

Acesso à Rede Mundial de Computador



A história da internet – Os primeiros passos da rede mundial

A história da internet pode surpreender muita gente. Foi um longo caminho até chegarmos aqui. Hoje é muito fácil criar um site ou um blog. Mas muita gente trabalhou duro para chegarmos a essa facilidade de hoje em dia. Como já diria Isaac Newton, só conseguimos ver mais longe porque “nos erguemos nos ombros de gigantes”.

A internet também é conhecida como World Wide Web, aquele “www” que vai antes do endereço do seu registro de domínio. Em bom português, rede mundial de computadores. Então, para falarmos da história da internet, precisamos voltar ao passado e relembrar como foram criados os primeiros computadores eletrônicos.

A previsão

Em 1964, o canadense Marshall McLuhan já previa em seus artigos que de alguma maneira a sociedade estava evoluindo para uma forma de grande comunidade global. Ele foi a primeira pessoa a colocar esse conceito no papel e falar sobre as suas consequências. McLuhan dizia que um sistema nervoso eletrônico, a mídia, estava integrando o planeta. Acontecimentos do outro lado do mundo podiam ser entendidos como se estivéssemos vivendo em um vilarejo.

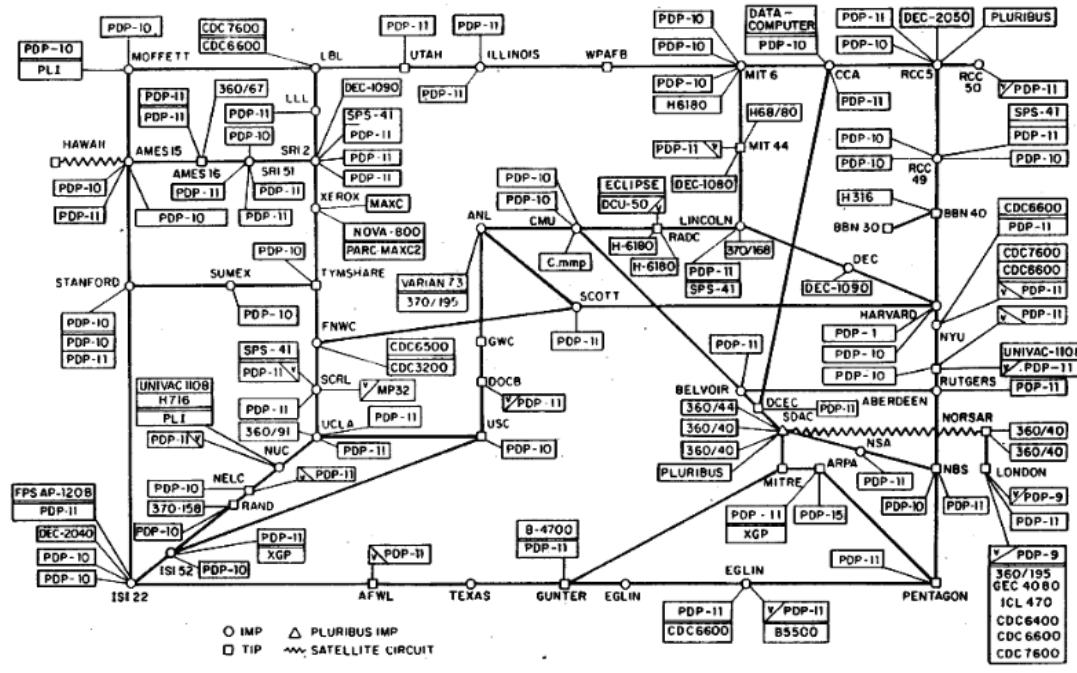
Antes dele Nicola Tesla já tinha dito que o homem um dia inventaria um instrumento que caberia no bolso e que com ele conseguiria se comunicar a longas distâncias, e que o mundo inteiro se converteria em um grande cérebro. Será que McLuhan e Tesla imaginariam que as suas previsões e conceitos se tornariam realidade no maior meio de comunicação que a humanidade já criou, levando à tal comunidade global?

O início da história da internet

A história da internet está ligada aos primeiros computadores conectados a energia elétrica que foram inventados nos anos 50, mas eles não eram nem um pouco parecidos com os computadores que nós conhecemos hoje. Eles eram enormes e só existiam em laboratórios, não eram feitos para o uso particular. Esses laboratórios ficavam no Reino Unido, na França e nos Estados Unidos.

Nos anos 60, em um desses laboratórios, o do Departamento de Defesa dos Estados Unidos, começou a ser desenvolvida uma rede que interligava computadores, chamada de ARPANET. Há quem diga que a rede era uma forma do governo americano se proteger caso perdesse comunicação durante a Guerra Fria, já que todos os computadores estariam conectados. O projeto da ARPANET, que ligava computadores em rede, inspirou a criação de uma rede que conectava várias redes, um conceito chamado de “internetworking”. Esse é um dos pontos chaves na história da internet.

ARPANET LOGICAL MAP, MARCH 1977



A criação

Vários outros projetos para desenvolver uma rede que conectasse os computadores do mundo todo começaram a ser criados nas principais universidades do mundo. A primeira vez que o termo internet foi utilizado foi em 1974, como abreviação do então “internetworking”. Era questão de tempo para que uma das muitas tentativas emplacasse.

Mas levou 20 anos para que a internet começasse a ganhar a cara que conhecemos hoje. Na década de 1980, uma pesquisa do cientista britânico Tim Berners-Lee resultou nessa rede que temos e que sem a qual não

conseguimos viver. Ele criou a World Wide Web no laboratório CERN, na Suíça. O que Berners-Lee fez foi linkar documentos de hipertexto em sistemas de informação, acessível de qualquer ponto daquela rede “primitiva” que tínhamos antes.

É difícil dizer que a internet é criação de apenas um homem, já que outros experimentos já existiam e já havia computadores conectados em rede quando Berners-Lee criou seu conceito. Mas pode-se dizer que a internet como nós conhecemos hoje foi criação dele. Ele é o criador do HTML, a primeira linguagem utilizada para a criação de sites; do HTTP, o principal protocolo utilizado; e da URL, que é o endereço que você escolhe no seu registro de domínio. Ou seja, basicamente tudo. Tim Berners-Lee ainda criou o primeiro browser, ou navegador, e o primeiro editor de sites. Ainda deixou tudo explicadinho para quem quisesse embarcar nessa também.

A abertura

No final de 1990, Tim Berners-Lee criou a primeira página web no formato que nós conhecemos. Hospedada em um servidor criado por ele mesmo. E em 1991 ele abriu ao mundo as portas para quem quisesse se juntar a essa nova comunidade online que ele havia inaugurado. Ele se deu conta que a sua criação só cresceria e funcionaria mesmo se ela fosse aberta a quem quisesse criar sua própria página sem custos, sem precisar pagar uma mensalidade, por exemplo, ou pedir algum tipo de permissão.

Então, em abril de 1993, foi anunciado que a internet como conhecemos hoje seria “royalty-free”, ou seja, livre de taxas para quem quisesse criar. E a partir disso ela cresceu sem limites, trazendo uma onda de inovação e criatividade sem precedentes na história da humanidade.

A revolução

Então, na metade dos anos 90, a internet começou a revolucionar a sociedade. Depois da internet, tivemos mudanças no modo como consumimos cultura, arte, notícias e produtos. As relações mudaram, as fronteiras diminuíram e a distância entre as pessoas ficou cada vez menor. Surgiram o e-mail, permitindo que as pessoas enviassem mensagens instantâneas e as ligações para outros

países ficaram muito mais baratas com a criação do sistema Voip (Voice Over IP). As discussões ficaram mais fáceis com os fóruns, e essa comunicação toda fez com que a internet se desenvolvesse exponencialmente.

Hoje, é possível até mesmo estudar pela internet através de vídeos gravados ou até mesmo ao vivo. As redes sociais se desenvolveram e a facilidade de comunicação revolucionou todos os setores. Alguns trabalhos sumiram enquanto novos empregos foram criados.



As iniciativas para globalização

A internet apenas seguiu uma tendência econômica e social. Enquanto os países mais desenvolvidos começavam a se inserir na rede, os chamados “países em desenvolvimento” foram de certa forma excluídos dessa novidade tecnológica, a princípio. Por isso que há quem diga que o sonho de uma rede mundial de computadores ainda não tenha se concretizado, porque falta bastante para a rede ser realmente mundial. Muitos lugares do continente africano ainda não tem nem mesmo luz elétrica, para se ter uma noção da distância para os países desenvolvidos.

Mas iniciativas para levar internet para todos os cantos do mundo já estão sendo tomadas por grandes empresas como o Google e o Facebook. Um dos projetos mais conhecidos é o “internet.org”, capitaneado por Mark Zuckerberg, o criador do Facebook. Em 2013, ele reuniu várias grandes empresas do mundo com a missão de levar conexão de internet para os cantos mais

remotos do planeta. O projeto surgiu de um estudo que apontava que dois terços da população do mundo ainda não tinha acesso a computadores.

O futuro

A história da internet você conheceu acima. O que falar sobre o futuro de um meio que muda tanto? O que se sabe é que ele chegou para ficar. A tendência é que cada vez mais pessoas utilizem a rede mundial de computadores para atividades cada vez mais corriqueiras. Ou seja, estaremos cada vez mais conectados. Hoje em dia nem mesmo usamos os termos “vou acessar a internet” ou “vou conectar na internet” porque já estamos o tempo inteiro conectados através de celulares.

Assim como cada vez mais pessoas devem usar a internet, ela deve estar em cada vez mais aparelhos. Já existe até um conceito, chamado de “Internet das Coisas”. Segundo especialistas do mundo digital, no futuro praticamente todos os objetos estarão conectados à internet, de roupas até eletrodomésticos. Então nos preparemos, porque o futuro, como se sabe, é logo ali.

Conclusão

A história da internet chegou ao momento em que a adesão no número de membros passa a ser maior e mais veloz do que qualquer outro meio de comunicação já criado pelo homem. Em menos de 50 anos desde a criação dos primeiros computadores eletrônicos já houve um salto gigantesco. E o propósito para o uso da rede também mudou, do uso militar na época da Guerra Fria para o uso pessoal e quase que universal nos dias de hoje.

Talvez não seja justo dar o mérito apenas a uma pessoa, mas o fato é que Tim Berners-Lee foi a figura preponderante nessa história. Ele que foi o responsável pela grande virada, que permitiu que hoje qualquer pessoa consiga criar seu site e se comunicar pela internet. E a expectativa é que cada vez mais pessoas sejam incluídas nesse verdadeiro universo de possibilidades.

Conceitos da Web para a Educação/Introdução às redes de computadores e a evolução da Internet

Introdução às Redes de Computadores e a Evolução da Internet

Rede de computadores

São dois ou mais computadores interligados entre si, com o intuito de trocar informações e compartilhar recursos. Exemplos de recursos compartilhados: físicos (impressora) e/ou lógicos (softwares). As Redes de Computadores sugeriram com a necessidade que os usuários de computadores das empresas terem de compartilhar programas, equipamentos e bases de dados. Atualmente, é muito difícil encontrar um computador que não trabalhe em rede, pois inclusive nas casas que contam com um só sistema, este passa a se tornar parte de uma rede mundial de computadores quando se conecta à internet.

Meios físicos de comunicação de redes

Os sistemas podem ser unidos por meio de cabos (comunicação tradicional: com fio) ou por meio de sinais infravermelho, entre outras (comunicação sem fio). Ou seja, os meios de comunicação podem ser: linhas telefônicas, cabos, satélites ou comunicação sem fios. Segundo o meio de transmissão de Rede por cabo (com fio) temos como exemplo: Rede de Cabo coaxial, Rede de Cabo de fibra óptica e Rede de Cabo de par trançado. A principal diferença das redes sem fio é que, como seu próprio nome indica, não utilizam cabos, ou seja, uma mídia guiada. Em seu lugar, o meio de transmissão é o ar, no qual são emitidas tanto as ondas de rádio como a luz infravermelha. Temos como exemplo: Rede por infravermelhos, Rede por microondas ou laser e Rede por rádio.

O QUE É A INTERNET?

Segundo o Ibope/NetRatings, já somos 79,9 milhões de internautas no Brasil, número quando fechou 2011, o 5º país mais conectado. Mas o que tanta gente faz por tanto tempo na internet? Consultas, pesquisas e compras, com certeza. Mas também relacionam-se com outras pessoas, escrevem blogs, trocam fotos, mantêm-se informados, participam de projetos e trabalham. A internet como se conhecia alguns anos atrás está mudando e rápido. Os números dos serviços que colocam os usuários na linha de frente não deixam dúvidas que o número de usuários de computador vai dobrar até 2012, chegando a 2 bilhões. A cada dia, 500 mil pessoas entram pela primeira vez na Internet e são publicados 200 milhões de tuítes; a cada minuto são disponibilizadas 48 horas de vídeo no YouTube; e cada segundo um novo blog é criado. 70% das pessoas consideram a Internet indispensável. Em 1982 havia 315 sites na Internet. Hoje existem 174 milhões.

De acordo o fragmento acima percebe-se a variedade de serviços que a internet oferece aos usuários. No entanto, o que realmente é a Internet? A internet é o conjunto de redes em escala mundial de milhões de computadores interligados pelo protocolo de comunicação TCP/IP (Transmission Control Protocol/Internet Protocol), que permite o acesso a todo tipo de informação e troca de dados. Esse protocolo é a linguagem comum dos computadores que integram a internet. Os serviços mais conhecidos da Internet são: o correio-eletrônico (protocolos SMTP, POP3), a transferência de arquivos (FTP), o compartilhamento de arquivos (NFS), a emulação remota de terminal (Telnet), o acesso à informação hipermídia (HTTP), conhecido como WWW (World Wide Web).

COMO SURGIU A INTERNET?

A Internet nasceu em 1969 no tempo de GUERRA, assim como várias evoluções criadas pela humanidade. Criada nos Estados Unidos na II Guerra Mundial, quando o país estava em guerra fria com a União Soviética, a rede interligava laboratórios de pesquisa do exército e se chamava ARPAnet (ARPA: Advance d Research Projects Agency / Net: Rede - Rede da Agência de Projetos de Pesquisa Avançados). Criada com o objetivo de descentralizar as informações, esta rede interligava várias redes em diversas regiões dos Estados Unidos. Ligava, inicialmente, computadores com informações sigilosas do governo para prevenir a perda destas informações caso houvesse um ataque russo, garantindo a segurança das mesmas informações em vários outros lugares. Com o fim da guerra fria, permitiram que cientistas e pesquisadores pudessem se conectar para estudo, logo depois as universidades e em seguidas universidades de outros países, desmanando para o resto do mundo. Hoje na nossa casa, na rua e quase todo lugar temos acesso a essa grande teia que hoje se chama Internet ou seja rede internacional. Nenhum outro meio de comunicação se expandiu tão rapidamente quanto a rede mundial de computadores.

Internet no Brasil

A Internet no Brasil chegou aqui em 1988, quando algumas universidades brasileiras começaram a fazer parte da rede de computadores das instituições de ensino superior dos Estados Unidos (a ARPANET). Mas, ainda nesta data, surgia a AlterNex, primeiro esboço do que seria a internet brasileira a partir dos anos 90. Assim como a ARPANET, a AlterNex começou como uma rede restrita para pesquisadores e acadêmicos de universidades. Mais tarde, em 1992 o público pode conhecer a rede mundial de computadores. Mais tarde, em 1997, os provedores comerciais de Internet passam a ganhar mercado no Brasil e o número de usuários começa a aumentar bastante. Os provedores puderam abaixar o preço com a chegada da conexão Banda Larga.

A WORLD WIDE WEB ou WWW

Para expansão da utilização da Internet foi decisiva a criação da www – World Wide Web. A Web nasceu em 1991, no laboratório CERN, na Suíça. Seu criador, Tim Berners-Lee e Robert Caillaiu, concebeu-a unicamente como uma linguagem que serviria para interligar computadores do laboratório e outras instituições de pesquisa, e exibir documentos científicos de forma simples e fácil de acessar. Estes cientistas também são responsáveis pelo desenvolvimento de duas ferramentas indispensáveis para a Internet: o código HTML e o protocolo HTTP. Com as invenções desses cientistas várias evoluções e melhorias nestes protocolos e códigos chegamos à Internet como a conhecemos. Hoje é o segmento que mais cresce e a chave do sucesso da World Wide Web (WWW) é o hipertexto. Os textos e imagens são interligados por meio de palavras-chave, tornando a navegação simples e agradável.

Classificação das redes de Computadores **Segundo a arquitetura de Rede:** - DSL - Ethernet - FDDI - ATM - e outras

Segundo a extensão geográfica: - LAN - Redes Locais - MAN - Redes Metropolitanas - WAN - Redes Mundiais - e outras...

Segundo a topologia - Rede em Anel - Rede em Barramento - Rede em Estrela - e outras

Segundo o meio de Transmissão - Por cabos - Sem fios

Introdução às Redes de Computadores e Evolução da Internet.

- Meios físicos de comunicação de redes;
- Protocolo;
- Pacote;
- Roteamento;
- Web;
- Internet e TCP/IP;
- Histórico da Internet e da web;
- Realidade aumentada e virtual;
- Computação nas nuvens;
- Tecnologias emergentes;

Meios físicos de comunicação de redes:

O meio físico de comunicação de redes mais usado atualmente é o padrão Ethernet. Esse padrão é formado por um conjunto de padrões conforme o meio de transmissão dos dados: Coaxial, par trançado, UTP, Gigabit ethernet, fibra óptica, e também a rede sem fio que se subdivide em outras: Wi fi, bluetooth, wimax e outras.

Protocolo:

Segundo o site do Wikipédia: “O TCP/IP é um conjunto de protocolos de comunicação entre computadores em rede (também chamado de pilha de protocolos TCP/IP). Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controlo de Transmissão) e o IP (Internet Protocol - Protocolo de Interconexão). O conjunto de protocolos podem ser vistos como um modelo de camadas, onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas estão logicamente mais perto do usuário (chamada camada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração”.

Como o próprio nome diz podemos fazer uma comparação com protocolo como

sendo um conjunto de procedimentos e regras de funcionamento a serem aplicados em cerimoniais e ocasiões em que se encontram representados os chefes de estado de um país, assim então comparando as duas definições podemos entender melhor o funcionamento do TCP/IP, que diz respeito a como os dados vão comunicar-se, as regras e o que deve ser feito em determinada circunstância, no que se refere ao tráfego dos dados.

Pacote:

É uma unidade de transferência de informação (carrinho que carrega os dados (bits)).

Pensando dessa maneira o cabo seja ele qual for (como os citados acima nos meios físicos), é a estrada por onde passam/trafegam esses carrinhos/dados empacotados.

Cada pacote carrega a informação que o ajudará a chegar a seu destino: o endereço IP do emissor, o endereço IP do destinatário pretendido, quantos pacotes essa mensagem de e-mail foi dividida e o número desse pacote em particular. Cada pacote é então enviado para seu destino por meio do melhor caminho disponível: um caminho que pode ser seguido por todos os outros pacotes da mensagem ou por nenhum deles. Isso torna a rede mais eficiente. Geralmente os pacotes têm três partes: cabeçalho (instruções e informações), corpo (dados a serem transmitidos) e rodapé (normalmente avisa ao receptor que o fim do pacote foi atingido, ou pode verificar se algum erro ocorreu).

Roteamento:

É definir a rota/caminho.

Roteamento é a forma utilizada na internet através da qual, duas máquinas em comunicação (conectadas através da rede) “acham” e usam o melhor caminho através dessa rede, para entregar os pacotes de dados entre hosts (equipamentos de rede de uma forma geral, incluindo computadores, roteadores etc.).

Essa sequência de transmissão de dados envolve:

- Definir que caminhos estão disponíveis;
- Escolher o “melhor” caminho, para um objetivo específico;
- Usar esse caminho para chegar ao destino desejado;
- Adaptar o formato dos dados às tecnologias de transporte (comunicação) disponíveis.

Web:

A World Wide Web que significa, "Rede de alcance mundial"; também conhecida como apenas Web ou WWW. Internet e TCP/IP: Segundo Wikipédia: "A Internet é um conglomerado de redes em escala mundial de milhões de computadores interligados pelo protocolo de comunicação TCP/IP que permite o acesso a informações e todo tipo de transferência de dados. Ela carrega uma ampla variedade de recursos e serviços, incluindo os documentos interligados por meio de hiperligações da World Wide Web (Rede de Alcance Mundial), e a infraestrutura para suportar correio eletrônico e serviços como comunicação instantânea e compartilhamento de arquivos."

A Internet possibilitou a integração e interação das pessoas em diversos lugares permitindo interação a troca de ideias e pontos de vista, além é claro de agilizar processos, antes jamais pensados de serem executados com tamanha rapidez e perspicácia de informações.

Realidade aumentada e virtual:

"De uma forma simples, Realidade Aumentada é uma tecnologia que permite que o mundo virtual seja misturado ao real, possibilitando maior interação e abrindo uma nova dimensão na maneira como nós executamos tarefas, ou mesmo as que nós incumbimos às máquinas. Assim, se você pensava que objetos pulando para fora da tela eram elementos de filmes de ficção científica, está na hora de mudar seus conceitos. Aliás, o que acontece com a Realidade Aumentada é o contrário: você pulará para dentro do mundo virtual para interagir com objetos que só estão limitados à sua imaginação."

Uma prova disso são os novos vídeos game que estão aí, levando você cada vez mais a entrar nesse mundo virtual e interagir, inserindo-se no contexto dos jogos, o que proporciona aumentar a realidade da interação através da virtualização. Com o aumento da capacidade de processamento dos celulares

eles estão se tornando uma plataforma para o desenvolvimento desses jogos que utilizam realidade aumentada para poder imergir os usuários na realidade dos jogos.

Computação nas nuvens:

“O conceito de computação em nuvem (em inglês, cloud computing) refere-se à utilização da memória e das capacidades de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet, seguindo o princípio da computação em grade. O armazenamento de dados é feito em serviços que poderão ser acessados de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas x ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da Internet - daí a alusão à nuvem. O uso desse modelo (ambiente) é mais viável do que o uso de unidades físicas. Num sistema operacional disponível na Internet, a partir de qualquer computador e em qualquer lugar, pode-se ter acesso a informações, arquivos e programas num sistema único, independente de plataforma. O requisito mínimo é um computador compatível com os recursos disponíveis na Internet. O PC torna-se apenas um chip ligado à Internet — a "grande nuvem" de computadores — sendo necessários somente os dispositivos de entrada (teclado, mouse) e saída (monitor).” Wikipédia.

Ainda sou contra essa modalidade de armazenamento e compartilhamento de recursos, acho que a confiabilidade ainda é um ponto a ser bem pensado antes de entregar seus dados a alguém, ou submeter-se a vontade de outrem de disponibilizar ou não recursos. Posso estar errada, mas por enquanto estou receosa em utilizar à computação em nuvem. Apesar de achar que esse compartilhamento de recursos possa ser viável para auxiliar na disseminação e uso de tecnologias pelas pessoas que não podem adquirir tais recursos. Muitos defendem falando das criptografias e que nem mesmo eles sabem onde estão seus dados, mas eu me pergunto por que eles seriam tão bonzinhos com todo mundo. E penso logo, o que eles querem alcançar “ganhar” com isso. Continuo não confiando e ainda me mantendo na retaguarda esperando o que vai acontecer daqui pra frente.

Tecnologias emergentes:

São as novas tecnologias, eletrônicas, programas, aplicativos, de lançamento recente, ou em fase de teste e com previsão de lançamento, para os consumidores.

- Informática para Agregação de Valor à Informação
- Biologia Sintética e Engenharia Metabólica
- Revolução Verde 2.0 - Tecnologias para a Alimentação e Aumento da Biomassa
- Materiais em Nanoescala
- Biologia de Sistemas e Modelagem Computacional e Simulação de Sistemas Químicos e Biológicos
- Utilização do Dióxido de Carbono como um Recurso
- Energia sem Fios
- Sistemas de Energia de Alta Densidade
- Medicina Personalizada, Nutrição e Prevenção de Doenças

E a melhor de todas. Porque através dessa todas as outras são desencadeadas e tornam-se possíveis.

- Tecnologias Avançadas para Educação

Fontes pesquisadas: google e Wikipédia.

“Bom mesmo é ir a luta com determinação, abraçar a vida com paixão, perder com classe e vencer com ousadia... Pois o triunfo pertence a quem se atreve.”

Charles Chaplin

Modelo OSI – Modelo de Referência de desenvolvimento de comunicação

No intuito de facilitar o processo de padronização e obter comunicação entre máquinas de diferentes fabricantes, a ISO (International Standards Organization em português: Organização Internacional de Normalização), criou um modelo de arquitetura para sistemas abertos, visando permitir a comunicação entre máquinas heterogêneas e definindo diretrizes genéricas para a construção de redes de computadores independente da tecnologia de

implementação.

O modelo foi denominado OSI (Open Systems Interconnection), servindo de base para a implementação de qualquer tipo de rede, seja de curta, média ou longa distância. Definindo exatamente o que cada camada deve fazer, mas não como fazer e nem define quais os protocolos que as camadas utilizaram. A arquitetura do modelo OSI é formada por camadas (ou níveis), interfaces e protocolos. Esses protocolos são conjuntos de regras e formatos que permitem a comunicação entre as camadas nas diferentes máquinas. Em cada camada podem ser definidos um ou mais protocolos. A forma mais simples de entender qual o princípio de funcionamento do modelo OSI é pensar que cada camada adicionar um cabeçalho com informações nos dados do usuário que serão transmitidos para outro sistema, e quando a informação chega ao outro lado a função do modelo é entender o cabeçalho, retirar a informação que precisa e passar a informação a diante para a próxima camada que entenderá e ao final do processo será exibido para o usuário final.

Exemplificando cada camada do modelo OSI, do nível mais baixo ao mais alto.

1 – Camada Física Os protocolos deste nível são os que realizam a codificação/decodificação de símbolos e caracteres em sinais elétricos lançados no meio físico. O nível físico tem a função de transmitir uma seqüência de bits através de um canal de comunicação.

2 – Camada de Enlace de Dados Neste nível a camada receber/transmiti uma seqüência de bits do/para o nível físico e transformá-los em uma linha que esteja livre de erros de transmissão, a fim de que essa informação seja utilizada pelo nível de rede.

3 – Camada de Rede A camada de rede controla a operação da rede de um modo geral. Fazendo o roteamento dos pacotes entre fonte e destino, o controle de congestionamento e a contabilização do número de pacotes ou bytes utilizados pelo usuário, para fins de tarifação.

4 – Camada de Transporte A camada de transporte inclui funções relacionadas com conexões entre a máquina fonte e máquina destino, segmentando os dados em unidades de tamanho apropriado para utilização pelo nível de rede, seguindo ou não as orientações do nível de sessão.

5 – Camada de Sessão A função da camada de sessão é administrar e sincronizar diálogos entre dois processos de aplicação. Os protocolos desse nível tratam de sincronizações na transferência de arquivos.

6 – Camada de Apresentação A função da camada de apresentação é assegurar que a informação seja transmitida de tal forma que possa ser entendida e usada pelo receptor.

7 – Camada de Aplicação A camada de aplicação fornece ao usuário uma interface que permite acesso a diversos serviços de aplicação, convertendo as diferenças que existem em diferentes fabricantes para um denominador comum. Esta camada de aplicação é o nível que possui o maior número de protocolos existentes, devido ao fato de estar mais perto do usuário e os usuários possuírem necessidades diferentes.

Tabela pra entender melhor:

CAMADA	FUNÇÃO
APLICAÇÃO	Funções especializadas (transferência de arquivos, terminal virtual, e-mail)
APRESENTAÇÃO	Formatação de dados e conversão de caracteres e códigos
SESSÃO	Negociação e estabelecimento de conexão com outro nó
TRANSPORTE	Meios e métodos para a entrega de dados ponta-a-ponta
REDE	Roteamento de pacotes através de uma ou várias redes
ENLACE	Detecção e correção de erros introduzidos pelo meio de transmissão
FÍSICA	Transmissão dos bits através do meio de transmissão

SPAM / Hackers

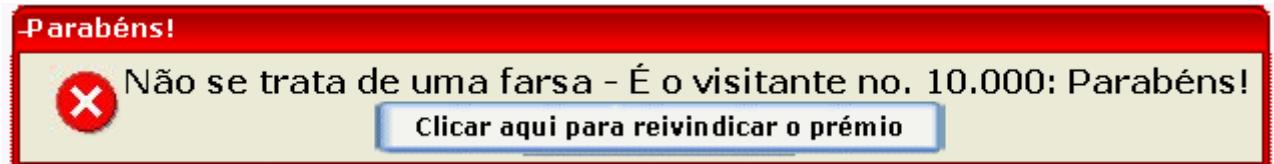
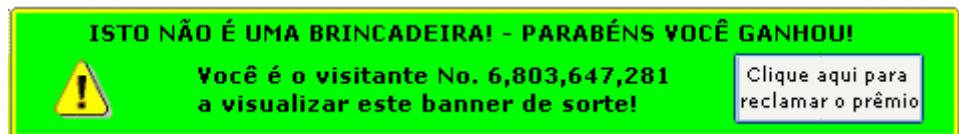
Quais cuidados devo ter para minha segurança na internet?

Imprimir dúvida

Proteja-se de fraudes - Atualize seu antivírus diariamente. - Não clique em links recebidos por e-mails. - Não execute arquivos recebidos por e-mail ou via serviços de mensagem instantânea. - Não clique em links informando:

Prêmios. Exemplos:

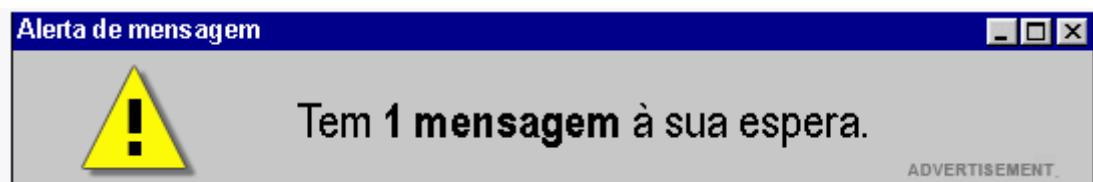




Serviços para seu sistema operacional. Exemplo:



Alerta de mensagem. Exemplo:



Consulte o canal de atendimento do site sempre que houver dúvidas se o pop-up ou banner pertence à página ou não. **Proteja-se de vírus, cavalos de tróia, spywares, worms e bots** - Mantenha todos os programas que você usa sempre atualizados. - Instale todas as correções de segurança. - Use antivírus, firewall pessoal e anti-spyware.

Navegue com segurança

- Mantenha seu navegador sempre atualizado. - Desative Java e ActiveX. Use-os apenas se for estritamente necessário. - Só habilite JavaScript, cookies e pop-up windows ao acessar sites confiáveis.

Cuide-se ao ler e-mails

- Mantenha o programa leitor de e-mails sempre atualizado. - Desative a visualização de e-mails em HTML. - Desative as opções de execução

automática de arquivos anexados. - Desative a execução de JavaScript e Java. **Proteja sua privacidade**

- Use senhas com letras, números e símbolos. - Nunca use como senha dados pessoais ou palavras de dicionários. - Não coloque dados pessoais em páginas Web, blogs ou sites de redes de relacionamentos.

Use celulares e PDAs com segurança

- Habilite bluetooth só quando for utilizá-lo. - Consulte o fabricante sobre atualizações para seu aparelho. - Não aceite qualquer arquivo enviado para seu aparelho. Cheque a procedência.

Dicas para quem usa banda larga

- Use antivírus e firewall pessoal. - Desligue o compartilhamento de recursos. - Mantenha os programas que você usa sempre atualizados. - Instale todas as correções de segurança.

Dicas para quem usa redes sem fio

- Use antivírus e firewall pessoal. - Use WEP ou WPA sempre que possível. - Use somente serviços com conexão segura. - Implemente também as dicas para quem usa banda larga.

Caso não tenha nenhum serviço nas dicas citadas acima, o Terra dispõe dos serviços de Antivírus e Firewall, conforme abaixo:

Com o Antivírus Terra não é preciso ficar desconfiado, porque ele oferece Proteção 2 em 1: contra vírus e spywares. O serviço evita, detecta, bloqueia e eliminam vírus, worms, cavalos de Tróia e spywares, que podem levar à perda ou a danos de documentos insubstituíveis, como fotos digitais, filmes de família ou declarações de imposto de renda. Deste modo, permitindo que o Cliente navegue na web e baixe arquivos com total segurança.

O Firewall Terra simplifica a segurança para seus usuários. Ele facilita a análise do status de segurança, verifica atualizações e soluciona possíveis

problemas de segurança. Além disso, com a assinatura paga, ele recebe automaticamente as últimas atualizações de software por conta do monitoramento da McAfee em todo o mundo contra as mais recentes ameaças. Oferecendo ao Cliente confiabilidade para navegar na web e baixar arquivos: "sempre ativo, sempre atualizado e sempre protegendo você".

Dicas Básicas para usar a Internet com segurança

Estar conectado à internet é estar sob alguma ameaça virtual em potencial. Sem adotar um tom de teoria da conspiração, é preciso estar ciente de que a web reserva coisas maravilhosas e também uma série de problemas. Porém, é preciso deixar claro também que muitos problemas podem ser evitados com alguns cuidados básicos tanto no computador quanto nos portáteis.

1. Escolha senhas fortes e não repetidas



The image shows the interface of the Secure Password Generator. At the top, there is a logo of two interlocking keys and the text "Secure Password Generator". Below this, there is a form with various settings for generating a password. The settings include:

- Password Length: 16
- Include Symbols: (e.g. @#\$%)
- Include Numbers: (e.g. 123456)
- Include Lowercase Characters: (e.g. abcdefgh)
- Include Uppercase Characters: (e.g. ABCDEFGH)
- Exclude Similar Characters: (e.g. I, l, 1, L, o, 0, O)
- Exclude Ambiguous Characters: ({ } [] () / \ ^ * ~ , ; : < >)
- Generate On The Client Side: (do NOT send across the Internet)
- Auto-Select: (select the password automatically)
- Save My Preference: (save all the settings above for later use)
- Load My Settings Anywhere: URL to load my settings on other computers quickly

At the bottom, there is a large blue button labeled "Generate secure password". Below the button, there is a text box labeled "Your New Password:" and a message: "Your new password will be shown here."

Um gerenciador de senha pode ajudar. (Foto: Reprodução/Secure Password Generator)

É claro que é mais fácil usar uma senha simples, fácil de ser memorizada, em todas as suas contas de serviços na internet, mas nem de longe isso é o

recomendável. Vamos analisar o seguinte caso: você usa a senha do e-mail também no Facebook, no Twitter e no Instagram; se ela for descoberta, o que já seria um grande problema se torna algo ainda maior.

Além disso, usar combinações pouco óbvias também é extremamente importante. Pensar em uma combinação assim pode ser mais complicado do que parece, afinal ela precisa fugir da obviedade, mas também deve se manter dentro do componível e decorável para você não precisar refazer a senha sempre que for acessar um serviço. Portanto, uma boa recomendação é o uso de geradores de senha como Secure Password Generator, Random Password Generator, LastPass Generate a Password ou Dashlane's Password Generator.

2. Use a autenticação de dois fatores

The image shows a screenshot of the Two Factor Auth (2FA) website. At the top, there is a large circular icon containing a smartphone. Below it, the text "Two Factor Auth (2FA)" is displayed in a bold, dark font. Underneath that, a subtext reads "List of websites and whether or not they support 2FA." A search bar with the placeholder "Search websites" is positioned below the subtext. Further down, there are five circular icons with corresponding labels: "Backup and Sync" (car icon), "Banking" (dollar sign icon), "Cloud Computing" (cloud icon), "Communication" (speech bubble icon), and "Cryptocurrencies" (Bitcoin icon).

Autenticação de dois fatores incrementa a segurança. (Foto: Reprodução/Two Factor Auth)

Este é um dos principais recursos da atualidade e está disponível em uma série de serviços da web. Neste tipo de autenticação, a senha que você define quando cria uma conta não é o suficiente para acessar o seu perfil; para isso, é

preciso digitar um código gerado especificamente para aquele acesso, normalmente enviado até você via SMS.

O site Two Factor Auth é um agregador no qual você encontra todos as páginas da web que oferecem este tipo de segurança extra. Serviços como Twitter, Facebook, Medium, Snapchat, Tumblr, WordPress, iCloud, Box, Dropbox, Evernote, OneDrive, Skype, Telegram, Gmail, Outlook.com e Yahoo Mail são apenas alguns dos inúmeros que contam com a autenticação de múltiplo fator.

3. Considere sempre o uso de criptografia para enviar informações

Informações sensíveis apenas via e-mail criptografados.

Se você vai mandar informações pessoais ou até mesmo fotos que não deveriam ser vistas por qualquer pessoa, uma ótima dica é recorrer à criptografia. Atualmente, o Gmail criptografa todas as mensagens que você envia, mas ainda há alguns serviços de e-mail focados no tema, como ProtonMail — por enquanto, é preciso solicitar um convite para utilizá-lo —, Lockbin e Sendinc.

Outra boa dica para “criptografar” informações sensíveis enviadas pela web, como nomes de usuário e senha, é fazer isso combinando diferentes serviços convencionais. Por exemplo, você manda uma mensagem no Messenger dizendo que enviará os dados de login e senha de um determinado serviço, mas envia tais informações via WhatsApp. Com isso, você descontextualiza esses dados, tornando-os inúteis para quem encontrá-los.

4. Coloque senha no seu roteador



O roteador é a ponte entre os seus dispositivos e a sua internet residencial, logo protegê-lo é uma das medidas mais efetivas para evitar maiores problemas. Quando você define uma senha, aumenta as barreiras para que possíveis invasores se conectem à sua rede e, com isso, tenham acesso facilitado a outras máquinas que compartilham a mesma conexão.

5. Reveja as permissões concedidas em suas contas nas redes sociais

Protect Your Personal Information

[Get alerts when apps and websites gain access to your info >](#)



Jogos e sites da web costumam oferecer a opção de login via Twitter, Google ou Facebook. Além disso, alguns serviços de terceiros que você usa em conjunto com alguma rede social ou e-mail também solicitam acesso a eles. Quando você oferece tal informação permite que alguns dados sejam visualizados, ou seja, é importante ficar atento.

Portanto, o ideal é verificar regularmente quais serviços têm acesso a essas informações, algo que pode ser feito diretamente dentro de sua conta. Google, Facebook e Twitter, por exemplo, contam com páginas específicas para isso, mas o site MyPermissions escaneia diversas contas suas a fim de encontrar quais apps de terceiros têm permissão para acessá-las.

6. Use VPN ao acessar uma rede pública

Uma VPN ainda é a principal proteção de quem acessa a internet a partir de uma rede pública — aquelas oferecidas em shoppings, aeroportos, bibliotecas, cafés e por aí vai. Elas ajudam você a se manter a salvo de ataques de invasores que acessam essas mesmas redes para roubar informações de outros dispositivos conectados a ela.

Caso você tenha o costume de acessar esse tipo de rede, o ideal é fazê-lo por meio de uma VPN. Ela cria uma espécie de túnel pelo qual transitam as informações entre o seu dispositivo e a web, mantendo você anônimo e dificultando o acesso indevido de outras pessoas à sua máquina. Alguns bons nomes do gênero são CyberGhost VPN, TotalVPN, SurfEasy, Tor + VPN e Private Tunnel.

O papel da internet e das redes sociais no desenvolvimento sustentável

Numa sociedade cada vez mais conectada, o papel das ferramentas web acaba ganhando mais importância a cada dia. Nesse cenário os websites organizacionais surgem como uma vitrine virtual e importante ferramenta de comunicação empresarial. Dentro do ambiente online todo o conhecimento gerado pela empresa é armazenado e compartilhado. Os sites também são utilizados para disponibilizar e divulgar as ações institucionais da

empresa, promover os benefícios da marca, produtos e serviços, estabelecer a comunicação com seus diversos públicos, e outras funções que ajudam na construção da imagem corporativa.

Os websites também estão sendo muito utilizados para divulgar as ações de responsabilidade social das empresas, suas ações sociais e ambientais, bem como todas as ações relacionadas à sustentabilidade. Eles são a própria tradução do mundo perfeito, os conteúdos inseridos no link de sustentabilidade descrevem o que podemos chamar de “mundo da fantasia” ou “universo fantástico”, pela beleza como são descritas as ações, produtos, discursos, certificações, códigos de comportamento, dentre outros. Sem esquecer o aspecto e aparência produzida para ilustrar todo esse composto de sustentabilidade, ou seja, toda a criação de imagens e design utilizado para que tenhamos a percepção de adentrar ao mundo da fantasia, assim como Alice no País das Maravilhas. No entanto, essa postura pode trazer certa desconfiança por parte daqueles que acessam o site da empresa.

Waddock e Googins, estudiosos do assunto, afirmam que quanto mais a empresa comunica suas práticas de responsabilidade social e sustentabilidade, menos as pessoas e stakeholders creditam que essas sejam verdade, ou seja, quanto mais excessiva for a comunicação, maior pode ser a desconfiança de seus públicos.

As empresas que investem recursos em projetos sociais e ambientais visam obter ganho e reconhecimento institucional e, para isso, investem recursos para comunicar suas iniciativas. Pode-se afirmar que quanto melhor o desempenho financeiro de uma empresa, mais ela investe em sustentabilidade e quer divulgar suas ações, principalmente em seus websites, onde pode reafirmar os valores e princípios que norteiam sua atuação responsável, seu código de ética, os projetos sociais e ambientais e os resultados alcançados, o relatório de sustentabilidade, certificações e premiações ambientais etc.

Apesar disso, é preciso que os comunicadores empresariais fiquem atentos com a utilização dos websites para a divulgação da sustentabilidade das empresas. A internet se tornou uma enorme rede social e, por isso, é preciso que os conteúdos institucionais sejam publicados também em outros

dispositivos digitais, blogs ou outras mídias sociais. O modelo de website corporativo que conhecemos tem sérios problemas, pois não oferece conteúdo relevante e não privilegia o lado social da web. As empresas já estão migrando para as redes sociais e concentrando suas estratégias online em redes sociais mais populares, como o Twitter e o Facebook, tornando os websites corporativos cada vez mais irrelevantes.

Isso significa também que as empresas precisarão estar mais dispostas ao diálogo, os conteúdos sustentáveis devem ser discutidos e promover mais interatividade. Não basta somente promover a imagem institucional no ambiente digital, é preciso que a sustentabilidade seja apresentada de forma natural, sem exageros, de forma coerente, onde todos possam ser participantes do processo de sustentabilidade.

A evolução das redes sociais e seu impacto na sociedade

Em pleno ano de 2018, difícil é encontrar alguém que não use nenhuma rede social. Essas poucas pessoas decidem viver à margem da sociedade 2.0 e, mesmo sabendo que ficam de fora de muita coisa bacana que acontece nessas plataformas, elas seguem firmes na decisão por uma série de fatores, que vão desde a garantia da privacidade até o medo de se tornarem "viciadas" em rede sociais – como acontece com muita gente por aí, que praticamente se esquece de todo o resto da internet, acessando somente Facebook, Instagram e Twitter no dia-a-dia.

Mas como foi que as redes sociais ganharam tanto poder, a ponto de transformar a maneira com que as pessoas se relacionam, se informam e se comunicam, em tão pouco tempo? Ainda, como exatamente as redes sociais impactaram a nossa sociedade cultural e socialmente falando? E o que vai acontecer daqui para frente com as plataformas sociais ganhando cada vez mais influência?

Nessa série de matérias, divididas em três partes, vamos fazer uma análise do surgimento, evolução e o status atual das redes sociais, bem como seu impacto na sociedade conectada em que vivemos.

O que é rede social, como e quando elas surgiram?

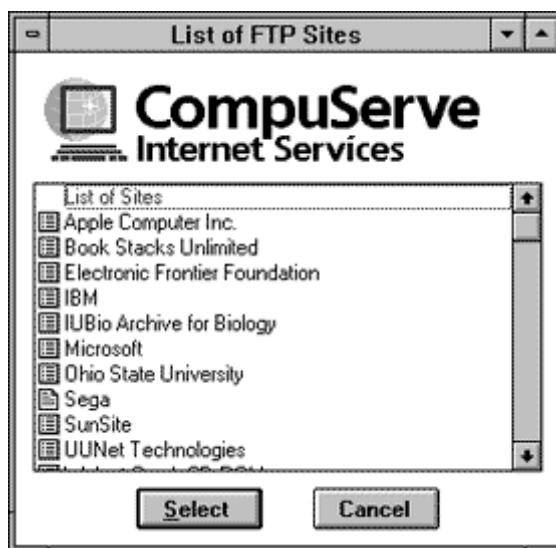
Há quem defina rede social como qualquer meio que proporcione a comunicação entre as pessoas, mas essa definição genérica acaba englobando métodos nada tecnológicos, como o envio de cartas, por exemplo. Já nos tempos modernos, rede social é como são chamados serviços que, usando a internet, permitem que as pessoas se conectem umas com as outras instantaneamente.

Na era pré-internet, o telégrafo fez as vezes de uma rede social pré-histórica, permitindo o envio de mensagens a longas distâncias usando a tecnologia. Então, antes da existência da internet como a conhecemos, existiu uma tecnologia militar chamada ARPANET, que conectava universidades em uma proto-internet. A primeira mensagem enviada por esta plataforma saiu da UCLA para o Stanford Research Institute em 1969.

29 Oct 69	2100	LOADED	OP. PROGRAM	CSK
		FOR	BEN BARKER	
		BBN		
22:30		TALKED TO SRI		CSL
		HOST TO HOST		
		LEFT OP. IMP. PROGRAM	CSL	
		running after sending		
		a host end message		
		to imp.		

Primeiro log IMP da ARPANET mostra transcrição da primeira mensagem enviada pela plataforma, em 29/10/1969 (Foto: Reprodução)

Então, já em 1982, a ARPANET foi a primeira rede a usar o protocolo TCP/IP, abrindo as portas para um mundo totalmente novo. Já com a chegada da computação pessoal, a CompuServe foi um dos primeiros serviços a oferecer conexão com a internet internacionalmente, sendo, também, a empresa que criou o formato GIF. Para acessar a rede, era preciso usar um cliente de acesso próprio, que oferecia serviços de e-mail e fóruns de discussão. Nos anos 1990, o serviço já era muito popular, sendo posteriormente fundido com a AOL, que dominou a internet na época.



Interface jurássica do CompuServe (Foto: Reprodução)

Mas, voltando um pouco nessa história, não podemos deixar de mencionar o BBS, que, em 1978, colocou no ar o seu primeiro sistema rudimentar de comunicação virtual. A coisa não era nada barata, visto que era necessário fazer chamadas telefônicas de longa distância para conseguir a conexão, sendo, portanto, algo restrito a um número seletivo de usuários naquele tempo, mas popularizando-se à medida em que o acesso à rede era expandido.



Assim era o BBS nos anos 1980 (Foto: Reprodução)

Mais ou menos na mesma época, surgiu a Usenet, ativa até os dias de hoje. A coisa funcionava como um Reddit em seus primórdios, permitindo que os usuários acompanhasssem longos tópicos de conversas em que se inscreviam para participar. Foi com a Usenet que muitos termos que usamos até hoje na rede se popularizaram, como "spam" ou "FAQ", por exemplo. Em 1995, o conteúdo mais antigo da Usenet foi arquivado, podendo ser acessado posteriormente.



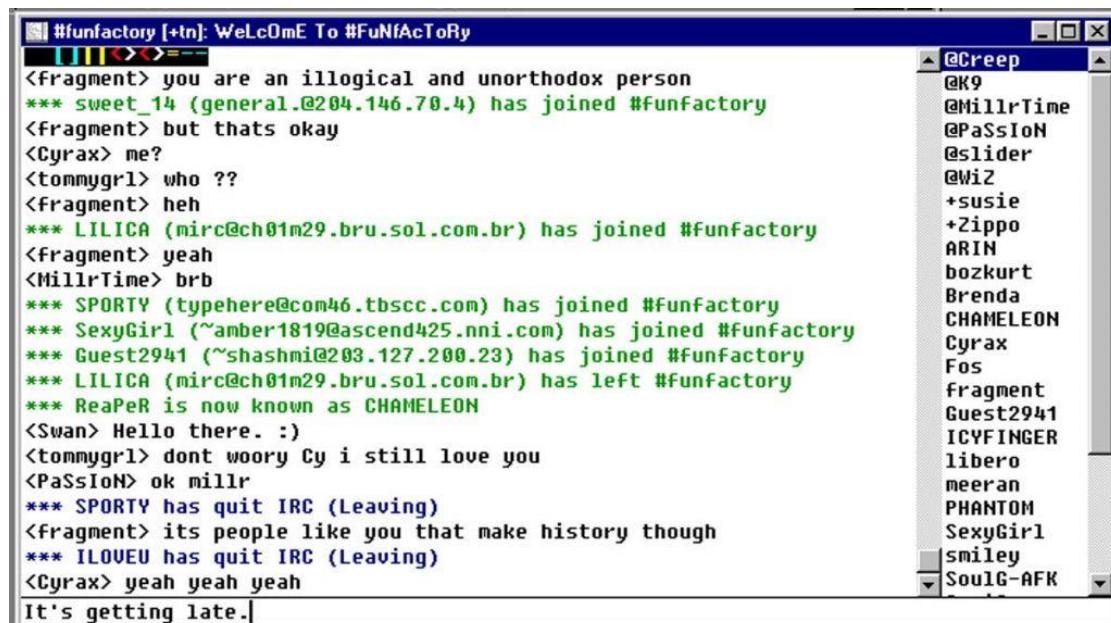
Menu de um grupo antigo da Usenet (Foto: Reprodução)

Ainda que timidamente, essas novidades começaram a mudar a forma com que as pessoas se comunicam, permitindo, ainda, conhecer gente que não

conheceríamos ao vivo por lá. Isso já marcou o início da transformação da nossa sociedade, com as pessoas cada vez mais buscando a internet como meio de entrar em contato com outras, se informar e se entreter.

A revolução do IRC e a World Wide Web

O termo "rede social" ainda não era usado nessa época, mas a chegada do IRC revolucionou esse universo. Criado em 1988, o protocolo serviu como base para vários serviços de comunicação virtual na época. Serviços baseados em mensagens de texto se dividiram em canais moderados por pessoas eleitas para colocar ordem na casa, e uma variedade de clientes de IRC começaram a surgir, com o mIRC sendo o mais famoso de todos eles.



Canal do mIRC na década de 1990 (Foto: Reprodução)

Na mesma época, a World Wide Web veio para ficar, com serviços como o Geocities se popularizando rapidamente. Com ele, era possível publicar sites rudimentares na rede mundial de computadores, e muitos fóruns de discussão surgiram hospedados ali. Isso aconteceu em 1994, bem na época em que a conexão discada com a internet estava começando a se popularizar em todo o mundo. Em 1999, o Yahoo! adquiriu o Geocities, que permaneceu no ar até 2009.



Página criada com o Geocities na década de 1990 (Foto: Reprodução)

Outros serviços similares ao Geocities pipocaram no período, ocasionando outra revolução: com eles, qualquer pessoa podia publicar suas ideias na internet, mesmo sem entender muita coisa de webdesign e programação, abrindo as portas para as chegadas dos blogs pessoais.

Mensageiros como os conhecemos

E por falar na popularização da internet discada, não podemos deixar de falar na AOL e seu Instant Messenger, lançado em 1997. O AIM, como ficou conhecido, trouxe às massas pela primeira vez um mensageiro instantâneo com interface agradável para quem não entende nada de códigos de programação.



Tela do programa da America Online, mostrando AIM ao fundo e os menus recheados de conteúdos

(Foto: Reprodução)

Ali, era possível criar um perfil de usuário, adicionar amigos, conversar por meio de mensagens de voz e transferir arquivos, pavimentando o terreno para o surgimento das redes sociais atuais, incluindo seus mensageiros modernos, como o Messenger, do Facebook, o WhatsApp e o Telegram. Mas, antes disso, mensageiros similares ao AIM, como o MSN Messenger e o ICQ, se tornaram o principal meio de comunicação de uma imensidão de pessoas.

Na segunda parte deste especial vamos falar da era que surgiu depois de 1997, quando a primeira rede social propriamente dita surgiu para transformar o mundo, mesmo que sem essa intenção. Também vamos falar da era dos blogs pessoais, que ajudaram a pavimentar a estrada das redes sociais atuais, e o furacão de transformações que foram os anos 2000.

Segurança de Redes: A importância de ter uma boa gestão e controle



Conforme a internet evolui — e as redes de computadores se tornam maiores e mais complexas — a segurança de redes transforma-se em um fator relevante para as empresas considerarem. Afinal, se gigantes como a Microsoft estão projetando e criando produtos de software que precisam ser protegidos constantemente contra-ataques de terceiros, a sua empresa também.

Ao aumentar a segurança de redes você diminui a chance de acontecerem roubos de identidade, falsificações e vazamentos. E, se a pirataria é outra de suas preocupações, é apenas com a segurança de redes que podemos evitá-la. Hoje você vai entender melhor a importância dessa segurança e como garantí-la em seu negócio.

O que é segurança de redes?

Segurança de redes é combinar múltiplas camadas de defesa a fim de proteger usabilidade e integridade de suas conexões e dados. A segurança de redes tradicionalmente inclui tecnologias de hardware e software e gerencia o acesso, buscando impedir que uma variedade de ameaças se instale em sua rede.

Existem vários recursos para a segurança de redes, dentre os quais temos o monitoramento de acesso, uso de software antivírus e antimalware, a

segurança em nível do aplicativo e a análise comportamental — capaz de detectar intrusões enquanto elas acontecem.

Além disso, soluções de prevenção de perda de dados, segurança de e-mail e segmentação de rede são outros dos recursos que, junto de uma VPN, podem salvaguardar as informações do seu negócio.

Há muitas maneiras de proteger seus dados na internet e você vai entender melhor a importância disso no tópico a seguir.

Por que a segurança de redes é importante?

Em um contexto em que negócios confiam cada vez mais na internet a nas redes de computadores, empresas podem enfrentar grandes desafios como ameaças de erros, invasões hackers e infecções por vírus. É por isso que é tão importante proteger a sua rede.

Quem trabalha online tem como um dos fatores mais importantes a se considerar a segurança de redes. Mesmo porque, ainda que nenhuma delas possa ser imune ao ataque, é responsabilidade de administradores garantir um sistema de alta qualidade para redução de riscos — pois é a segurança de redes que protege dados de clientes.

Hoje o roubo de identidade está em ascensão e, como fornecedor de produtos ou serviços, é seu dever manter as informações de consumidores em segurança. Uma boa segurança de redes pode ajudar a reduzir o risco de seu negócio ser vítima de roubo de dados.

Outro motivo para investir é que os sistemas de segurança de rede podem ser eficazes para proteger seus computadores e demais equipamentos de danos físicos causados por vírus e malware. Pense no ransomware e no seu impacto, que torna virtualmente inutilizáveis computadores e arquivos. Para não ter de abrir mão de suas máquinas, empresas ganham muito investindo em segurança de redes.

Além disso, para computadores em uma rede compartilhada, um sistema de segurança e controle é o que ajuda a manter informações — e dados — seguros. Por último, instalações de segurança tendem a beneficiar seu negócio massivamente e reduzir custos a longo prazo. Com menores tempos de inatividade e menos atrasos é possível lucrar muito mais.

Como garantir boa gestão e controle de redes?

Então, quão seguros estão os dados da sua empresa? Você consegue garantir a segurança de redes? A notícia boa é que existem várias etapas simples e econômicas para proteger dados corporativos, fortalecer as barreiras em suas redes e proteger sua reputação.

Confira o que você pode começar a fazer agora mesmo para uma melhor gestão e controle de redes.

Aplique uma boa estratégia de senha

Senhas complexas são o primeiro passo para uma boa estratégia de segurança de redes, e elas devem ser alteradas pelo menos a cada 90 dias. Criar uma política de senha forte é fundamental para ajudar seus usuários a protegerem sistemas críticos em que confiam todos os dias.

Uma senha de 6 caracteres com apenas letras têm 308915776 possíveis combinações, enquanto uma senha de 8 caracteres com letras maiúsculas e minúsculas, que inclui números de símbolos, tem 6095689385410816. Boas senhas são críticas para a segurança da informação e as políticas que garantem isso são uma responsabilidade institucional.

Use um plano de backup seguro

Toda estratégia de TI tem um bom plano de backup, e quando o assunto é segurança de redes não poderia ser diferente. Backups são responsáveis por eliminar o risco de apagamentos acidentais e diminuir o impacto do roubo de dados em ataques como o ransomware.

Um plano de backup eficiente responde a três perguntas:

- Que tipo de dados meu negócio coleta?
- Com que frequência esses dados mudam?
- Quão seguro é o sistema utilizado para armazená-los?

Pois apenas de posse dessas informações que é possível traçar uma estratégia. Os recursos que não podem faltar em um backup de qualidade, por sua vez, são:

1. automação;
2. planejamento;
3. isolamento.

Para que um backup funcione bem ele precisa estar desconectado de sua máquina atual, já que dispositivos USB podem ser comprometidos com facilidade no caso de um ataque. A nuvem é uma ótima opção para isolar seu sistema de backup dos demais arquivos do computador, mas mídias físicas armazenadas fora do local de trabalho também são um método tradicional para executar cópias de segurança.

Adquira proteção

Para garantir a segurança das redes é preciso investir em soluções proativas de segurança, por isso, compre proteção. Firewalls, sistemas de bloqueio de malware para a filtragem do spam, anti-phishing e que detectam intrusões são grandes aliados da sua empresa.

Crie uma cultura de segurança

Salvaguardar em definitivo os seus dados, porém, só será possível com o desenvolvimento de uma cultura de proteção. Afinal, são usuários os responsáveis por manter seguros os dados de uma empresa.

Lembre-os constantemente de que é importante não compartilhar informações de login, da necessidade de criar senhas fortes e proíba o compartilhamento de contas. Não arrisque os dados da sua empresa: eles são ativos tão valiosos quanto seu inventário ou equipamentos.

Um negócio pode não funcionar adequadamente sem segurança de redes. Por isso não deixe as portas abertas para cibercriminosos e tome sempre medidas para proteger seus dados.

Se você gostou dessas ideias para aumentar a segurança de redes, assine a newsletter da Alerta Security e receba mais dicas para se proteger na internet!

Segurança de rede

No campo de redes, a área de segurança de rede^[11] consiste na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados. Segurança de rede envolve a autorização de acesso aos dados de uma rede, os quais são controlados pelo administrador de rede. Usuários escolhem ou são atribuídos uma identificação e uma senha, ou outra informação de autenticação que permite que eles acessem as informações e programas dentro de sua autorização. A segurança de rede cobre uma variedade de redes de computadores, tanto públicas quanto privadas, que são utilizadas diariamente conduzindo transações e comunicações entre empresas, agências governamentais e indivíduos. Redes podem ser privadas, como as de uma companhia, e outras podem ser abertas para acesso público. Segurança de rede está envolvida em organizações, empresas e outros tipos de instituições. Faz como seu nome sugere: torna a rede segura, assim como protege e supervisiona as operações sendo feitas. A maneira mais comum e simples de proteger um recurso de rede é atribuir um nome único e uma senha correspondente.

Conceitos de Segurança de Rede

Segurança de rede começa com autenticação do usuário, geralmente com um usuário e senha. Já que isto requer apenas um detalhe para autenticar o usuário — a senha, o que é algo que o usuário 'conhece' — isto algumas vezes é chamado de autenticação de um fator. No caso da autenticação de dois fatores, alguma coisa que o usuário 'tem' também é utilizada (por exemplo, um Token, um dongle, um cartão de crédito ou um telefone celular; já em

uma autenticação de três fatores, alguma coisa que o usuário 'é' também é utilizada (impressão digital ou escaneamento de retina).

Uma vez autenticado, um firewall aplica políticas de acesso, como os serviços que são permitidos a serem acessados pelos usuários da rede.^[2] Embora efetivo na prevenção de acesso não autorizado, este componente pode falhar na checagem de conteúdo potencialmente perigoso, como worms ou Trojans sendo transmitido pela rede. Um software Antivírus ou um Sistema de prevenção de intrusos '(IPS - Intrusion Prevention System)^[3] ajudam a detectar e inibir as ações deste tipo de malwares. Um Sistema de Detecção de Intrusão baseado em anomalias também pode monitorar a rede e o tráfego de rede, procurando por um conteúdo ou comportamento inesperado (suspeito) e outras anomalias para proteger os recursos de, mas não limitado a, um ataque de negação de serviço ou um empregado acessando arquivos em horários estranhos. Eventos individuais que acontecem na rede podem ser registrados para serem auditados e para análises posteriores de alto nível.

A comunicação entre dois hospedeiros utilizando uma rede pode ser encriptada para manter sua privacidade.

A segurança de rede envolve diversas áreas, onde as principais são:

- Criptografia de Chaves Públicas
- Vulnerabilidade em Máquinas de Sistemas Distribuídos
- Vulnerabilidade em Redes Locais e de Grande Escala
- Firewalls
- Sistemas de Detecção de Intrusões - IDS
- Redes Privadas Virtuais ('Virtual Private Network')
- Segurança em Redes Sem Fios
- Controle de roteamento

A Segurança de rede pode ser implementada com o uso de vários mecanismos, como por exemplo:

- Assinatura digital
- Autenticação

- Controle de acesso
- Rótulos de segurança
- Detecção, registro e informe de eventos
- Enchimento de tráfego
- controle de enchimento

Navegador web

Um navegador de rede, navegador web, navegador da internet ou simplesmente navegador (em inglês: Web browser, browser), é um programa que habilita seus usuários a interagirem com documentos HTML hospedados em um servidor da rede. Tem destacada relevância na era da *web 2.0*, uma vez que quase tudo do que se necessita está *online*.

Tim Berners-Lee, que foi um dos pioneiros no uso do hipertexto como forma de compartilhar informações, criou o primeiro navegador, chamado WorldWideWeb (www), em 1990. Mais tarde, para não confundir-se com a própria rede, trocou de nome para Nexus. A web, entretanto, só explodiu realmente em popularidade com a introdução do NCSA 'Mosaic, que era um navegador gráfico (em oposição a navegadores de modo texto) rodando originalmente no Unix, mas que foi também portado para o Macintosh e Microsoft Windows logo depois. A versão 1.0 foi liberada em setembro de 1993. Marc Andreessen, o líder do projeto Mosaic na NCSA, demitiu-se para formar a companhia que seria conhecida mais tarde como Netscape Communications Corporation.

História

Os primeiros navegadores exibiam apenas texto (exemplo: imagem ao lado), no decorrer do tempo foram inseridas novas funcionalidades.

Com o advento da *Internet*, o conhecimento gerado por todos os seus usuários ganhou uma nova forma de ser exibida e gerada, ampliou-se o campo da informação. A ferramenta mais popular de visualização de informações disponíveis na internet é o navegador. Com o advento das rede sociais o

usuário dos navegadores passaram a ser um dos grandes geradores de informação, por exemplo facebook, twitter ..

Logo o navegador é uma ferramenta que nos auxilia a visualizar e gerar conteúdo na internet. Os navegadores atuais são compostos por diversos componentes. Na linguagem de informática o navegador é um *software*.

Personagens desta história

Tim Berners-Lee, que foi um dos pioneiros no uso do hipertexto como forma de compartilhar informações, criou o primeiro navegador, chamado WorldWideWeb, em 1990. Ele ainda o introduziu como ferramenta entre os seus colegas do CERN em Março de 1991. E tem sido intrinsecamente ligado ao desenvolvimento da própria *Web*.

A *Web*, entretanto, só explodiu realmente em com a introdução do NCSA Mosaic, que era um navegador gráfico (em oposição a navegadores de modo texto) rodando originalmente no Unix, mas que foi também portado para o Apple Macintosh e Microsoft Windows logo depois. A versão 1.0 do Mosaic foi lançada em setembro de 1993. Marc Andreessen, o líder do projeto Mosaic na NCSA, demitiu-se e fundou a Netscape Communications.

A Netscape lançou o seu produto líder Navigator em outubro de 1994, e este tornou-se o mais popular navegador no ano seguinte. A Microsoft, que até então havia ignorado a *Internet*, entrou na briga com o seu Internet Explorer, comprado às pressas da Spyglass Inc. Isso marca o início da Guerra dos navegadores, que foi a luta pelo mercado dessas aplicações entre a gigante Microsoft e a companhia menor largamente responsável pela popularização da *Web*, a Netscape.

O Opera, um navegador rápido e pequeno, popular principalmente em Compu1996 e permanece um produto de nicho no mercado de navegadores para os computadores pessoais (*PC*).

Essa disputa colocou a *Web* nas mãos de milhões de usuários ordinários do *PC*, mas também mostrou como a comercialização da *Web* podia arruinar os esforços de padronização. Tanto a Microsoft como a Netscape deliberadamente incluíram extensões proprietárias ao HTML em seus produtos, e tentaram ganhar superioridade no mercado através dessa diferenciação. A

disputa terminou em 1998 quando ficou claro que a tendência no declínio do domínio de mercado por parte da Netscape era irreversível. Isso aconteceu, em parte, pelas ações da Microsoft no sentido de integrar o seu navegador com o sistema operacional e o empacotamento do mesmo com outros produtos por meio de acordos OEM; a companhia acabou enfrentando uma batalha legal em função das regras antitruste do mercado norte-americano.

A Netscape respondeu liberando o seu produto como código aberto, criando o Mozilla. O efeito foi simplesmente acelerar o declínio da companhia, por causa de problemas com o desenvolvimento do novo produto. A companhia acabou comprada pela AOL no fim de 1998. O Mozilla, desde então, evoluiu para uma poderosa suíte de produtos Web com uma pequena mas firme parcela do mercado.

O Lynx Browser permanece popular em certos mercados devido à sua natureza completamente textual.

Apesar do mercado para o Macintosh ter sido tradicionalmente dominado pelo Internet Explorer e pelo Netscape Navigator, o futuro parece pertencer ao próprio navegador da Apple Inc., o Safari, que é baseado no mecanismo de renderização KHTML, parte do navegador de código aberto Konqueror. O Safari é o navegador padrão do Mac OS X.

Em 2003, a Microsoft anunciou que o Internet Explorer não seria mais disponibilizado como um produto separado, mas seria parte da evolução da plataforma Windows, e que nenhuma versão nova para o Macintosh seria criada.

Expectativas para o futuro

Em 2008, a W3C anunciou a especificação do HTML5, que entre outras, muda a forma de "execução e funcionamento" dos navegadores, fazendo com que os mesmos não mais executem as linhas de comandos em HTML, buscando os recursos agregados (arquivos contendo dados e informações, ou mesmo, configurações adicionais de funcionamento), atrelando programas adicionais à sua execução (como plugin), e como ocorre atualmente, limitando o acesso a alguns conteúdos da Web, que ficam "amarrados" a programas de terceiros

(outras empresas). Assim sendo, a especificação HTML5 propicia uma liberdade incondicional do navegador, transformando-o de mero "exibidor e agregador" em um "programa on-line", que contém as especificações (comandos) de forma única, não sendo necessário o complemento de outros recursos e ferramentas. Excetuando-se o IE8, todos os demais navegadores já contêm o algoritmo que os torna "compatíveis" com a especificação HTML5.

Características

Os principais navegadores possuem características em comum na interface tais como: voltar para a página anterior, ir para página posterior, recarregar (*refresh*) a página atual, espaço para digitar a URL, estratégias para escolher sites favoritos e o conceito de abas (entre outros). Uma outra característica comum entre eles é apresentar um histórico dos *sites* navegados ao longo do tempo.

Diferentes navegadores podem ser distinguidos entre si pelas características que apresentam. Navegadores modernos e páginas *Web* criadas mais recentemente tendem a utilizar muitas técnicas que não existiam nos primórdios da *Web*. Como notado anteriormente, as disputas entre os navegadores causaram uma rápida e caótica expansão dos próprios navegadores e padrões da *World Wide Web*. A lista a seguir apresenta alguns desses elementos e características:

- ActiveX
- Bloqueio de anúncios
- Preenchimento automático de URLs e dados de formulário
- Bookmarks (marcações, favoritos) para manter uma lista de locais freqüentemente acessados
- Suporte a CSS
- Suporte a cookies, que permitem que uma página ou conjunto de página rastreie usuários
- Cache de conteúdo Web
- Certificados digitais
- Gerenciamento de downloads

- DHTML e XML
- Imagens embutidas usando formatos gráficos como GIF, PNG, JPEG e SVG
- Flash
- Favicons
- Fontes, (tamanho, cor e propriedades)
- Histórico de visitas
- HTTPS
- Integração com outras aplicações
- Navegação offline
- Applets Java
- JavaScript para conteúdo dinâmico
- Plugins
- Tabbed browsing
- Modo anônimo de navegação
- Verificador de spyware

Protocolos e padrões

Eles comunicam-se geralmente com servidores da rede (podendo hoje em dia se comunicar com vários tipos de servidores), usando principalmente o protocolo de transferência de hipertexto HTTP para efetuar pedidos a ficheiros ou arquivos, e processar respostas vindas do servidor. Estes arquivos, são por sua vez identificados por um URL.

O navegador, tem a capacidade de ler vários tipos de arquivos, sendo nativo o processamento dos mais comuns (HTML, XML, JPEG, GIF, PNG, etc.), e os restantes possíveis através de plugins (Flash, Java, etc.).

Os navegadores tem a capacidade de trabalhar também com vários outros protocolos de transferência.

A finalidade principal do navegador é fazer-se o pedido de um determinado conteúdo da *Web* e providenciar a exibição do mesmo. Geralmente, quando o processamento do ficheiro não é possível através do mesmo, este apenas

transfere o ficheiro localmente. Quando se trata de texto (Markup Language e/ou texto simples) e/ou imagens bitmaps, o navegador tenta exibir o conteúdo.

Os primeiros navegadores suportavam somente uma versão mais simples de HTML. O rápido desenvolvimento do mercado de navegadores levou à criação de dialetos não padronizados do HTML, causando problemas de interoperabilidade na Web. Navegadores mais modernos (tais como o Mozilla Firefox, Opera, Google Chrome, Apple Safari e Microsoft Internet Explorer) suportam versões padronizadas das linguagens HTML e XHTML (começando com o HTML 4.01), e mostram páginas de uma maneira uniforme através das plataformas em que rodam.

Alguns dos navegadores mais populares incluem componentes adicionais para suportar Usenet e correspondência de e-mail através dos protocolos NNTP e SMTP, IMAP e POP3 respectivamente.

Segurança

Hoje em dia, a maioria suporta protocolo de transferência de hipertexto seguro (HTTPS) [identificado no browser por um cadeado fechado] e oferecem uma forma rápida e fácil para deletar cache da web, cookies e histórico.

Com o crescimento e as inovações das técnicas de invasões e infecções que existem na *Internet*, torna-se cada vez mais necessária segurança nos navegadores. Atualmente eles são "obrigados" a possuir proteções contra *scripts* maliciosos, entre outros conteúdos maliciosos que possam existir em páginas web acessadas.

Podemos destacar o esforço da W3C (principal organização de padronização da rede mundial de computadores) com o CSP - Content Security Policy (em inglês ou "Política de Segurança do Conteúdo" tradução livre). O CSP destina-se a ajudar os criadores da Web ou os administradores de servidores a especificar como o conteúdo interage nos seus sites.

Tipo de ameaça	Descrição
XSS - Cross-site scripting	Tipo de vulnerabilidade do sistema de segurança de um computador, encontrado normalmente em <u>aplicações web</u> que activam ataques maliciosos ao injectarem <u>client-side script</u> dentro das páginas web vistas por outros usuários.
Framekiller (em inglês)	Técnica usada como parte de um ataque de "furto de click".

A segurança dos navegadores gera disputa entre eles em busca de mais segurança. Sua proteção tem que ser sempre atualizada, pois com o passar do tempo, surgem cada vez mais novas técnicas para burlar os sistemas de segurança dos navegadores.

Como os navegadores funcionam: bastidores dos navegadores modernos

Navegadores da web são provavelmente os softwares mais amplamente utilizados. Nesta cartilha, explicarei como eles funcionam nos bastidores. Veremos o que acontece desde quando você digita google.com na barra de endereço até quando a página do Google é exibida na tela de seu navegador.

Os navegadores sobre os quais falaremos

Atualmente, existem quatro principais navegadores em uso: Internet Explorer, Firefox, Safari, Google Chrome e Opera. Os exemplos dados serão relacionados aos navegadores em código aberto – Firefox, Google Chrome e Safari (que é parcialmente em código aberto). Conforme as estatísticas de navegadores StatCounter (link em inglês), atualmente (em agosto de 2011), a parcela de uso do Firefox, do Safari e do Google Chrome em conjunto é de quase 60%. Isso significa que hoje em dia os navegadores em código aberto são parte substancial do negócio de navegação.

A funcionalidade principal do navegador

A funcionalidade principal de um navegador é apresentar o recurso da web escolhido por você por meio de uma solicitação ao servidor e exibição na janela do navegador. O recurso geralmente é um documento HTML, mas também pode ser um PDF, uma imagem ou outro tipo de arquivo. O local desses recursos é especificado pelo usuário por meio de um URI (Identificador Uniforme de Recursos).

A forma como o navegador interpreta e exibe arquivos HTML é apresentadas nas especificações de HTML e CSS. Essas especificações são mantidas pelo W3C(Consórcio World Wide Web), a organização que controla os padrões para a web.

Por muitos anos, os navegadores mantiveram-se parcialmente de acordo com

as especificações e desenvolveram as próprias extensões. Isso causou sérios problemas de compatibilidade para autores da web. Hoje a maioria dos navegadores está relativamente de acordo com as especificações.

As interfaces do usuário dos navegadores têm muito em comum. Entre os elementos comuns às interfaces do usuário estão:

- Barra de endereço para inserção do URI
- Botões voltar e avançar
- Opções para adicionar favoritos
- Botões atualizar e parar para atualizar e parar o carregamento dos documentos atuais
- Botão Início que o leva à página inicial

Estranhamente, a interface do usuário do navegador não está em nenhuma especificação formal. Ela é resultado de boas práticas moldadas ao longo de anos de experiência e da influência de um navegador sobre outro. A especificação HTML5 não define os elementos de interface do usuário que um navegador deve possuir, mas lista alguns elementos comuns. Entre eles estão a barra de endereço, a barra de status e a barra de ferramentas. Existem, é claro, recursos exclusivos de cada navegador, como o gerenciador de downloads do Firefox.

A estrutura de nível superior do navegador

Os principais componentes do navegador são (1.1):

1. **A interface do usuário**, que inclui a barra de endereço, o botão voltar/avançar, o menu de favoritos, etc. Todas as áreas do display do navegador, exceto a janela principal em que você visualiza a página solicitada.
2. **O mecanismo de navegação**, que faz a triagem das ações entre a interface do usuário e o mecanismo de renderização.
3. **O mecanismo de renderização**, responsável pela exibição do conteúdo solicitado. Por exemplo, se o conteúdo solicitado estiver em HTML, ele é responsável pela análise do HTML e do CSS e pela exibição do conteúdo analisado na tela.

4. **Networking**, utilizado para chamadas de rede, como solicitações HTTP. Possui interface independente de plataforma e sub-implementações para cada plataforma.
5. **Back-end da interface do usuário**, utilizada para desenhar widgets básicos como caixas de combinação e janelas. Exibe uma interface genérica que não é específica à plataforma. Sob a interface, utiliza os métodos da interface do usuário do sistema operacional.
6. **Intérprete JavaScript** Utilizado para analisar e executar o código JavaScript.
7. **Armazenamento de dados**. Esta é uma camada persistente. O navegador precisa salvar dados de diversos tipos no disco rígido, como cookies. A nova especificação HTML (HTML5) define "banco de dados da web", que é um banco de dados completo (embora leve) no navegador.

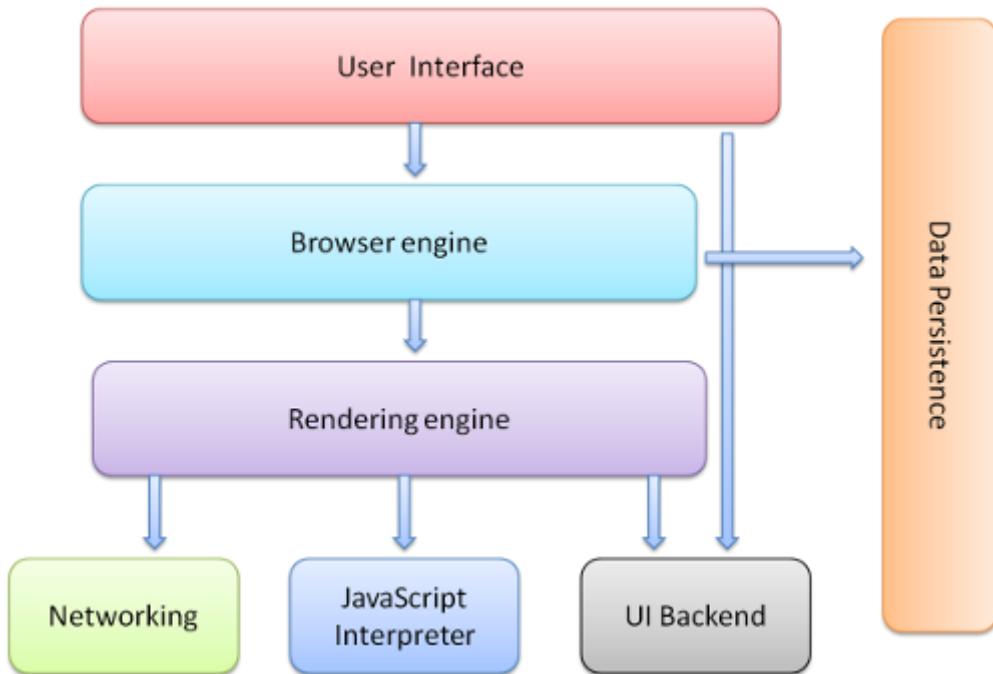


Ilustração : principais componentes do navegador.

O Google Chrome, diferente da maioria dos navegadores, mantém múltiplas instâncias do mecanismo de renderização, uma para cada guia. Cada guia é um processo independente.

O mecanismo de renderização

A responsabilidade do mecanismo de renderização é, claro, renderizar, ou seja, exibir os conteúdos solicitados na tela do navegador.

Por padrão, o mecanismo de renderização pode exibir documentos e imagens HTML e XML. Ele pode exibir outros formatos por meio de plug-ins (ou extensões do navegador). Por exemplo, é possível exibir um PDF por meio de um plug-in do navegador para visualização de PDFs. No entanto, neste capítulo, nosso foco estará no uso principal: a exibição de HTML e de imagens formatadas com CSS.

Mecanismos de renderização

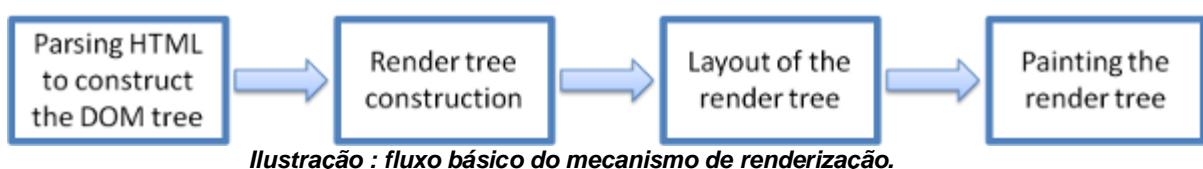
Nossos navegadores de referência – Firefox, Google Chrome e Safari – foram construídos com base em dois mecanismos de renderização. O Firefox utiliza o Gecko, um mecanismo de renderização criado pelo próprio Mozilla. O Safari e o Google Chrome usam o Webkit.

O Webkit é um mecanismo de renderização em código aberto que começou como um mecanismo para a plataforma Linux e foi modificado pela Apple para ser compatível com os sistemas Mac e Windows. Consulte webkit.org (link em inglês) para obter mais detalhes.

O fluxo principal

O mecanismo de renderização inicia pela obtenção do conteúdo do documento solicitado a partir da camada de rede. Isso geralmente é feito em parcelas de 8 KB.

Em seguida, o fluxo básico do mecanismo de renderização:



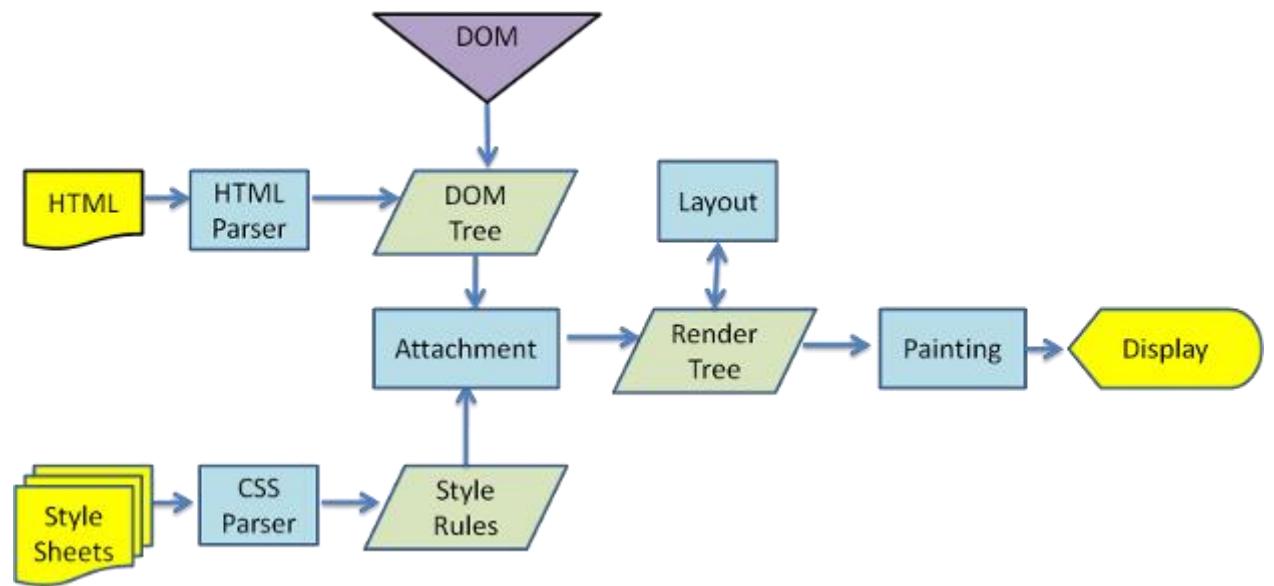
O mecanismo de renderização inicia a análise do documento HTML e transformará as tags em nós DOM de uma árvore chamada "árvore de conteúdo". Ele analisa os dados de estilo nos arquivos externos CSS e nos elementos de estilo. As informações de estilo, aliadas às instruções visuais no HTML são utilizadas para criar outra árvore, a árvore de renderização.

A árvore de renderização contém retângulos com atributos visuais como cor e dimensões. Os retângulos estão na ordem correta para serem exibidos na tela.

Após a construção da árvore de renderização, ela passa por um processo de "layout". Isso significa dar a cada nó as coordenadas exatas de onde ele deve ser exibido na tela. A próxima etapa é a pintura. A árvore de renderização será atravessada e cada nó será pintado usando a camada de back-end da interface do usuário.

É importante entender que este é um processo gradual. Para uma melhor experiência do usuário, o mecanismo de renderização tenta exibir conteúdos na tela assim que possível. Ele não espera que todo o HTML seja analisado para começar a construir e fazer o layout da árvore de renderização. Partes de conteúdo são analisadas e exibidas, enquanto o processo continua para o restante do conteúdo recebido da rede.

Principais exemplos de fluxo



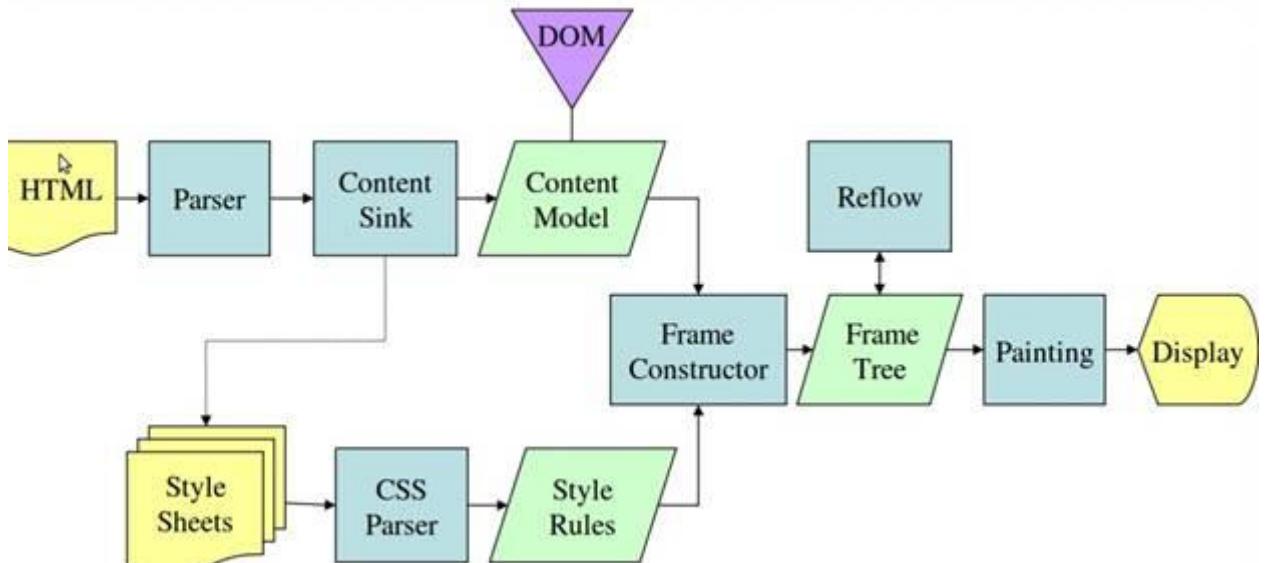


Ilustração : fluxo principal do mecanismo de renderização Gecko(3.6)

As ilustrações 3 e 4 mostram que, embora o Webkit e o Gecko usem terminologias diferentes, o fluxo é basicamente o mesmo.

O Gecko nomeia a árvore de elementos formatados visualmente "Árvore de molduras". Cada elemento é uma moldura. O Webkit usa o termo "Árvore de renderização", que é formada por "Objetos de renderização". O Webkit utiliza o termo "layout" para a disposição dos elementos, enquanto o Gecko utiliza "Redimensionamento". "Attachment" é o termo do Webkit para conectar nós DOM e informações visuais para criar a árvore de renderização. Uma pequena diferença não-semântica é que o Gecko tem uma camada adicional entre o HTML e a árvore DOM. Essa camada se chama "coletor de conteúdo" e é uma fábrica para a criação de elementos DOM.

Como funciona a Internet?

A Internet é uma grande rede de computadores, roteadores e outros elementos que têm como objetivo levar a informação de uma localidade à outra. Sob o ponto de vista de tráfego de informação, podemos dividir a rede em core (núcleo) e acesso, como mostra a figura 1.2.

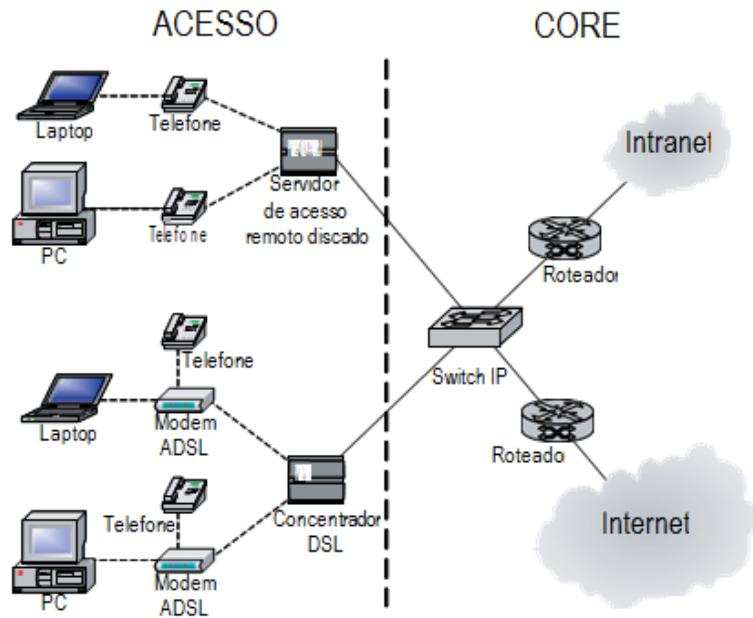


Figura 1.2 – Acesso e core.

Core é a parte da rede onde trafegam grandes volumes de informação, onde se concentram os dados dos diversos usuários para encontrar o caminho dos pacotes até seu destino. Nele constam roteadores de grandes capacidades com velocidades que atingem vários gigabits por segundo (num futuro próximo deverão atingir até terabits por segundo).

Acesso é o ponto da rede por onde os usuários se conectam a ela. No acesso é que se encontram os modems, as linhas telefônicas, os roteadores de menor capacidade, os modems ADSL e outros elementos que têm como função levar a informação da casa do usuário até a Internet.

Como as informações são enviadas para a direção correta dentro da Internet? Como conseguimos acessar um computador ou um site específico, dentre milhões de opções? A resposta está no protocolo TCP/IP (Transmission Control/Internet Protocol).

O protocolo TCP/IP é o responsável por garantir a conectividade entre os milhões de usuários da Internet. Por meio dos endereços IPs que os roteadores montam suas tabelas de rotas e conseguem enviar as informações para a direção correta.

Um endereço IP é constituído de 4 bytes. Cada um desses 4 bytes tem o valor definido entre 0 a 255 (em hexadecimal 0 a FF). Por exemplo, o endereço 192.168.0.100 é um IP.

Quando entramos na Internet, recebemos um endereço IP do nosso provedor. Esse endereço é único em toda a rede, ou seja, apenas você o estará usando naquele instante. Cada provedor tem um intervalo único de IPs para ser usado, os quais serão distribuídos ao seus usuários conforme a necessidade.

Para montar e atualizar as tabelas de roteamento, os roteadores usam os chamados protocolos de roteamento, cujos principais nomes são RIP (Routing Information Protocol), OSPF (Open Shortest Path First) e BGP (Border Gateway Protocol).