**Questão 7 –** C

**Questão 8 –** D

**Questão 10 –** A

**Questão 6 –** B

**Questão 9 –** B

**Questão 5 –** O gerenciamento adequado de credenciais na segurança cibernética é importante para que dados e informações pessoas sejam protegidas de forma eficiente e evitando futuros vazamentos na internet, fazendo com que pessoas mal-intencionadas tenham acesso a essas informações e façam com que os ataques sejam piores e mais frequentes. As melhores práticas para a criação e manutenção de senhas seguras são: sempre verificar em sites confiáveis se o seu email foi vazado (onde, geralmente, suas senhas também são), usar um aplicativo de gerenciador de senhas confiável, que ajude a criar senhas fortes e que sejam armazenadas de forma segura e correta, sempre ter um plano de ação caso as informações tenham sido explorada por algum site, aplicativo, ou empresa, sempre bloquear links ou sites suspeitos, que além de acessarem a máquina, roubam seus dados, mudar de senha com frequência, sempre usar senhas com diferentes letras, caracteres, números e evitar o nome de pessoas ou lugares (se usar, trocar as letras da palavra por números e caracteres especiais), entre outras coisas que é possível fazer para manter suas contas e informações seguras.

**Questão 3 –** Um ataque ransomware é quando um invasor consegue acesso aos dados, arquivos, contas, etc em sua máquina e criptografa eles. Após isso ele pede uma quantia exorbitante em dinheiro (geralmente criptomoedas, pois são mais difíceis de rastrear), e diz ao usuário que se aquele valor não for pago até o dia estabelecido por ele, os dados serão expostos para toda a internet e ele nunca mais terá acesso a eles. Ele se tornou um ataque prevalente nos últimos anos por tratar-se de um ataque que deixa poucos rastros e faz com que os golpistas ganhem uma quantia grande de dinheiro de maneira “fácil” e “rápida”. Para se proteger, as organizações podem armazenar seus dados em uma nuvem, fazer backups frequentes, alterar senhas constantemente e oferecer treinamentos para suas equipes para evitarem o acesso a sites suspeitos, etc, fazendo com que se protejam cada vez mais e evitem esse e outros tipos de ataque.

**Questão 2 –** Vírus, worms e trojans são diferentes tipos de malwares. Vírus podem acessar o computador quando você baixa algum tipo de aplicativo ou executa algum arquivo de texto, propagando-se por toda a máquina e fazendo com que arquivos e aplicativos sejam corrompidos, um exemplo é: achar um pendrive, colocá-lo em seu computador e baixar algum arquivo que tem nele, apenas por “curiosidade”, facilitando a entrada do vírus. Worms são como o vírus, podem não precisam que o usuário, necessariamente, baixe um arquivo para acessar a sua máquina, é preciso que ele apenas esteja conectado a rede, fazendo com que ele seja contaminado e contamine os outros que também estão nessa mesma rede, um exemplo é: quando você se conecta a uma rede desconhecida ou alguma rede pública (onde há pouca fiscalização) e não há o uso de VPN, facilitando o acesso desse malware... por isso é importante o uso de VPNs, para que esse tipo de ataque não aconteça ou que seus danos sejam minimizados. Já o Trojan (ou Cavalo de Tróia), é um malware que se disfarça de um aplicativo (aparentemente verídico), porém em seu código há algum tipo de vírus, fazendo com que danifique sua máquina, um exemplo é: quando você tenta baixar algum aplicativo em algum site não-oficial (que também parece com o verdadeiro) e não verifica se o endereço está correto, fazendo com que você facilite a entrada de um Trojan em seu computador, por isso é importante sempre baixar aplicativos em seus respectivos sites oficiais e evitar, ao máximo, o “pirateamento” de plataformas.

**Questão 4 –** Engenharia Social é quando o invasor ou a pessoa má intencionada usa as informações que ela sabe sobre você (que ela pode encontrar nas redes sociais) ou até mesmo táticas de manipulação, usando a persuasão e a sensação de emergência para manipular e fazer com que o usuário entregue suas informações. Ela é considerada uma das formas mais eficazes de ataque cibernético por não depender de nenhum tipo de descuido de uma pessoa, apenas fazer com que ela acredite no que está dizendo e faça conforme o que o invasor fala, não verificando se aqueles dados ou informações são realmente verdadeiras e se ele realmente responde por uma empresa. Existem diversas técnicas como o Phising: quando a pessoa mal-intencionada envia diversos ou anúncios falsos que são do interesse do usuário no qual está atacando, e faz com que ele realmente acredite que sejam reais, o Pretexting: onde o golpista se passa por alguém que tem um cargo mais importante e pede dados ou acessos da empresa onde o manipulado trabalha, fazendo com que ele passe essas informações sem questionar, e também há a Troca Equivalente: onde o golpista dá ao usuário alguma informação e ele pede outra de volta, ou quando o golpista pega as informações do usuário e diz que somente irá devolver caso ele passe algum dado sigiloso de onde ele trabalha (por exemplo).

**Questão 1 –** Segurança Cibernética podem ser a junção de práticas, aplicativos, uso de firewalls, VPNs para proteger a sua rede ou seu computador de ataques de terceiros ou invasores mal-intencionados. Ela importante para que o sistema operacional não tenha arquivos essenciais apagados, fique lento ou até mesmo tenha suas informações vazadas para a internet, gerando ainda mais problemas. Três consequências possíveis de uma falha de segurança no SO podem ser: travamento (ele fica mais lento com o tempo), vazamento de dados (informações pessoais como nome, email, senhas, localização, arquivos importantes, entre outros, podem ser vazadas na internet por algum invasor) e também podem aparecer anúncios e pop-ups sem parar (não causando nenhum dano significativo, porém é irritante e pode causar, novamente, a lentidão do SO, em um geral).