# SEGURANÇA DIGITAL

Calixto, Matheus

Delma, Marc-Alder

Stevanato, Thiago

# INTRODUÇÃO

Segurança Digital (SI) e fundamental nos dias de hoje e muitas pessoas leigas no assunto podem correr riscos ao acessar sistemas inseguros como sites não confiáveis, responder e-mails com seus dados pessoais para fontes desconhecidas, utilizar número de cartão de crédito em compras online de sites e vendedores não conhecidos e baixar arquivos piratas como jogos e softwares.

O risco de um computador adquirir um vírus e ocorrer danos em seu computador, ou até mesmo uma pessoa sair prejudicada por um engenheiro social (hacker) ter obtido dados pessoais como número de cartão de credito ou outra informação importante, o risco é alto. É importante a conscientização dos usuários sobre os riscos que podem causar grandes prejuízos.

Também constitui, a SI, uma questão de grande atualidade e inegável relevância. Isto é, por todo lado que se aplica a tecnologia de informação, bibliotecas, e-mail, sistemas bancários, sistemas escolares, sistemas hospitalares, qualquer seja o sistema que usa a tecnologia da informação, a segurança digital é um fator primordial para a sobrevivência das informações (PEREIRA, 2005).

Com a ampla evolução de desenvolvimento da tecnologia na atualidade, os riscos e ameaças cibernéticos ampliaram e a segurança está a cada vez mais precária. O grande desafio é garantir a proteção das informações nos meios digitais, pois, a informação digital, resultado de conhecimento e da evolução da sociedade, representa um patrimônio intelectual e cultural (Campos, 2002).

A segurança cibernética pode ser dividida em duas categorias: segurança física e segurança lógica. A segurança física abrange a proteção dos locais onde estão instalados os hardwares ou conjunto de hardwares para impedir acesso ás pessoas não autorizados, já a lógica consiste na segurança nomeadamente das informações garantindo a confiabilidade, a integridade, a disponibilidade e a autenticidade das mesmas por meio de software de proteção (anti-malware) (BENTO, 2013).

**Objetivo:**

Identificar a importância da conscientização dos riscos do mundo digital.

# O QUE SÃO OS ATAQUES DIGITAIS

O conceito de segurança na área de SI resume-se em apenas uma palavra: segredo, pois ele é fundamental para manter as informações confidenciais e integras. Devido ás técnicas, métodos e ferramentas desenvolvidos pela Engenharia Social (a ciência que estuda como o conhecimento do comportamento humano para induzir pessoas a atuarem contra o seu desejo) o sigilo das informações se tornou vulnerável. Sabendo que os computadores são operados por humanos, as falhas humanas são fatos que comprometem bastante a SI. Um exemplo disso, é o caso na qual, influenciado por alguém, a pessoa revela as informações involuntariamente ou por negligência da pessoa alguém descobrir as informações (BATISTA, 2015).

Em virtude das falhas humanas os hackers usam as ferramentas da engenharia social aproveitar da vulnerabilidade por parte dos usuários.

O vírus, uma das ferramentas mais aplicadas nos ataques, é fragmento de programa e só executa com auxílio de outro programa, este trecho de código de programa se auto multiplica e ocupa muito espaço de armazenamento, tomar autonomia do sistema, podendo alterar configurações, instalar e desinstalar programas. O conjunto de programas usados nos ataques chama-se de malware (programas maliciosos que burlam a SI), engloba o vírus, já citado; o worm ao contrário do vírus é um programa completo que executa por si só, instalado no computador, ele pode fazer qualquer alteração; o trojan que é um veículo de transmissão de vírus ou worms, ele é transmitido através de e-mails falsos; backdoor conhecido como porta dos fundos, transmitido através de trojan, permite o acesso remoto indevido á maquina alvo; o key logger que captura as posições tecladas no teclado podendo assim descobrir informações como: senhas, contas bancarias, dentre outros (KAMANSKI, 2012).

# Como evitar os ataques ditais

A gestão de riscos é relevante para a SI digital e na preservação da segurança. Para garantir que as informações são seguras é preciso levar em consideração esses eixos: confidencialidade, integridade, disponibilidade e autenticidade. Confidencialidade consiste em manter sigilosas as informações; integridade garante que as informações sejam acessadas por pessoas autorizadas; além de serem confidenciais e integras, as informações devem ser disponíveis e enfim a autenticidade permite o não repúdio, assim os usuários se autentificam ao acessar as informações e não podem negar que as acessam. Embora essas medidas evitam alterações e perdas de informações, elas não a totalidade de segurança. (CABRAL; CAPRINO, 2015).

A possibilidade de ataque é alta para os computadores que são conectados na rede mundial de computadores e ela, a Internet (rede mundial de computadores), está cada vez mais indispensável no cotidiano. Existem outras ferramentas e métodos aplicados na SI para minimizar riscos e ataques que são boas práticas para promover a segurança digital. São elas: uso de senhas, criptografia, uso de firewall, backup, etc. A maioria dos sistemas requer um login e uma senha ao acessá-lo, o login é uma chave público por isso é preciso ter uma senha bem elaborada e mantida sigilosa, pois isso impede que alguém rouba a sua identidade (CERT, 2017).