre pode gerar perdas e causar impactos.
- **Ameaça:** refere-se a tudo que pode comprometer a segurança de um sistema. Pode ser intencional, acidental ou natural.
- **Ataque:** refere-se a ação de tentar destruir, alterar, roubar ou obter acesso não autorizado de modo a comprometer a segurança da informação.
- **Senha:** método utilizado para autenticar o usuário, ou seja, garantir que é o usuário legítimo.
- **Criptografia:** meio que permite escrever mensagens em código, ou seja, transformar um texto simples em um formato que seja difícil de decifrar.
- **Vírus:** programa ou parte de um programa de computador, normalmente malicioso, que infecta o sistema e realiza cópias de si mesmo dificultando a ação do antivírus. O vírus se propaga quando o arquivo ao qual ele foi anexado é aberto.
- **Spam:** refere-se aos e-mails não solicitados, que geralmente são enviados a diversas pessoas.
- **Cavalo de Tróia:** programa que parece inofensivo que executa as funções que foram projetadas, mas também executa funções maliciosas e sem o conhecimento do usuário. Abre portas de acesso em seu computador para que outros códigos maliciosos possam ser instalados.
- **Hacker:** Profissional que busca falha em sistemas para torná-los mais seguros.
- **Cracker:** Pessoa que invade para tirar proveito e assim ganhar dinheiro.
- **Firewall:** pode ser definido como uma barreira de proteção que controla o tráfego de dados entre seu computador e a internet e protege o computador de acessos não autorizados.
- **Backup:** cópia dos dados de um dispositivo para outro de forma a protegê-los e recuperá-los depois.
- **Antivírus:** ferramentas que detectam vírus e outros códigos maliciosos em seu computador.

3. Navegação Segura

A internet é um ambiente dinâmico e sem fronteiras, que disponibiliza um verdadeiro universo de informações e possibilidades de comunicação democrática. Mas, assim como o “mundo real”, a internet não está livre de riscos.

Dessa forma, é necessário entender a dimensão pública desse espaço, acompanhar e orientar a utilização da internet pelas crianças, adolescentes e até mesmo os adultos, prevenindo a incidência de violações de direitos humanos e crimes.



Figura - Acesso Seguro

Com o aumento significativo nos últimos tempos de usuários, todos nós precisamos estar atentos e ter alguns cuidados. Filtros e outros softwares de segurança podem ajudar.

NOTA: O acompanhamento presencial e o diálogo são as formas mais eficazes e, portanto, indispensáveis de proteção.

Na internet é preciso ter cuidados com golpe, espionagem e roubo de arquivos e senhas que são apenas alguns dos problemas que as pessoas podem enfrentar nesse tão vasto submundo da Web.

3.1. Acesso seguro ao Internet Banking

Para acessar o Internet Banking de um determinado banco, devemos primeiramente verificar se a página é a verdadeira. Neste exemplo utilizaremos a página do Banco do Brasil. Depois, deve-se preencher com a agência e conta.



Figura - Site do Banco do Brasil

ATENÇÃO: Sempre verificar se tem o cadeado.

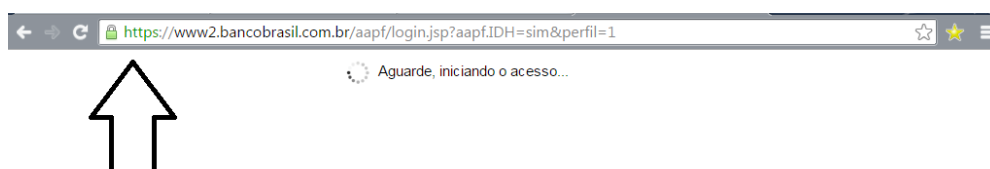


Figura - Acessando o painel pessoal no Banco do Brasil.

Depois de preencher todos os dados referentes à conta, agora só navegar pelo painel pessoal no banco do Brasil.

[Nota: Esse processo é semelhante nos outros bancos.](#)

4. Pirataria

Frequentemente nos deparamos com produtos pirateados. Na rua principalmente, locais de livre comércio e feiras livres que são especializados nesses tipos produtos. Por ser financeiramente bem melhor para o bolso do consumidor, muitos aderem a prática de comprar apenas produtos pirateados. Porém, o que poucos sabem, é que esse tipo de comércio prejudica na arrecadação de impostos e também fere o comércio de produtos legalizados, já que eles acabam perdendo na concorrência. Além de tudo, produtos piratas não oferecem garantias contra defeitos, bem como possíveis danos aos consumidores.

4.1. Direitos Autorais

Refere-se ao direito do autor sobre a sua obra intelectual, ela pode ser literária, artística ou científica. Exemplos de obras intelectuais: Textos, livros, pinturas, esculturas, músicas, fotografias e dentre outros.

Os direitos morais asseguram que o autor criou determinada obra, ou seja, certifica que a obra é de sua autoria. Os direitos patrimoniais referem sobre o uso econômico da obra. Uma obra intelectual não precisa estar registrada para ter os seus direitos garantidos. O registro serve como prova de autoria e demonstra quem primeiro declarou a obra publicamente.

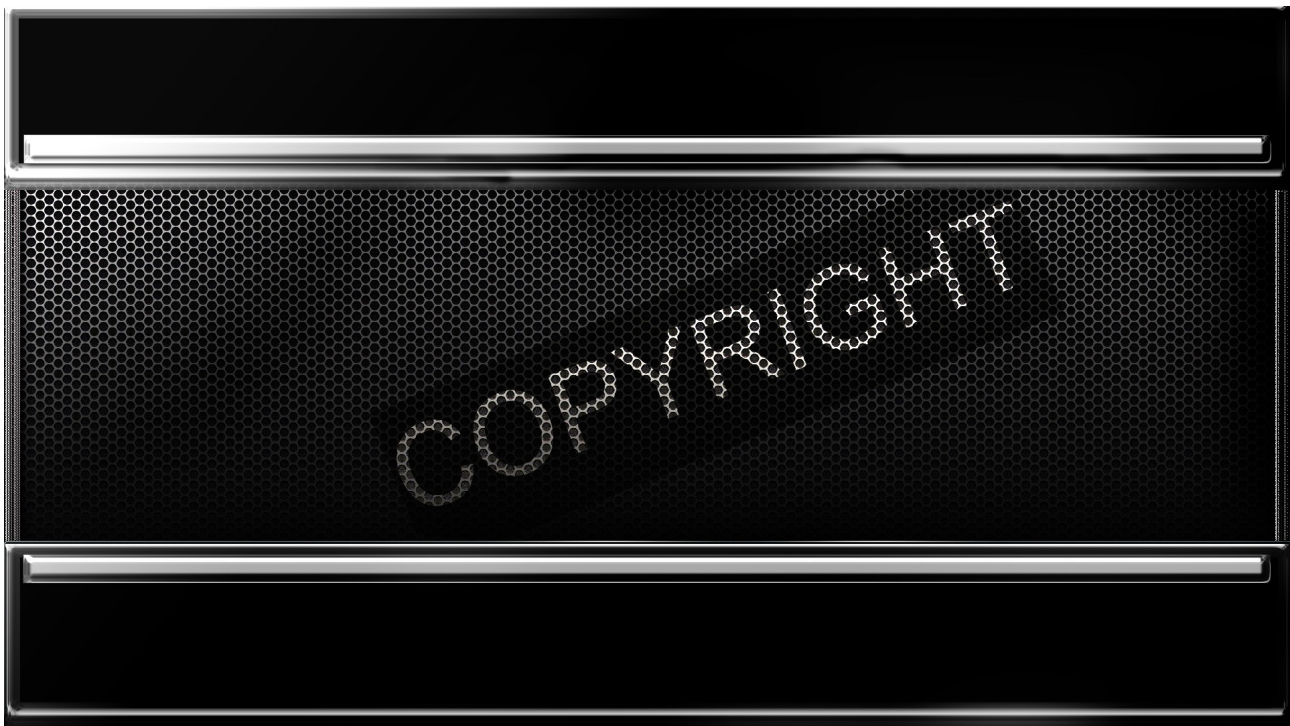


Figura - Direitos Autorais

4.2. Plágio

Refere-se ao ato de apresentar ou assinar uma obra intelectual quem contém parte de uma obra que pertença à outra pessoa e sem definir o devido crédito ao autor da obra. No plágio, a pessoa assume autoria da obra.

4.3. Pirataria de Software

Segundo a **Lei nº 9609/98 de 20 de fevereiro de 1998** que “Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.”.

Quando é adquirida uma licença, não é permitido ao usuário realizar cópias indevidas, por isso que incentivamos o uso do Software livre que nesse âmbito dá ao usuário o poder de distribuir o software.

Quando o usuário decide usar uma cópia pirata de um Software proprietário, ele perde o direito de usar o suporte do Software, à sua documentação, como exemplo o manual, e às atualizações liberadas pelo fornecedor do software. E em muitos casos, o software pode conter vírus com grande potencial de danificar o computador do usuário.

Nota: Em caso de dúvida, rever o capítulo 1 que fala sobre Software livre e Software proprietário.

ATENÇÃO: Toda forma de pirataria é crime, então todo cuidado é pouco.



Figura - Pirataria de Software

5. Dicas Básicas de Segurança

- Usar ferramentas de segurança: para manter a segurança digital, devemos utilizar alguns artifícios que nos mantém mais seguros na internet. Primeiramente, devemos ter um Firewall, instalado e atualizado, também é importante possuir um bom antivírus, atualizado.



Figura - Antivírus e Firewall

- Essa Página é a oficial? certificar-se se a página que está acessando é a verdadeira, pois tem um golpe chamado “Phishing” que se passa pela original. Para saber se está acessando a página verdadeira, é sempre bom conferir o nome do site na barra de navegação.



Figura - Página Oficial BB

- Senha forte: sempre que tiver que criar senha, sempre tenha em mente que a cada dia as técnicas que quebram senhas estão melhorando, neste caso, deve-se sempre criar senhas fortes que contenha letras, maiúsculas e minúsculas, números, e caracteres especiais. Periodicamente, deve-se trocá-la!

Exemplo de uma senha forte: wS*KbN]e)D\5KgE

No site <http://testedesenha.com.br/>, podemos verificar a força da senha.

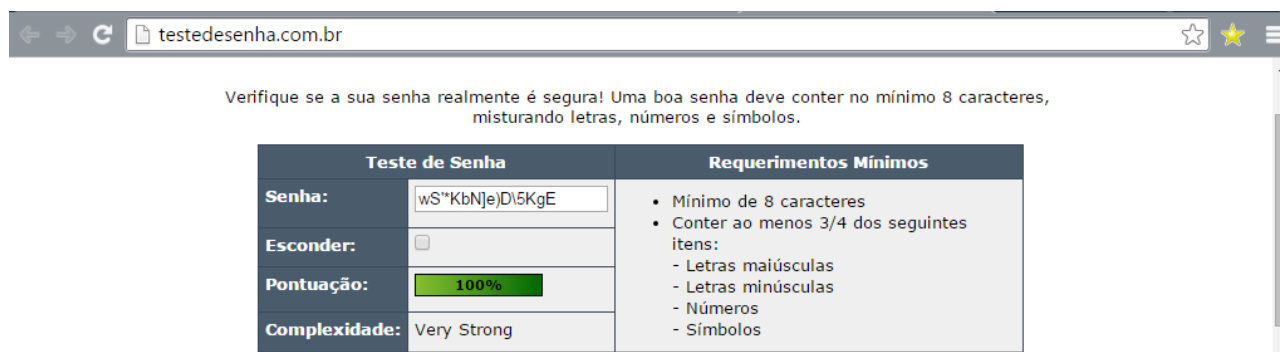


Figura - Teste de Senha

- Escanear o computador: caso utilize o Windows, deve-se realizar um escaneamento no computador para verificar se não há vírus instaurado.
- Cuidado com Download: muito cuidado ao realizar downloads, muitos serviços de downloads, quando são baixados vêm com algumas coisas que não são agradáveis. Deve-se sempre baixar de sites confiáveis.
- Cuidado com cadastros: jamais fornecer dados restritos em cadastros. Exemplo: Conta bancária, documentos pessoais e dentre outros. Certifique a autenticidade do site, verificar se o site é confiável.

- **SPAM:** *jamais clique em e-mails suspeitos mandando baixar algo ou pedindo para inserir informações. Um banco nunca manda um e-mail pedindo para alterar/atualizar informações. A figura abaixo é um exemplo de um SPAM.*

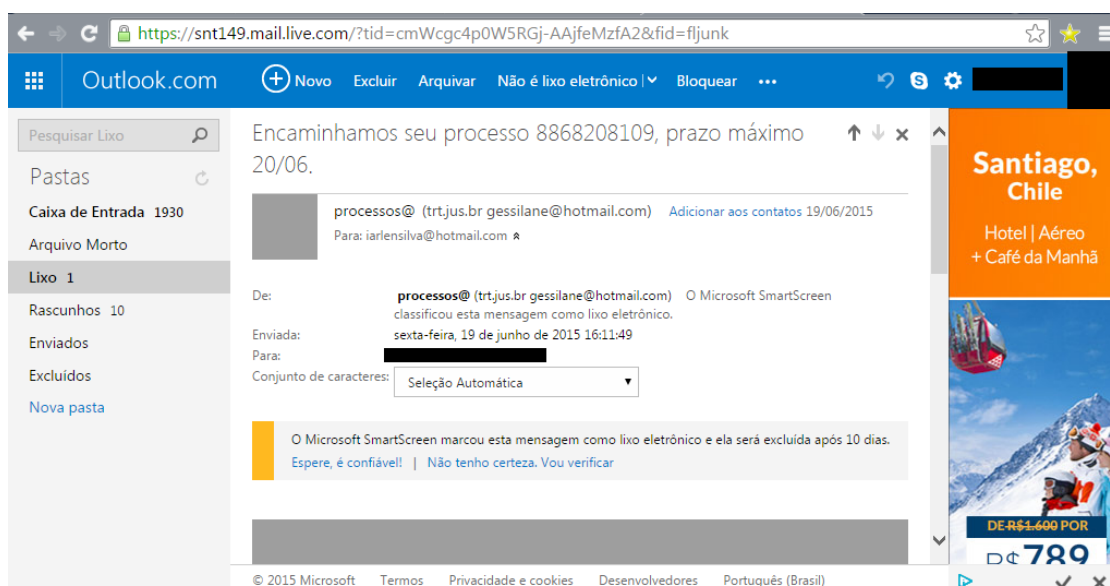


Figura - SPAM

- **Propagandas:** *nunca clique em link suspeito, ou propaganda dizendo que caso clicar ganha R\$ 1.000.000,00(um milhão de reais).*



Figura - Propaganda



Figura - Propaganda

- Redes sociais: muito cuidado ao se expor muito nas redes sociais. Muitas vezes, pode ser alvo de coisas indesejadas. Por isso, muito cuidado.



Figura - Redes Sociais

- Computador de terceiros: ao acessar o computador de terceiros, deve-se verificar se saiu de todas as suas contas.