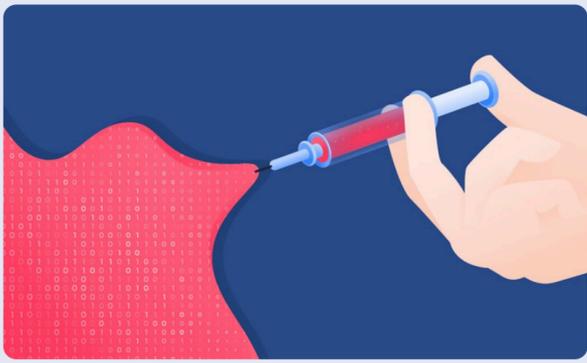


Proteja-se dos Hackers

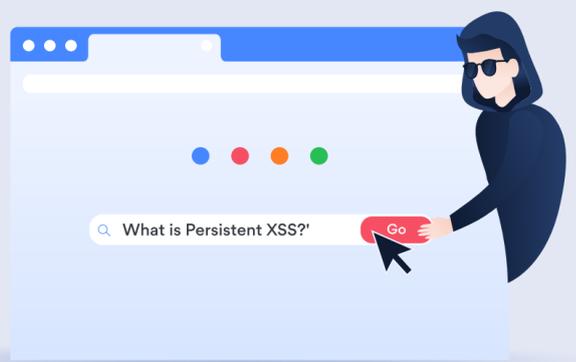
É necessário proteger os aplicativos, dados, programas, redes e sistemas contra ataques cibernéticos, pois pode ser divulgada informação pessoal.

Principais Riscos



Injeção de Código, é uma vulnerabilidade de segurança que ocorre quando um invasor consegue inserir e executar código malicioso em um aplicativo ou sistema.

Cross-Site Scripting (XSS) ocorre quando um invasor insere scripts maliciosos em campos de entrada que são exibidos em páginas da web.



Roubo de Dados Pessoais ocorre quando informação pessoal é divulgada na internet, normalmente originada por passwords fracas ou “back-doors” existentes no código.

Problemas de autenticação ocorre quando informação pessoal é divulgada na internet, normalmente originada por passwords fracas ou “back-doors” existentes no código.



Boas Práticas para Evitar Riscos

Testes de Segurança e Antivirus

O Antivirus serve prevenir que alguma anomalia penetre no seu computador, por precaução é melhor executar testes de segurança

Palavra -Passe segura

Usar uma palavra-passe com uma mistura de símbolos especiais, letras minúsculas e maiúsculas, e/ou com mais de 15 caracteres ajuda a proteger os dados e informações sensíveis. Existem gestores de palavras-passe para ajudar a melhorar a segurança,

Usar Redes Sociais de forma prevenida

Ter cuidados para não partilhar informação confidencial nas redes sociais como palavras passes ou ficheiros privados é o ideal para não criar uma crise cibernética.

Conclusão

É importante tomar todas as medidas possíveis para proteger os teus dados e isso pode ser coisas bastantes simples, como uma palavra-passe boa ou cuidados não muito exigentes.

FONTES

<https://napoleon.com.br/glossario/o-que-e-code-injection-2/>

Trabalho feito por: Bogdan Paily N°2 & Dinis Vleira N°6