Introdução a Redes de Computadores e a Internet

Professor Antônio Eugênio Silva

As redes de computadores e a internet têm desempenhado um papel fundamental em nossa sociedade moderna, conectando pessoas, dispositivos e informações em todo o mundo. Neste material introdutório, vamos explorar os conceitos básicos das redes de computadores e entender como a internet funciona.

Sumário

Elementos de uma comunicação

Para que haja comunicação entre um transmissor e um receptor, são necessários os seguintes elementos:

Mensagem: A mensagem é a informação que está sendo transmitida do transmissor para o receptor. Pode ser qualquer forma de dados, como texto, áudio, vídeo, imagens, comandos, entre outros. A mensagem contém o conteúdo que o transmissor deseja transmitir e que o receptor deve receber e interpretar corretamente. O transmissor codifica a mensagem em sinais adequados para a transmissão, e o receptor decodifica os sinais recebidos para reconstruir a mensagem original

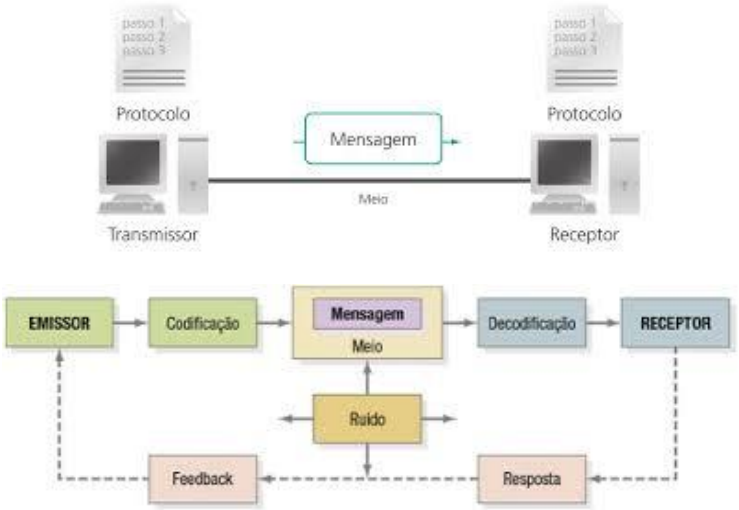
Meio de comunicação: É necessário um meio físico ou uma tecnologia de comunicação que permita a transmissão das informações. Pode ser um cabo de cobre, fibra óptica, ondas de rádio, sinais infravermelhos, ou uma conexão sem fio, como o Wi-Fi ou outros meios de transmissão.

Transmissor: O transmissor é o dispositivo que converte as informações em sinais adequados para a transmissão. Ele codifica os dados em um formato adequado para o meio de comunicação utilizado e os envia através do meio de transmissão.

Sinal: O sinal é a representação física dos dados que está sendo transmitida. Pode ser uma onda elétrica, uma onda de luz, um sinal de rádio, etc. O sinal é modulado com base na informação a ser transmitida.

Receptor: O receptor é o dispositivo que recebe o sinal transmitido pelo transmissor. Ele decodifica o sinal e converte-o de volta para o formato original dos dados. O receptor interpreta as informações e as disponibiliza para o usuário final.

Protocolos: São os conjuntos de regras e formatos padronizados que garantem a comunicação correta entre o transmissor e o receptor. Os protocolos definem aspectos como o formato dos dados, a detecção e correção de erros, a sequência de comunicação e outros aspectos necessários para uma transmissão confiável e eficiente. Os protocolos trabalham em conjunto formando modelos ou “pilha” de protocolos, como o OSI e o TCP/IP (internet).



Protocolos de rede

Para que os dispositivos em uma rede possam se comunicar de forma eficiente, é necessário o uso de protocolos de rede. Um protocolo é um conjunto de regras e procedimentos que define como os dispositivos devem se comunicar e trocar informações. Alguns protocolos comuns incluem:

TCP/IP (Transmission Control Protocol/Internet Protocol): é o conjunto de protocolos usados na internet e define como os dados são transmitidos e roteados entre os dispositivos.

DHCP (Dynamic Host Configuration Protocol): é responsável por atribuir endereços IP aos dispositivos na rede de forma automática.

DNS (Domain Name System): converte nomes de domínio, como www.exemplo.com, em endereços IP para permitir o acesso aos sites na internet.

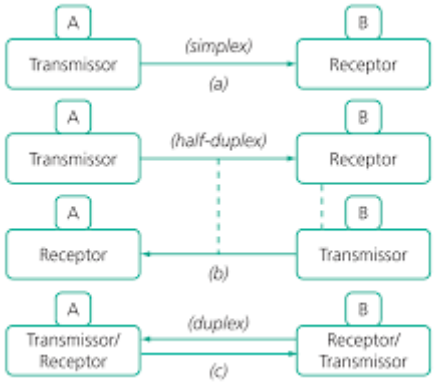
Modos de comunicação

Os modos de comunicação referem-se à maneira como a comunicação ocorre entre os dispositivos ou sistemas. Existem três modos principais de comunicação: simplex, half duplex e full duplex. Vamos descrever cada um deles:

Simplex: No modo simplex, a comunicação ocorre em apenas uma direção, do transmissor para o receptor. Nesse modo, um dispositivo transmite os dados, enquanto o outro dispositivo apenas recebe os dados. Não há uma troca bidirecional de informações. Um exemplo comum de comunicação simplex é a transmissão de rádio ou televisão, onde os usuários recebem informações, mas não podem enviar respostas diretamente.

Half Duplex: No modo half duplex, a comunicação ocorre em ambas as direções, mas apenas uma direção pode ser usada de cada vez. Isso significa que os dispositivos podem transmitir e receber dados, mas não simultaneamente. Os dispositivos alternam entre transmitir e receber, compartilhando o canal de comunicação. Um exemplo de comunicação half duplex é uma chamada de rádio onde um operador fala e, em seguida, aguarda a resposta antes de poder falar novamente.

Full Duplex: No modo full duplex, a comunicação ocorre em ambas as direções simultaneamente. Os dispositivos podem transmitir e receber dados ao mesmo tempo, permitindo uma comunicação bidirecional completa e simultânea. É como uma conversa telefônica, onde ambas as partes podem falar e ouvir ao mesmo tempo, sem precisar esperar a vez um do outro. A comunicação full duplex é comumente usada em redes de computadores e em chamadas telefônicas por meio de sistemas de telefonia modernos.



Modelo OSI (Open Systems Interconnection)

O modelo OSI é um modelo de referência que descreve como os sistemas de rede devem se comunicar e trocar informações. Ele é dividido em sete camadas, cada uma com funções específicas. Essas camadas são:

Camada física: trata da transmissão dos dados através dos meios físicos, como cabos e sinais elétricos.

Camada de enlace de dados: garante a entrega de dados confiável entre os nós da rede, controlando erros e fluxo de dados.

Camada de rede: gerencia o roteamento dos pacotes de dados pela rede, determinando o caminho mais eficiente para a entrega.

Camada de transporte: garante a entrega dos dados de forma confiável e ordenada, dividindo-os em segmentos.

Camada de sessão: estabelece, mantém e finaliza as conexões entre os dispositivos.

Camada de apresentação: lida com a formatação e a representação dos dados, garantindo a interoperabilidade entre diferentes sistemas.

Camada de aplicação: fornece serviços de rede aos aplicativos, permitindo que os usuários acessem e interajam com a rede.

Modelo TCP/IP (internet)

O modelo TCP/IP é um conjunto de protocolos amplamente utilizado na internet. Ele também é dividido em camadas, embora não seja idêntico ao modelo OSI. As camadas do modelo TCP/IP são:

Camada de acesso à rede: lida com a interconexão entre dispositivos e redes físicas, como Ethernet ou Wi-Fi.

Camada de internet: trata do roteamento dos pacotes de dados pela rede, usando o protocolo IP (Internet Protocol).

Camada de transporte: fornece serviços de transporte confiável de dados, com os protocolos TCP (Transmission Control Protocol) e UDP (User Datagram Protocol).

Camada de aplicação: oferece serviços de rede aos aplicativos, como HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol) e DNS (Domain Name System).

O que é uma rede de computadores?

Uma rede de computadores é um conjunto de dispositivos interconectados que se comunicam entre si, trocando informações e recursos. Esses dispositivos podem ser:

Computadores: como desktops, laptops e servidores;

Dispositivos móveis: como smartphones e tablets;

Dispositivos de rede: como roteadores, switches, hubs e pontos de acesso sem fio;

Dispositivos de armazenamento em rede: como servidores de arquivos e sistemas de armazenamento em nuvem;

Dispositivos de segurança: como firewalls e sistemas de detecção e prevenção de intrusões.

Esses dispositivos são conectados através de cabos (como Ethernet) ou de forma sem fio (Wi-Fi) para permitir a troca de dados e o compartilhamento de recursos.

Por que as redes de computadores são importantes?

As redes de computadores são essenciais para permitir a comunicação e o compartilhamento de recursos entre os dispositivos. Elas possibilitam o envio de e-mails, acesso a sites na internet, compartilhamento de arquivos, transmissão de dados em tempo real, entre outras atividades. Além disso, as redes são usadas em ambientes corporativos para facilitar o trabalho em equipe e o acesso a sistemas e informações compartilhadas.

Elementos ativos de rede

Existem vários dispositivos utilizados em redes de computadores para garantir o funcionamento adequado. Alguns dos principais dispositivos incluem:

Roteador (router): é um dispositivo responsável por encaminhar os dados entre diferentes redes. Ele recebe pacotes de dados de uma rede e determina a rota mais eficiente para entregá-los ao destino correto.

Switch: é um dispositivo que permite a conexão de vários dispositivos em uma rede local (LAN). Ele direciona os pacotes de dados apenas para o dispositivo de destino, melhorando a eficiência e a segurança da rede.

Modem: é um dispositivo utilizado para conectar uma rede local à internet. Ele converte os dados digitais do computador em sinais analógicos ou vice-versa, permitindo a transmissão de dados pela linha telefônica, cabo ou fibra óptica.

Firewall: é um dispositivo ou software responsável por proteger a rede contra ameaças externas, filtrando o tráfego de dados e bloqueando acessos não autorizados.

Access Point: é um dispositivo utilizado para estabelecer uma rede sem fio (Wi-Fi), permitindo que dispositivos móveis e outros equipamentos se conectem à rede sem a necessidade de cabos.

Classificação das redes quanto a abrangência

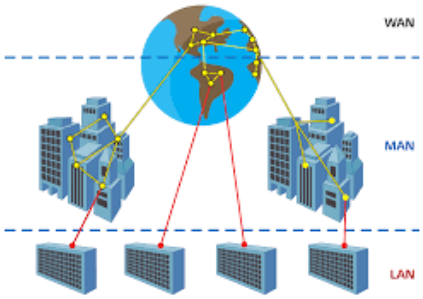
Levando em consideração o aspecto da escala de cobertura, as redes podem ser classificadas da seguinte maneira:

LAN (Local Area Network): É uma rede de área local que abrange uma área geográfica limitada, como um escritório, prédio, campus universitário ou residência. As LANs são utilizadas para interconectar dispositivos próximos, como computadores, impressoras e servidores, permitindo o compartilhamento de recursos e informações.

WLAN (Wireless Local Area Network): É uma rede de área local sem fio, que utiliza tecnologias como Wi-Fi para conectar dispositivos em uma área geográfica restrita. As WLANs são amplamente usadas em ambientes onde a instalação de cabos é inviável ou indesejada, oferecendo mobilidade aos dispositivos conectados.

MAN (Metropolitan Area Network): É uma rede de área metropolitana que abrange uma cidade ou região metropolitana. As MANs conectam diferentes locais dentro de uma área geográfica maior, como escritórios de uma empresa em várias partes da cidade. Elas geralmente utilizam tecnologias de telecomunicações, como fibra óptica, para fornecer alta velocidade e largura de banda.

WAN (Wide Area Network): É uma rede de longa distância que cobre uma área geográfica extensa, como um país, continente ou até mesmo uma rede global, como a Internet. As WANs conectam diferentes LANs ou MANs através de tecnologias como linhas alugadas, links de satélite ou redes de telefonia.



Topologias de redes

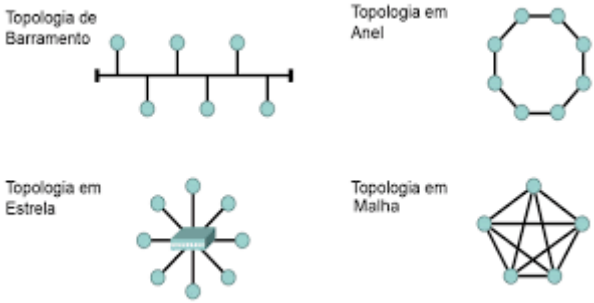
As redes de computadores podem ser organizadas em diferentes topologias, que descrevem a forma como os dispositivos estão interconectados. As topologias comuns incluem:

Rede em barramento (bus): os dispositivos são conectados em um único cabo compartilhado, formando uma linha reta.

Rede em anel (ring): os dispositivos são conectados formando um loop fechado, onde cada dispositivo está conectado ao próximo.

Rede em estrela (star): todos os dispositivos são conectados a um ponto central, como um switch ou hub.

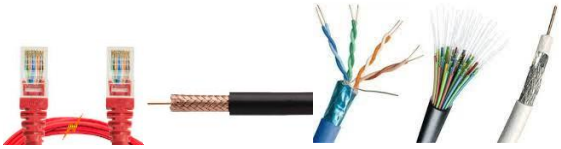
Rede em malha (mesh): cada dispositivo é conectado diretamente a todos os outros dispositivos da rede.



Meios de transmissão em redes

Os principais meios físicos utilizados em redes de computadores são:

Cabos de cobre: Os cabos de cobre são amplamente utilizados para a transmissão de dados em redes locais (LANs). Existem diferentes tipos de cabos de cobre, como o cabo de par trançado (como o cabo Ethernet) e o cabo coaxial.



Fibra óptica: A fibra óptica é um meio físico que utiliza fios de vidro ou plástico para transmitir sinais de luz. Ela oferece altas taxas de transferência de dados, maior largura de banda e maior imunidade a interferências eletromagnéticas do que os cabos de cobre.

Redes sem fio: As redes sem fio utilizam ondas de rádio ou sinais infravermelhos para transmitir dados. Alguns exemplos de tecnologias de redes sem fio incluem Wi-Fi (Wireless Fidelity), Bluetooth e redes celulares (como 3G, 4G e 5G).

Redes via satélite: As redes via satélite são utilizadas quando é necessário estabelecer conectividade em áreas remotas ou onde a infraestrutura terrestre é limitada. Elas envolvem a transmissão de dados por meio de sinais de rádio entre uma estação terrestre e um satélite em órbita.

Redes de energia elétrica: Algumas tecnologias, como a Power Line Communication (PLC), utilizam a rede de energia elétrica existente para transmitir dados. Elas permitem a comunicação por meio da infraestrutura elétrica, eliminando a necessidade de cabos de dados separados.

A escolha do meio físico depende das necessidades da rede, como a distância que precisa ser coberta, a velocidade de transmissão desejada e o ambiente em que a rede será implantada.

A internet

A internet é um conjunto de redes de computadores interconectadas, que abrange o mundo todo. Na realidade são Sistemas Autônomos interconectados – que é uma grande rede ou grupo de redes que possui uma política unificada de roteamento. Todo computador ou dispositivo que se conecta à internet está conectado a um AS.

A internet permite o compartilhamento de informações e serviços, como e-mail, acesso a páginas da web, chamadas de vídeo, streaming de mídia, entre outros. A internet é baseada no modelo cliente-servidor, onde os dispositivos dos usuários (clientes) se conectam aos servidores para obter os recursos desejados.

No modelo cliente-servidor, os dispositivos na Internet são divididos em duas categorias principais:

Cliente: Um cliente é um dispositivo, como um computador, smartphone ou tablet, que solicita serviços ou recursos de um servidor. Os clientes enviam solicitações para os servidores e aguardam as respostas correspondentes.

Servidor: Um servidor é um dispositivo que fornece serviços ou recursos aos clientes. Ele recebe as solicitações dos clientes, processa-as e envia as respostas apropriadas de volta aos clientes.

A troca de dados na Internet é facilitada por meio de protocolos de comunicação. Ela opera com base em um conjunto de princípios de funcionamento e protocolos padrão que garantem a transferência confiável de dados. O princípio de funcionamento da Internet e alguns dos principais protocolos utilizados são:

Protocolo de Controle de Transmissão (TCP): O TCP é um protocolo confiável de camada de transporte que garante a entrega ordenada e sem erros dos dados. Ele estabelece conexões virtuais entre os dispositivos e segmenta os dados em pacotes que são enviados de forma sequencial, verificando se todos são recebidos corretamente.

Protocolo de Internet (IP): O protocolo IP é responsável pelo endereçamento e roteamento dos pacotes de dados na Internet. Ele define como os pacotes são enviados de um dispositivo para outro, garantindo que eles sejam direcionados ao destino correto com base nos endereços IP.

O Protocolo de Internet (IP) é um protocolo de comunicação que permite que dispositivos se comuniquem e troquem dados em redes de computadores, incluindo a Internet. É a base fundamental da comunicação de rede e é responsável pela identificação e endereçamento dos dispositivos conectados em uma rede.

O IP é um protocolo de camada de rede que fornece endereços IP únicos a cada dispositivo na rede. Ele define como os pacotes de dados são formatados, endereçados, transmitidos, encaminhados e entregues corretamente aos seus destinos.

A Internet utiliza o Protocolo de Internet (IP) para atribuir um endereço único a cada dispositivo conectado. Os endereços IP, que podem ser do tipo IPv4 (exemplo: 192.168.0.1) ou IPv6 (exemplo: 2001:0db8:85a3:0000:0000:8a2e:0370:7334), permitem que os pacotes de dados sejam roteados corretamente entre os dispositivos.

Existem duas versões principais do Protocolo IP em uso atualmente: o IPv4 (Internet Protocol version 4) e o IPv6 (Internet Protocol version 6). O IPv4 ainda é a versão mais amplamente utilizada e utiliza endereços IP de 32 bits, enquanto o IPv6 utiliza endereços IP de 128 bits, permitindo um número muito maior de endereços disponíveis.

No IPv4 existem dois tipos de endereços, o público e o privado. A diferença entre IP público e privado está relacionada à sua atribuição e ao escopo de rede em que são usados:

- IP Público: Um endereço IP público é atribuído a um dispositivo diretamente conectado à Internet. É um endereço único e globalmente roteável, o que significa que pode ser acessado e alcançado na Internet pública. Os IPs públicos são fornecidos por provedores de serviços de Internet (ISPs) e são usados para identificar dispositivos em redes públicas, como servidores da web, roteadores ou computadores diretamente conectados à Internet.

_ IP Privado: Um endereço IP privado é atribuído a dispositivos dentro de uma rede privada, como uma rede doméstica ou uma rede corporativa. Esses endereços IP não são roteáveis na Internet pública e são usados para identificar dispositivos dentro de uma rede local. Os IPs privados são reservados para uso interno e não são exclusivos globalmente. Isso significa que vários dispositivos em redes diferentes podem ter o mesmo endereço IP privado. Alguns exemplos de faixas de IP privado são 192.168.0.0 a 192.168.255.255 e 10.0.0.0 a 10.255.255.255.

A comunicação entre dispositivos com endereços IP privados e a Internet pública é possível por meio de tradução de endereço de rede (Network Address Translation - NAT), que mapeia os endereços IP privados para um único endereço IP público compartilhado por vários dispositivos em uma rede.

Protocolo de Transferência de Hipertexto (HTTP): O HTTP é um protocolo de aplicação usado para transferir conteúdo da web, como páginas da web, imagens, vídeos etc. Ele permite a solicitação e o recebimento de recursos entre um cliente (geralmente um navegador web) e um servidor web.

Protocolo de Correio Eletrônico (SMTP, POP, IMAP): Esses protocolos são usados para o envio e recebimento de e-mails. O SMTP (Simple Mail Transfer Protocol) é usado para enviar e-mails, enquanto o POP (Post Office Protocol) e o IMAP (Internet Message Access Protocol) são usados para receber e-mails de servidores de correio.

Protocolo de Sistema de Nomes de Domínio (DNS): O DNS é um protocolo que traduz nomes de domínio (como www.exemplo.com) em endereços IP correspondentes. Ele permite que os usuários acessem sites usando nomes em vez de endereços IP numéricos.

Protocolo de Transferência de Arquivos (FTP): O FTP é utilizado para a transferência de arquivos entre dispositivos na Internet. Ele permite o envio e o download de arquivos de forma eficiente e segura.

Esses são apenas alguns exemplos dos principais protocolos utilizados na Internet. Existem muitos outros protocolos que desempenham papéis específicos para diferentes tipos de comunicação e serviços na rede. Em conjunto, esses protocolos permitem a comunicação e a transferência de dados eficientes e confiáveis na Internet.

A Intranet

A intranet é uma rede privada de computadores que utiliza tecnologias da Internet para compartilhar informações e recursos dentro de uma organização ou empresa. É uma rede interna que funciona de forma semelhante à Internet, porém é restrita aos usuários e dispositivos da organização. A intranet geralmente oferece recursos como compartilhamento de arquivos, acesso a bancos de dados, comunicação interna (por exemplo, e-mail corporativo) e publicação de informações para os funcionários. Ela é usada para melhorar a colaboração e o acesso a informações dentro da organização.

A Extranet

A extranet é uma extensão da intranet que permite a comunicação e a colaboração com usuários externos, como parceiros de negócios, fornecedores, clientes ou outras organizações relacionadas. Ela permite que esses usuários acessem recursos específicos da intranet de forma controlada e segura. Por meio da extranet, as organizações podem compartilhar informações, colaborar em projetos, realizar transações comerciais e fornecer acesso limitado a determinados sistemas ou dados para parceiros externos autorizados. A extranet é uma forma de estender a infraestrutura de rede da intranet para além dos limites internos da organização.

Segurança de redes

A segurança das redes de computadores e da internet é uma preocupação importante. Existem diversas ameaças, como malware, ataques de hackers e roubo de dados, que podem comprometer a segurança das informações. Por isso, medidas de segurança, como firewalls, antivírus, autenticação de usuários e criptografia, são fundamentais para proteger as redes e os dados transmitidos.

A segurança em redes é um conjunto de medidas e práticas adotadas para proteger os sistemas, dados e recursos de uma rede contra ameaças e ataques maliciosos. A segurança em redes é de extrema importância, especialmente em um cenário em que a troca de informações e dados sensíveis é uma parte vital das operações de negócios e comunicações pessoais. Aqui estão alguns conceitos básicos relacionados à segurança em redes:

Autenticação: É o processo de verificar a identidade de um usuário, dispositivo ou sistema antes de permitir o acesso a recursos da rede. A autenticação geralmente envolve o uso de senhas, certificados digitais, chaves de autenticação ou outras formas de autenticação de dois fatores.

Autorização: Uma vez autenticado, um usuário ou dispositivo deve ter permissões adequadas para acessar determinados recursos ou executar certas ações dentro da rede. A autorização garante que apenas usuários autorizados tenham acesso aos recursos necessários.

Criptografia: É a técnica de codificar informações para torná-las ilegíveis para qualquer pessoa que não tenha a chave correta. A criptografia é usada para proteger a confidencialidade dos dados transmitidos em uma rede, garantindo que somente as partes autorizadas possam acessá-los.

Firewall: É um componente de segurança que monitora e controla o tráfego de rede com base em regras predefinidas. Os firewalls protegem a rede bloqueando o acesso não autorizado, filtrando pacotes de dados indesejados e impedindo ameaças de entrar ou sair da rede.

Atualizações e Patches: É importante manter os sistemas e dispositivos da rede atualizados com as últimas correções de segurança (patches). As atualizações de software e firmware corrigem vulnerabilidades conhecidas e ajudam a proteger a rede contra ameaças conhecidas. Os patches, também conhecidos como correções de segurança, são atualizações de software fornecidas pelos fabricantes para corrigir falhas, vulnerabilidades ou problemas de desempenho identificados em um programa, sistema operacional, aplicativo ou firmware. Os patches são projetados para atualizar o software existente, substituindo o código com falhas por um código corrigido. Eles podem abordar uma variedade de questões, como vulnerabilidades de segurança, bugs de software, melhorias de desempenho ou compatibilidade com novos recursos.

Conscientização e Treinamento: A conscientização sobre segurança em redes é essencial para todos os usuários. Treinamentos e políticas de segurança ajudam a educar os usuários sobre práticas seguras, como o uso de senhas fortes, identificação de ameaças, phishing, engenharia social, entre outros.

Phishing é uma forma de ataque cibernético em que os criminosos se passam por entidades confiáveis, como empresas legítimas, instituições financeiras ou organizações governamentais, para enganar os usuários e obter informações confidenciais, como senhas, números de cartão de crédito, informações bancárias ou dados pessoais. Os ataques de phishing geralmente ocorrem por meio de mensagens de e-mail, mensagens de texto, mensagens instantâneas ou até mesmo chamadas telefônicas fraudulentas. Os golpistas se fazem passar por uma fonte confiável e convencem os usuários a revelarem suas informações pessoais ou a visitarem sites falsos, que se assemelham aos legítimos, para coletar dados sensíveis.

Engenharia social é uma prática utilizada por indivíduos mal-intencionados para manipular, enganar ou explorar a confiança das pessoas, com o objetivo de obter informações confidenciais, acesso a sistemas, realizar fraudes ou outros tipos de ataques. Diferentemente dos ataques cibernéticos tradicionais que exploram vulnerabilidades em sistemas e redes, a engenharia social se concentra em explorar as fraquezas humanas, como a curiosidade, a ingenuidade, a confiança ou a vontade de ajudar, para obter acesso não autorizado a informações ou recursos.

Esses são apenas alguns dos conceitos básicos relacionados à segurança em redes. A segurança em redes é um campo amplo e em constante evolução, e é importante adotar uma abordagem em camadas, combinando diferentes medidas de segurança para proteger a rede contra ameaças internas e externas.