**Segurança da Informação na Internet**

**Resumo**

Nos dias atuais a informação e tratada como uma fonte de ouro por diversos segmentos, muitas das vezes acabamos expondo informações que não deveríamos colocar na rede seja a localização onde estamos, dados pessoais e diversos outros dados uma vez que na internet diversas pessoas podem se apropria ou roubar essas informações para nos prejudicar se passando por nós ou até mesmo usando essas informações para nos causar vários prejuízos inestimáveis. E muito importante sabemos onde utilizamos essas informações pois muitas das vezes colocamos esses dados em sites não confiáveis ou até a instalação de programas que achamos confiáveis acabam contendo diversos tipos de vírus capazes de capturar informações pessoais sem nós percebemos.

**Introdução**

Com o avanço da tecnologia muitas melhorias foram proporcionadas assim gerando uma flexibilidade enorme como pagamentos através de aplicativos, transferência de dinheiro e entre outros , muitas das vezes os usuários acabam expondo suas informações pessoais na internet ou pode sofrer ataques por vírus, malwares, ou até em muitos casos sofrem ataques de Ransomweres que bloqueia o determinado aparelho infectado sem deixar o usuário ter acesso algum as aplicações contidas no aparelho e que para liberar o acesso e preciso pagar ou até mesmo passar informações pessoais. Na maioria das vezes as pessoas acabam colocando essas informações em lugares onde não conhecem assim sendo enganados por sites que se mostram ser verdadeiros e em aplicativos e programas que baixamos muitas vezes sem saber se são confiáveis, assim não sabendo que esses serviços estão infectados com algum tipo de vírus capaz de rouba informações sem percebemos.

O uso e proteção desses dados e muito importante para várias empresas e usuários pois estão lidando com diversos dados pessoais de vários clientes e dados da empresa então tem que haver uma forte proteção desses dados que ficam armazenados e também a proteção desses dados sendo trafegados na rede. Existem diversas ferramentas de proteção contra o roubo de dados sejam eles Softwares pagos ou livres, em muitos dos casos ajudam na proteção como firewalls, programas de sistemas de controle de acesso, a implementação de protocolos de segurança e criptografia, softwares de monitoramento de anomalias entre outros. Diversas empresas treinam seus usuários de todos os setores de trabalho a terem boas práticas de proteção de dados assim evitando que o mesmo não sofra com o acesso e o uso não autorizado.

**Como evitar o roubo de dados**

Na maioria das vezes o roubo de dados se dá por conta de usuários que não conhecem os perigos de expor as informações e também muitas das vezes acabam usando programas maliciosos que o mesmo não conhecem, nas empresas geralmente o roubo de dados pode ocorrer por falhas no equipamentos que armazenam e fazem o trafego dos dados assim os hackers que são pessoas que tem um bom conhecimento de invasão de sistemas acabam se aproveitando dessas falhas, um outro ponto importante mencionado e o uso muitas das vezes de engenharia social onde uma determinada pessoa abusa da ingenuidade dos usuários ou confiança de outra pessoa assim obtendo informações confidencias que só podem ser acessadas por pessoas autorizadas. Para que essas informações não sejam roubadas deve haver uma conscientização nas organizações informando que os dados expostos sem devidos cuidados pode causar grandes prejuízos para uma determinada organização, assim deve haver treinamento para os usuários praticarem bons métodos de segurança e também contratação de profissionais com boas qualidades para manter os ativos e aplicações sempre atualizados e seguros, já no caso dos usuários domésticos e muito difícil aplicar boas condutas pois muitas das vezes a sempre uma desproteção dos próprios acessando e colocando essas informações de maneira totalmente errada mas em muitos dos casos quando se há algum tipo de ataque a roubo de dados as mídias de informação sempre alertam sobre a pratica de boas condutas de segurança.

**Segurança dos ativos Físicos**

A proteção nos ativos físicos sejam eles celulares, computadores, tablets, notebooks entre outros e muito importante pois em alguns casos o roubo de dados pode se dar pelo acesso não autorizado a ativos onde pode ocorrer a danificação do mesmo ou até o furto de algum componente que contém informações confidencias, diversos segmentos investem na proteção dos ativos físicos como a instalação de câmeras que podem captar pessoas não autorizadas, o uso da biometria e da íris e muito importante pois na maioria dos casos há sempre uma autenticação de dois fatores.

A autenticação de dois fatores e muito importante e torna o acesso a sistemas muito mais seguro, em muitos casos essa autenticação pode ser usada como a primeira autenticação o uso de uma senha e já na segunda autenticação pode ocorrer o uso da biometria onde só o usuário tem aquela determinada característica, a proteção aos ativos pode ocorrer também com a contratação de guardas de segurança para fazer o controle de acesso entre vários outros métodos de proteção.

**Considerações Finais**

A informação nos dias atuais são tratados como grandes minas de ouro pois o uso desses dados ajudam grandes empresas a gerarem vantagem competitiva entre outras possibilidades, mas em diversos dos casos os usuários acabam expondo ou sofrem com ataques de roubos de dados, com o crescimento do roubo de dados as mídias socias sempre falam das boas práticas do uso de informações e assim criando métodos para a proteção das informações ou seja os usuários dessas aplicações devem esta sempre precavidos para que essa coleta de informações não autorizada não aconteça e também se utilizando de ferramentas que fazer a proteção dos dados uma vez que uma determinada empresa pode ter as melhores ferramentas não está totalmente protegida onde e preciso de profissionais qualificados e que sempre estão atualizados sobre novos ataques pois com o passar do tempo os hackers encontram novas maneiras de burla sistemas para extrair informações de forma não autorizada.