1. O que são firewall pessoais e quais os cuidados a serem tomados?

R: Firewall pessoal é um software ou hardware de segurança que protege seu computador contra acessos não autorizados, controlando o tráfego de rede.

Os cuidados a serem tomados são sempre mantê-lo ativado, atualizar frequentemente, apenas permitir conexões confiáveis, usar junto com antivírus e redobrar a segurança em redes públicas.

1. Explique filtro antispam.

R: Filtro antispam é um sistema que serve pra bloquear e-mails indesejados, tipo propaganda ou mensagens falsas que podem ter vírus ou tentar aplicar golpes. Ele analisa o conteúdo do e-mail e o remetente, e se achar suspeito, manda direto pra pasta de spam. Isso ajuda a manter a caixa de entrada mais limpa e segura. É bom sempre dar uma olhada nessa pasta, porque às vezes e-mails importantes podem parar lá sem querer.

1. Cite outros mecanismos de antispam e explique cada um deles.

R: Listas Negras (Blacklists):  
 Bloqueia e-mails de servidores conhecidos por enviar spam.

Listas Brancas (Whitelists):  
 Permite e-mails de remetentes confiáveis sem filtrar como spam.

DNSBL (DNS-based Blackhole List):  
 Usa o DNS para bloquear e-mails de servidores que enviam spam.

SPF (Sender Policy Framework):  
 Verifica se o servidor de envio é autorizado a usar o domínio do remetente.

DKIM (DomainKeys Identified Mail):  
 Assina digitalmente os e-mails para garantir que não foram alterados.

1. Explique o que são contas e senhas.

R: Contas são registros em serviços online, como e-mail, redes sociais ou bancos, que armazenam informações pessoais e preferências.

Senhas são códigos secretos usados para proteger suas contas e garantir que só você tenha acesso a elas.

1. Cite as formas de sua senha ser descoberta e quais os cuidados a serem tomados ao usar suas contas e senhas.

R: Phishing: Golpistas tentam enganar você para pegar suas credenciais.

Força bruta: Hackers tentam várias combinações para adivinhar sua senha.

Keyloggers: Programas que gravam suas teclas e capturam a senha.

Vazamentos de dados: Senhas expostas em brechas de segurança de sites.

Senha fraca ou reutilizada: Senhas simples ou as mesmas em várias contas são mais fáceis de descobrir.

Cuidados a se tomar são usar senhas fortes misturando letras, números e símbolos, não reutilizar senhas em várias contas, ativar a autenticação em dois fatores, evitar e-mails e sites suspeitos, mudar suas senhas regularmente e usar um gerenciador de senhas para armazená-las de forma segura.