

1) Tom, você poderia nos explicar o que é internet?

A Internet é um conglomerado de redes em escala mundial de milhões de computadores interligados pelo Protocolo de Internet (TCP/IP) que permite o acesso a informações e todo tipo de transferência de dados. Ao contrário do que normalmente se pensa, Internet não é sinônimo de World Wide Web (WWW). Esta é parte daquela, sendo a World Wide Web, que utiliza hipermídia na formação básica, um dos muitos serviços oferecidos na Internet. De acordo com dados de março de 2007, a Internet é usada por 16,9% da população mundial (em torno de 1,1 bilhão de pessoas).

2) Esse mundo de siglas me deixa confuso(a). Se internet é um conglomerado de redes, o que vem a ser PAN, LAN, MAN, WAN?

PAN - Rede de área pessoal, tradução de Personal Area Network, é uma tecnologia de rede formada por nós muito próximos uns dos outros (geralmente não mais de uma dezena de metros). Por exemplo, um computador portátil conectando-se a um outro e este a uma impressora. São exemplos de PAN as redes do tipo Bluetooth¹ e IR.

LAN - rede de área local (ou LAN, acrônimo de local area network) é uma rede de computador utilizada na interconexão de equipamentos processadores com a finalidade de troca de dados. Um conceito mais definido seria: é um conjunto de hardware e software que permite a computadores individuais estabelecerem comunicação entre si, trocando e compartilhando informações e recursos. Tais redes são denominadas locais por cobrirem apenas uma área limitada (10 Km no máximo, quando passam a ser denominadas **MANs**), visto que, fisicamente, quanto maior a distância de um nó da rede ao outro, maior a taxa de erros que ocorrerão devido à degradação do sinal.

As LANs são utilizadas para conectar estações, servidores, periféricos e outros dispositivos que possuam capacidade de processamento em uma casa, escritório, escola e edifícios próximos.

MAN - MAN (Metropolitan Área Network): É o nome dado às redes que ocupam o perímetro de uma cidade. São mais rápidas e permitem que empresas com filiais em bairro diferentes se conectem entre si.

A partir do momento que a internet atraiu uma audiência de massa, as operadoras de redes de TV a cabo, começaram a perceber que, com algumas mudanças no sistema, elas poderiam oferecer serviços da Internet de mão dupla em partes não utilizadas do espectro. A televisão a cabo não é a única MAN. Os desenvolvimentos mais recentes para

¹ **Bluetooth** é uma especificação industrial para áreas de redes pessoais sem fio. O Bluetooth provém uma maneira de conectar e trocar informações entre dispositivos como telefones celulares, notebooks, computadores, impressoras, câmeras digitais e consoles de videogames digitais através de uma frequência de rádio de curto alcance.

Classe	Potência máxima permitida (mW/dBm)	Alcance (Aproximadamente)
Classe 1	100 mW (20 dBm)	~ 100 metros
Classe 2	2.5 mW (4 dBm)	~ 10 metros
Classe 3	1 mW (0 dBm)	~ 1 metro

Versão	Taxa de transmissão
Versão 1.2	1 Mbit/s
Versão 2.0 + EDR	3 Mbit/s
Versão 3.0 (Em desenvolvimento)	53 - 480 Mbit/s (Proposto)

acesso à internet de alta velocidade sem fio resultaram em outra MAN, que foi padronizada como IEEE 802.16².

WAN - A Wide Area Network ou Rede de longa distância, também conhecida como Rede geograficamente distribuída, é uma rede de computadores que abrange uma grande área geográfica, com frequência um país ou continente. Difere, assim, das PAN, das LAN e das MAN. As WAN tornaram-se necessárias devido ao crescimento das empresas, onde as LAN não eram mais suficientes para atender a demanda de informações, pois era necessária uma forma de passar informação de uma empresa para outra de forma rápida e eficiente. Surgiram as WAN que conectam redes dentro de uma vasta área geográfica, permitindo comunicação de longa distância.

3) Poxa, parece que uma coisa puxa outra. Esses dias, fazendo uma prova encontrei o termo WLAN. Seria isso uma rede de longo alcance junto com uma rede local?

Não. O termo WLAN significa Wireless Local Area Network, ou seja, uma rede local sem fio. O padrão mais usado é o IEEE 802.11, também conhecido como Wi-Fi (Fidelidade sem fio).

802.11a = 54Mbps

802.11b = 11Mbps

802.11g = 54Mbps

4) Mudando um pouco de assunto, você nos disse que o protocolo usado na internet é o TCP/IP, ele é da Microsoft?

Não! O TCP/IP é o protocolo padrão da internet desde 1982. E foi criado tomando como base um modelo da ISO (**International Organization for Standardization**) chamado OSI (**Open Systems Interconnection**) e é baseado em camadas.

Camada	Protocolo
5. Aplicação	HTTP, SMTP, FTP, SSH, RTP, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS, Ping ...
4. Transporte	TCP, UDP, SCTP, DCCP ...
3. Rede	IP (IPv4, IPv6), ARP, RARP, ICMP, IPsec ...
2. Enlace	Ethernet, 802.11 WiFi, IEEE 802.1Q, 802.11g, HDLC, Token ring, FDDI, PPP, Frame Relay,
1. Física	Modem, RDIS, RS-232, EIA-422, RS-449, Bluetooth, USB, ...

Hoje o protocolo TCP/IP é gerenciado por um consórcio de empresas chamado W3C (World Wide Web Consortium).

As camadas mais próximas do topo estão logicamente mais perto do usuário, enquanto aquelas mais abaixo estão logicamente mais perto da transmissão física do dado. Cada camada tem um protocolo de camada acima e um protocolo de camada abaixo (exceto as camadas da ponta,

obviamente) que podem usar serviços de camadas anteriores ou fornecer um serviço, respectivamente.

Vamos aqui aos principais protocolos usados na internet e suas respectivas camadas.

CAMADA DE REDE

IP - "Internet Protocol" (ou Protocolo de Internet), que é um protocolo usado entre duas ou mais máquinas em rede para encaminhamento dos dados.

Os dados numa rede IP são enviados em blocos referidos como **pacotes** ou **datagramas**.

² 802.16 (WiMax) - Worldwide Interoperability for Microwave Access - O WiMax é uma tecnologia de rádio que permite o acesso à Internet em banda larga, com um raio de cobertura superior ao garantido pelo Wi-Fi e que alguns especialistas consideram potencial substituto do DSL, sobretudo para cobrir zonas remotas. Séria concorrente da telefonia celular 3G.

O IP oferece um serviço de datagramas não confiável (também chamado de melhor esforço); ou seja, o pacote vem quase sem garantias. O pacote pode chegar desordenado (comparado com outros pacotes enviados entre os mesmos hosts), também podem chegar duplicados, ou podem ser perdidos por inteiro. Se a [aplicação](#) precisa de confiabilidade, esta é adicionada na [camada de transporte](#).

Os [roteadores](#)³ são usados para reencaminhar datagramas IP através das redes interconectadas. O IP é o elemento comum encontrado na [internet](#) pública dos dias de hoje. Temos duas versões atualmente do protocolo IP; a versão 4, ou IPv4, que usa endereços de 32 bits. O [IPv6](#) tem endereçamento de origem e destino de 128 bits, oferecendo mais endereçamentos que os 32 bits do IPv4.

Ex.

200.221.2.45

3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344

ICMP - Internet Control Message Protocol, é utilizado para fornecer relatórios de erros à fonte original. Qualquer [computador](#) que utilize IP precisa aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado. Os [gateways](#) devem estar programados para enviar mensagens ICMP quando receberem [datagramas](#) que provoquem algum erro.

As mensagens ICMP geralmente são enviadas automaticamente em uma das seguintes situações:

Um pacote [IP](#) não consegue chegar ao seu destino (i.e. Tempo de vida do pacote expirado)

O [Gateway](#) não consegue retransmitir os pacotes na frequência adequada (i.e. Gateway congestionado)

O [Roteador](#) ou [Encaminhador](#) indica uma rota melhor para a máquina a enviar pacotes.

Ferramenta comumente usada baseada nesse protocolo: [Ping](#).

CAMADA DE TRANSPORTE

TCP - (Transmission Control Protocol) é um dos protocolos sob os quais assenta o núcleo da Internet nos dias de hoje. A versatilidade e robustez deste protocolo tornou-o adequado para redes globais, já que este verifica se os dados são enviados de forma correta, na sequência apropriada e sem erros, pela rede. É chamado de protocolo confiável e é orientado a conexão.

UDP - O protocolo UDP é normalmente utilizado por aplicações que exigem um transporte rápido e contínuo de dados entre equipamentos. Enquanto no protocolo TCP é dado prioridade à conexão e a chegada correta dos dados no ponto de destino, o UDP não verifica o recebimento e a integridade dos dados enviados. Por consequência, existe a possibilidade de que, eventualmente, as informações transmitidas sejam recebidas de forma incorreta ou mesmo não cheguem ao destinatário. Entretanto, a maior simplicidade do UDP faz com que este protocolo apresente ganhos na velocidade de transmissão e recepção de dados, algo que nos dias atuais se torna cada vez mais importante. É conhecido como protocolo não confiável.

CAMADA DE APLICAÇÃO

³ Equipamento usado para a interligação de redes. Usam endereços IP e são capazes de escolher a melhor rota para os pacotes IP entre o host (servidor) e o cliente.

DNS - Domain Name System ou Sistema de Nomes de Domínios é um sistema de gerenciamento de nomes hierárquico operando segundo duas definições:

- Examinar e atualizar seu banco de dados.
- Resolver nomes de servidores em endereços de rede (IPs).

O servidor DNS traduz nomes para os endereços IP e endereços IP para nomes respectivos, e permitindo a localização de hosts em um domínio determinado.

No Brasil, o registro de domínios é feito pelo NIC (Núcleo de Informação e Coordenação - <http://nic.br>).

FTP - File Transfer Protocol (Protocolo de Transferência de Arquivos), e é uma forma bastante rápida e versátil de transferir arquivos, sendo uma das mais usadas na internet.

Pode referir-se tanto ao protocolo quanto ao programa que implementa este protocolo (Cliente FTP).

A transferência de dados em redes de computadores envolve normalmente transferência de arquivos e acesso a sistemas de arquivos remotos (com a mesma interface usada nos arquivos locais). O FTP é baseado no TCP. É o padrão da pilha TCP/IP para transferir arquivos, é um protocolo genérico independente de hardware e do sistema operacional e transfere arquivos por livre arbítrio, tendo em conta restrições de acesso e propriedades dos mesmos.

TELNET e SSH - Protocolos usados para acesso a máquinas remotas.

SMTP - Simple Mail Transfer Protocol é o protocolo padrão para envio de e-mails através da Internet (através de programas cliente de e-mail).

SMTP é um protocolo relativamente simples, baseado em texto simples, onde um ou vários destinatários de uma mensagem são especificados (e, na maioria dos casos, validados) sendo, depois, a mensagem transferida ao servidor.

MIME - Multipurpose Internet Mail Extensions ou Extensões Multi função para Mensagens de Internet. É uma norma da internet para o formato das mensagens de correio eletrônico. A grande maioria das mensagens de correio eletrônico são trocadas usando o protocolo SMTP e usam o formato MIME. As mensagens na Internet tem uma associação tão estreita aos padrões SMTP e MIME que algumas vezes são chamadas de mensagens SMTP/MIME.

O protocolo básico de transmissão de e-mail pela Internet, SMTP, suporta apenas 7-bit de caracteres ASCII. Isto limita as mensagens de emails, incluindo somente os caracteres usados na língua inglesa.

O MIME provê mecanismos para o envio de outros tipos de informação por e-mail, incluindo caracteres não utilizados no idioma inglês usando codificações diferentes do ASCII, assim como formatos binários contendo imagens, sons, filmes, e programa de computadores.

POP - O Post Office Protocol (POP3) é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico. O POP3 permite que todas as mensagens contidas numa caixa de correio eletrônico possam ser transferidas seqüencialmente para um computador local. Aí, o utilizador pode ler as mensagens recebidas, apagá-las, responder-lhes, armazená-las, etc.

É chamado de protocolo de coreio off-line.

IMAP - Internet Message Access Protocol é um protocolo de gerenciamento de correio eletrônico superior em recursos ao POP3 - protocolo que a maioria dos provedores oferece aos seus assinantes. A última versão é o IMAP4. O mais interessante é que as mensagens

ficam armazenadas no servidor e o internauta pode ter acesso a suas pastas e mensagens em qualquer computador, tanto por webmail como por cliente de correio eletrônico (como o Outlook Express ou o Thunderbird). Outra vantagem deste protocolo é o compartilhamento de caixas postais entre usuários membros de um grupo de trabalho. Além disso, é possível efetuar pesquisas por mensagens diretamente no servidor, utilizando palavras-chaves.

Tem, no entanto, alguns inconvenientes:

O número de mensagens possível de se armazenar depende do espaço limite que nos é atribuído para a caixa de correio;

Caso o servidor IMAP esteja numa localização remota, pela Internet, e não numa rede local LAN, é necessário estar ligado à Internet todo o tempo que quisermos consultar ou enviar mensagens, podendo não ser adequado a quem utiliza a Internet através de ligação telefônica Dial-up, devido aos custos associados. No entanto, a maioria dos clientes de e-mail oferecem a possibilidade de criar uma cópia local (offline) das mensagens contidas em uma ou várias pastas (Recebidas, Enviadas, etc.). Sendo assim, toda vez que você dispuser de uma conexão (estiver online) sua cópia local será sincronizada com o servidor de e-mail.

HTTP - Hypertext Transfer Protocol, que significa Protocolo de Transferência de Hipertexto) é um protocolo de comunicação (na camada de aplicação segundo o Modelo OSI) utilizado para transferir dados por intranets e pela World Wide Web (WWW).

Normalmente, este protocolo utiliza o porta 80 e é usado para a comunicação de sítios web, comunicando na linguagem HTML.

Para acessarmos um outro documento a partir de uma palavra presente no documento atual podemos utilizar hiperligações (ou hiperlinks). Estes documentos encontram-se em sítios ou sites com um endereço de página da Internet - e para entrarmos neles devemos digitar o respectivo endereço, denominado URL (Universal Resource Locator).

Páginas estáticas – São páginas criadas usando HTML. O conteúdo exibido é o mesmo, independente de quem e onde acesse a página. O processamento dessas páginas é feito no computador do usuário (processamento LOCAL).

Páginas dinâmicas – São páginas criadas em HTML associadas a outras linguagens de programação para internet (as mais usadas são ASP, JAVA, PHP). Possuem conteúdo personalizado e são processadas no SERVIDOR WEB.

5) Tom, estou verdadeiramente fascinado com tudo isso. Esse mundo da informática é encantador, porém surgiu uma dúvida. Onde fica esse SERVIDOR WEB? Ele é um supercomputador nos EUA?

Não. Pelo que vimos anteriormente, a internet é um conglomerado de redes, portanto qualquer computador na internet pode ter um software chamado SERVIDOR WEB instalado, tornando-o um servidor de conteúdo na rede.

Os dois servidores WEB mais usados são:

APACHE – Software livre – 60%

IIS (Internet Information Service) – Microsoft.

6) Tom, acho que você esqueceu um protocolo importante. Sempre que acesso algumas páginas, em vez de aparecer http aparece HTTPS, são iguais?

Olha, iguais não, mas o HTTPS é o HTTP com uma camada de conexão segura (SSL – Security Socket Layer), o que faz com que os dados transmitidos sejam criptografados. Essa criptografia é, normalmente, de 128 bits, o que possibilita uma chave de criptografia com 340.282.366.920.938.000.000.000.000.000.000.000.000 combinações diferentes. Isso não quer dizer que seja impossível um hacker descobrir o que significam os dados, porém desencoraja esse tipo de fraude. Eles preferem usar técnicas de phishing e pharming, que veremos mais tarde.

7) Legal! Notei uma coisa. Olhando no esquema dos protocolos da Internet na página 1 percebi que você não falou nada sobre a camada 1 e 2, foi intencional?

É, realmente falamos da 3, 4 e 5 que são camadas compostas por software (a exceção é o roteador, que está na camada de rede 3ª camada). As camadas 1 e 2 (Física e Enlace), são compostas por hardware e o padrão mais usado é o ETHERNET.

ETHERNET - Ethernet é uma tecnologia de interconexão para [redes locais](#) - Local Area Networks ([LAN](#)) - baseada no envio de pacotes. Ela define cabeamento e sinais elétricos para a [camada física](#), e formato de pacotes e protocolos para a camada de controle de acesso ao meio (Media Access Control - [MAC](#)) do modelo [OSI](#). A Ethernet foi padronizada pelo [IEEE](#) como [802.3](#). A partir dos [anos 90](#), ela vem sendo a tecnologia de LAN mais amplamente utilizada e tem tomado grande parte do espaço de outros padrões de rede como [Token Ring](#), [FDDI](#) e [ARCNET](#). Cada ponto tem uma chave de 48 bits globalmente única, conhecida como endereço MAC, para assegurar que todos os sistemas em uma ethernet tenham endereços distintos.

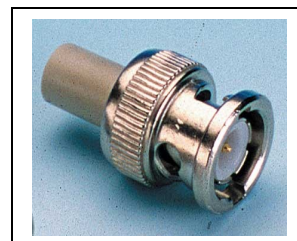
FISICA

É constituída por equipamentos que não possuem nenhum controle do fluxo de dados.

Cabos

- Coaxiais (10base2, 10base5) – impedância 50 OHMS

- Comprimento máximo de 185 metros
- Conectores BNC, BNC T
- Velocidade de transmissão 10 Mbps.

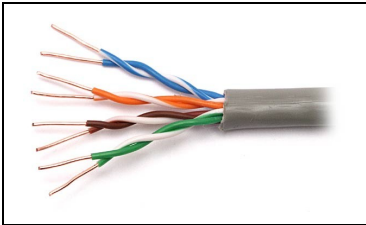


Redes locais montadas com cabos coaxiais normalmente usam uma topologia chamada BARRA ou BARRAMENTO.



- UTP (Par trançado sem blindagem)
- STP (Par trançado blindado)
 - Comprimento máximo é de 100 metros
 - Categorias
 - Cat. 5E – 100baseT - (Fast Ethernet) – 100 Mbps
 - Cat. 6 – 1000baseT - (Gigabit Ethernet) – 1000 Mbps
 - Normas de construção
 - 568A, 568B, Crossover

Conector RJ-45



HUB (Concentrador)

Transmite os pacotes ETHERNET para todos os computadores da rede. Trabalha com os endereços físicos da placa de rede (MAC – Media Access Control).

O Hub é indicado para redes com poucos terminais de rede, pois o mesmo não comporta um grande volume de informações passando por ele ao mesmo tempo devido sua metodologia de trabalho por broadcast, que envia a mesma informação dentro de uma rede para todas as máquinas interligadas. Devido a isto, sua aplicação para uma rede maior é desaconselhada, pois geraria lentidão na troca de informações.

Um concentrador se encontra na primeira camada do modelo OSI, por não poder definir para qual computador se destina a informação, ele simplesmente a replica.

SWITCH (Comutador) - Segmenta a rede. Envia os pacotes ETHERNET somente para a máquina que possua o endereço MAC correto. Um comutador opera na camada 2 (camada de enlace), encaminhando os pacotes de acordo com o [endereço MAC](#) de destino, e é destinado a [redes locais](#) para segmentação.



Satisfeita?

8) Sim, Então quer dizer que internet e Ethernet são coisas diferentes né? E Intranet, o que é?

Sim, você está certa. Internet é a reunião de milhões de redes usando um protocolo em comum, já ethernet e a tecnologia usada na fabricação de equipamentos para uma LAN que usa a metodologia de fragmentar a informação em pacotes.

Então você quer saber o que é intranet? Você se lembra o que é um servidor web?

Então, uma intranet é quando eu instalo um servidor web em um computador, desenvolvo e hospedo páginas nesse servidor e limito o acesso à minha rede local. Ou seja, uma intranet usa os mesmos recursos da internet, porém o acesso é apenas local.

As principais vantagens são:

- Compatibilidade de software – Sistemas operacionais diferentes apresentam muitas incompatibilidades. Como na intranet os programas da empresa são feitos normalmente com páginas dinâmicas o processamento vai ser feito pelo servidor web local, cabendo aos usuários terem em suas máquinas apenas um navegador/Browser (Internet Explorer, Mozilla Firefox ou outro) para exibir os dados processados.
- Compatibilidade de hardware – Pelo fato do processamento ser feito no servidor, as máquinas pertencentes à intranet não precisam ser tão potentes, aproveitando melhor máquinas mais antigas.

9) Tom, estou achando que vou mudar de profissão! Surgiu mais uma dúvida. Seria possível conectar a Intranet da regional Goiás com a Intranet da Regional Minas Gerais, por exemplo para troca de informações sobre presos?

Sim, é possível. O nome que damos a isso é EXTRANET. Grandes empresas contratam linhas dedicadas para esse fim. Pequenas empresas ou usuários domésticos podem fazer isso usando a própria internet, através de uma VPN.

VPN - Uma Rede Particular Virtual (Virtual Private Network) é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a [Internet](#)). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros.

VPNs seguras usam protocolos de [criptografia](#) por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

10) Recentemente vi, no Jornal da Globo, uma entrevista de um diretor do site Google, onde ele falava sobre um projeto chamado “nas nuvens”; na mesma reportagem falaram sobre WEB 2.0, qual a diferença dela para a WEB normal?

<http://googlediscovery.com/2008/05/08/computacao-nas-nuvens-google-quer-construir-o-futuro-dos-computadores/>

O conceito. No início a web exibia apenas informações estáticas, depois surgiram as páginas dinâmicas, que possibilitam conteúdo personalizado. A grande onda do momento (web 2.0) passa a usar a internet como plataforma para a execução de aplicativos, sem a necessidade de o usuário ter que instalar esses programas em seu computador.

Exemplos de sites que trabalham com o conceito Web 2.0.

<http://internauta20.blogspot.com/2007/06/exemplos.html>

11) Um pouco antes você falou um termo que nunca ouvi. Afinal de contas o que é um browser?

Com o advento da Internet, ampliou-se o campo da informação. A Internet é uma grande teia ou rede mundial de computadores. Para utilizarmos todos os recursos disponíveis nesta imensa ferramenta de informação, necessitamos de um software que possibilite a busca pela informação. Este, é denominado de **navegador** – também conhecido como Web browser ou simplesmente browser, termos em inglês. Em sua epistemologia, browser tem como raiz o verbo to browse, ou seja, olhar páginas de um livro, revista, etc. – um olhar sem propósito particular; exemplificando, como alguém que vai a uma loja, olha tudo, mas sem a intenção explícita de comprar. O Navegador é um programa que habilita seus usuários a interagirem com documentos virtuais, chamados de HTML (linguagem de hipertexto), hospedados em um servidor Web, de acesso à Internet. A sigla www, conhecida como World Wide Web é uma coleção intercalada de documentos de hipertexto, dos quais os documentos HTML são uma substancial fração da imensidão de informações dispostas na Internet.

Os navegadores mais utilizados atualmente são:

- Internet Explorer 6/7

- Mozilla Firefox
- Opera
- Safari

Características dos navegadores

Característica	IE6	IE7	MF2
Navegação por abas/guias	N	S	S
Gerenciador de downloads	N	N	S
Agregador RSS	N	S	S
Extensões e temas	N	N	S
Pluguins	S	S	S
Bloqueador de POPUP	S(SP2)	S	S
Anti-Phishing	N	S	S
Localizar dinâmico	N	N	S
Página inicial multipla	N	S	N
Barra de Pesquisa na web	N	S	S

12) Meu Deus! Quer dizer que podemos pescar na internet?

Não. Phishing, assim como pharming, são técnicas usadas por pessoas mal intencionadas com o objetivo de roubar informações do usuário. Veja os conceitos:

PHISHING - O phishing online (pronuncia-se fichin) é uma maneira de enganar os usuários de computador para que eles revelem informações pessoais ou financeiras através de uma mensagem de email ou site. Um scam típico de phishing online começa com uma mensagem de email que parece uma nota oficial de uma fonte confiável como um banco, uma empresa de cartão de crédito ou um comerciante online de boa reputação. No email, os destinatários são direcionados a um site fraudulento em que são instruídos a fornecer suas informações pessoais, como número de conta ou senha. Em seguida, essas informações são geralmente usadas para o roubo de identidade. Ou seja, explora a ingenuidade dos usuários.

PHARMING – É o termo atribuído ao ataque baseado na técnica [DNS](#) cache poisoning (envenenamento de cache DNS) que, consiste em corromper o [DNS](#) (Sistema de Nomes de Domínio ou Domain Name System) em uma rede de computadores, fazendo com que a [URL](#) (Uniform Resource Locator ou Localizador Uniforme de Recursos) de um site passe a apontar para um servidor diferente do original.

Ao digitar a [URL](#) (endereço) do site que deseja acessar, um banco por exemplo, o servidor [DNS](#) converte o endereço em um número [IP](#), correspondente ao do servidor do banco. Se o servidor DNS estiver vulnerável a um ataque de Pharming, o endereço poderá apontar para uma página falsa [hospedada](#) em outro servidor com outro endereço [IP](#), que esteja sob controle de um golpista.

Os golpistas geralmente copiam fielmente as páginas das instituições, criando a falsa impressão que o usuário está no site desejado e induzindo-o a fornecer seus dados privados como [login](#) ou números de contas e [senha](#) que serão armazenados pelo servidor falso.

13) E RSS, é risadinha no MSN?

Não. É uma sigla que quer dizer Really Simple Syndication ou Distribuição Realmente S imples. A [tecnologia](#) do RSS permite aos [usuários](#) da [internet](#) se inscreverem em sites que fornecem "[feeds](#)" (fontes) RSS. Estes são tipicamente sites que





Mesmo durante uma conversa, se receber um link que não estava esperando, pergunte ao contato se, de fato, ele o enviou. Se ele negar, não clique no link e avise-o de que seu computador pode estar com um vírus.

7 - Cuidado com e-mails falsos

Recebeu um e-mail dizendo que você tem uma dívida com uma empresa de telefonia ou afirmando que um de seus documentos está ilegal, como mostra a imagem abaixo?



Ou, ainda, a mensagem te oferece prêmios ou cartões virtuais de amor? Te intima para uma audiência judicial? Contém uma suposta notícia importante sobre uma personalidade famosa? É provável que se trate de um phishing/scam, ou seja, um e-mail falso. Se a mensagem tiver textos com erros ortográficos e gramaticais, fizer ofertas tentadoras ou tem um link diferente do indicado (para verificar o link verdadeiro, basta passar o mouse por cima dele, mas sem clicar), desconfie imediatamente. Na dúvida, entre em contato com a empresa cujo nome foi envolvido no e-mail.

Acesse os seguintes links para saber como lidar com e-mails falsos:

- [Dicas contra e-mails falsos;](#)
- [Fique atento: scams usam sustos para enganar internautas.](#)

8 - Evite sites de conteúdo duvidoso

Muitos sites contêm em suas páginas scripts capazes de explorar falhas do navegador de internet, principalmente do Internet Explorer. Por isso, evite navegar em sites pornográficos, de conteúdo hacker ou que tenham qualquer conteúdo duvidoso.

9 - Cuidado com anexos de e-mail

Essa é uma das instruções mais antigas, mesmo assim, o e-mail ainda é uma das principais formas de disseminação de vírus. Tome cuidado ao receber mensagens que te pedem para abrir o arquivo anexo, principalmente se o e-mail veio de alguém que você não conhece. Para aumentar sua segurança, você pode checar o arquivo anexo com um antivírus, mesmo quando estiver esperando recebê-lo.

10 - Atualize seu antivírus e seu antispyware

Muita gente pensa que basta instalar um antivírus para o seu computador estar protegido, mas não é bem assim. É necessário atualizá-lo regularmente, do contrário, o antivírus não saberá da existência de vírus novos. Praticamente todos os antivírus disponíveis permitem configurar uma atualização automática. Além disso, use um antispyware com frequência para tirar arquivos e programas maliciosos de seu computador. Uma boa opção é o [Spybot](#). Assim como o antivírus, o antispyware também deve ser atualizado para que este conheça pragas novas.

Em ambos os casos, verifique no manual do software ou no site do desenvolvedor, como realizar as atualizações.

11 - Cuidado ao fazer compras na internet ou usar sites de bancos

Fazer compras pela internet é uma grande comodidade, mas só o faça em sites de venda reconhecidos. Caso esteja interessado em um produto vendido em um site desconhecido, faça uma pesquisa na internet para descobrir se existe reclamações contra a empresa. Um bom serviço para isso é o site [Reclame Aqui](#).

Ao acessar sua conta bancária através da internet, também tenha cuidado. Evite fazer isso em computadores públicos, verifique sempre se o endereço do link é mesmo o do serviço bancário e siga todas as normas de segurança recomendadas pelo banco.

12 - Atualize seu sistema operacional

O Windows é o sistema operacional mais usado no mundo e quando uma falha de segurança é descoberta nele, uma série de pragas digitais são desenvolvidas para explorá-la. Por isso, vá em Iniciar / Painel de Controle / Atualizações Automáticas / Windows Update e siga as orientações no site que abrir para atualizar seu sistema operacional. Fazer isso uma vez ao mês é suficiente para manter seu sistema operacional atualizado.

Se for usuário de outro sistema operacional, como o Mac OS ou alguma distribuição Linux, saiba que essa dica também é válida. Falhas de segurança existem em qualquer sistema operacional, por isso, é importante aplicar as atualizações disponibilizadas pelo desenvolvedor.

13 - Atualize também os seus programas

Também é importante manter seus programas atualizados. Muita gente pensa que as versões novas apenas adicionam recursos, mas a verdade é que elas contam também com correções para falhas de segurança. Por isso, sempre utilize a última versão dos seus programas, especialmente os que acessam a internet (navegadores de internet, clientes de e-mail, etc). Muitos aplicativos contam com uma funcionalidade que atualiza o programa automaticamente ou avisa do lançamento de novas versões. É um bom hábito deixar esse recurso ativado.



14 - Não revele informações importantes sobre você

Em serviços de bate-papo (chat), no [Orkut](#), em fotologs ou em qualquer serviço onde um desconhecido pode acessar suas informações, evite dar

detalhes da escola ou da faculdade que você estuda, do lugar onde você trabalha e principalmente de onde você mora. Evite também disponibilizar dados ou fotos que forneçam qualquer detalhe relevante sobre você, por exemplo, fotos em que aparecem a fachada da sua casa ou a placa do seu carro. Nunca divulgue seu número de telefone por esses meios, tampouco informe o local em que você estará nas próximas horas ou um lugar que você frequenta regularmente. Caso esses dados sejam direcionados aos seus amigos, avise-os de maneira particular, pois toda e qualquer informação relevante sobre você pode ser usada indevidamente por pessoas má-intencionadas, inclusive para te localizarem.

15 - Cuidado ao fazer cadastros

Muitos sites exigem que você faça cadastro para usufruir de seus serviços, mas isso pode ser uma cilada. Por exemplo, se um site pede o número do seu cartão de crédito sem ao menos ser uma página de vendas, as chances de ser um golpe são grandes. Além disso, suas informações podem ser entregues a empresas que vendem assinaturas de revistas ou produtos por telefone. Ainda, seu e-mail pode ser inserido em listas de SPAMs.

Por isso, antes de se cadastrar em sites, faça uma pesquisa na internet para verificar se aquele endereço tem registro de alguma atividade ilegal. Avalie também se você tem mesmo necessidade de usar os serviços oferecidos pelo site.

Finalizando

Se proteger no "mundo virtual" pode ser um pouco trabalhoso, mas é importante para evitar transtornos maiores. A maioria dos golpes e das "ciladas" pode ser evitada se o usuário estiver atento