AMEAÇAS AOS SISTEMAS DE SEGURANÇA	AMEAÇAS AOS SISTEMAS DE SEGURANÇA
O que são **ameaças** aos Sistemas de Informação?	**São condições perigosas para o Sistema de Informação que ainda não se concretizaram.** São condições que poderiam gerar algum risco ou dano para o sistema ou para os dados armazenados nele. Como por exemplo a corrupção do sistema, gerando falhas de funcionamento e a perca de dados relevantes para os usuários e para o sistema como um todo.
O que são **Incidentes**?	**Incidentes:** é quando a ameaça passa de apenas um risco para se tornar uma realidade. **Quando uma ação maliociosa se concretiza, acontece um "Incidente Informático"**, a grande luta dos sistemas de segurança da informação é que os riscos não se tornem incidentes.
Quais são as **principais ameaças** aos sistemas de informação?	As principais ameaças aos sistemas de informação são: **- Falhas de Hardware;** **- Vulnerabilidades em Softwares;** **- Ataques Cibernéticos;** **- Malwares;** **- SPAM's;** **- SCAM's (Golpes);**
Quais as características da ameaça **Falha de Hardware**?	**Falhas de Hardware:** São ameaças imprevisíveis, podem acontecer a qualquer momento, portanto são inevitáveis. O que pode ser feito é minimizar as percas causadas por essa ameaça, como por exemplo: Fazendo **backups**, quando fazemos backups dos dados regurlamento podemos recuperá-los a partir do seu ponto de salvamento. Outra estratégia seria trabalhar com um **Sistema Reduntante, também conhecidos como "Computadores Espelho"**, um servidor que copia os mesmos dados que o principal para se, caso um falhar, o outro possa assegurar o mantenimento das informações.
Quais as características da ameaça **Vulnerabilidade de Software**?	**Vulnerabilidade de Software:** São ameaças existentes no próprio código fonte do software, onde o desenvolvedor do software - intencionalmente ou não - deixou **"brechas" (cracks)** na programação. Um Hacker poderia se aproveitar destas brechas de programação e invadir o software se apropriando de dados que não lhe pertencem. Como essas brechas são inevitáveis, o que podemos fazer é minimizar o encontro destas brechas, fazemos isso por **utilizar softwares de fontes seguras** e por **atualizar constantemente os nossos softwares para as últimas versões**, pois as versões mais atuais podem vir com essas falhas já sanadas.
Quais as características da ameaça **Ataques Cibernéticos**?	**Ataques Cibernéticos:** São ameaças partidas de uma pessoa por através de ataques intencionais com o objetivo de invadir, prejudicar, e destruir sistemas e harwares. Esses são os famosos ataques executados pelos **Crackers** (Vulgarizados como Hackers) amadores ou não que utilizam técnicas de programação ou exploits para invadir sistemas e realizar atos maliciosos. Nesses momentos uma **boa verificação de autenticidade** vai ajudar a barrar a entrada de pessoas que não deveriam ter acesso ao sistema, quanto mais sofisticado o método de autenticação mais difícil seria a invação de Cracker.
Qual a **diferença entre** Crackers Legítimos e Amadores?	**Cracker Legítimo:** É o cracker que tem um bom conhecimento da programação e do sistema que está sendo utilizado, e consegue invadir sistemas "apenas com o conhecimento e as mãos". Alguns até mesmo criam exploits para facilitar suas invasões; **Cracker Amador:** É o cracker que se aproveita de exploits para fazer invasões;
O que são **Exploits**?	**Exploits:** São programas desenvolvidos por Crackers Legítimos com o objetivo de facilitar a invasão em sistemas operacionais.
Quais as características da ameaça **Malware**?	**Malware:** é um acrônimo para "**Malicious Ware**", são rotinas desenvolvidas com o objetivo de invadir sistemas de informação, como os exploits por exemplo. Geralmente essas rotinas aparecem como um vírus de computador, como: **Cavalo de Tróia** e **WORMs**. O melhor método para evitar os Malwares é investir em boas aplicações de **Anti-Vírus**.
Quais as características da ameaça **SPAM**?	**SPAM:** é um acrônimo para **Sending and Posting Advertisement in Mass (Envio e Recebimento de Propagandas em Massa)**, que são mensagens de e-mail, geralmente comerciais, que tem o objetivo de fazer propagandas. Essas mensagens são enviadas em massa para o máximo de endereços de e-mail possíveis, e são indesejáveis, podendo até conter rotinas maliciosas, além de contribuir para o congestionamento de fluxo de rede, devido a grande quantidade de envios. A melhor foram de impedir os SPAMs é **utilizar protocolos de e-mail que não permitem o envio e recebimento de mensagens em massa.**

AMEAÇAS AOS SISTEMAS DE SEGURANÇA	AMEAÇAS AOS SISTEMAS DE SEGURANÇA
Quais as características da ameaça **SCAM**?	**SCAM:** literalmente significa **"Golpe"** em inglês, são golpes utilizados por pessoas que aparentam trazer algum benefício com o objetivo de que façamos alguma coisa que dispare uma rotina maliciosa, roube os nossos dados ou dinheiro mesmo. Por exemplo, artigos promocionais, onde um criminoso pede pelos dados da vítima em busca de algum benefício, esse é um método de SCAM. Geralmente nesse método nem é preciso usar tecnologia, esse tipo de criminoso usa somente a manipulação e lábia para enganar os usuários. A melhor forma de impedir essa ameaça é **não se deixar levar por promoções que parecem ser "boas demais para ser verdade".**