# CONSIDERAÇÕES SOBRE A SEGURANÇA DIGITAL

Calixto, Matheus

Delma, Marc-Alder

Stevanato, Thiago

# RESUMO

O mundo digital, resultado do avanço da tecnologia e retrato de uma sociedade em constante evolução, tem oferecido grandes vantagens e oportunidades às pessoas, quebrando barreiras, encurtando as distâncias e transformando o mundo em uma aldeia globalizada. Portanto, no que se trata de segurança, ele traz uma grande preocupação e muitas pessoas não são cientes dos riscos, de fato, acabam sendo vítimas. Esse artigo tem como objetivo de identificar a importância da conscientização sobre os riscos do mundo digital no âmbito de minimizá-los. Essa pesquisa foi realizada com base em bases de dados diversos em 2018. Foram consultados artigos, blogs e e-books, num total de 8 documentos. A Engenharia Social (ES) tem uma grande importância no combate aos ataques digitais, o desafio da atualidade. Os hackers (engenheiros sociais) através de métodos da ES criam falhas ou aproveitam das falhas existentes em um sistema para invadi-lo, com o motivo de mostrar vulnerabilidades do mesmo. É evidente mostrar para os usuários como funcionam as invasões ou ataques e como evitar tais riscos, pois é extremamente difícil garantir a totalidade da segurança no mundo digital, mas sim conscientemente é possível minimizá-la. Não há dúvida alguma que a conscientização é um fator de extrema relevância para a gestão dos riscos digitais.

**Palavras chaves :** Mundo digital, engenharia social, riscos digitais, conscientização.

# ABSTRACT

The digital world, a result of the advancement of technology and a portrait of a society in constant evolution, has offered great advantages and opportunities for people, breaking barriers, shortening the distances and turning the world into a global village. Therefore, when it comes to security, he brings a great deal of concern and many people are not aware of the risks, in fact, end up being victims. This article aims to identify the importance of awareness of the risks of the digital world in the context of minimizing them. This survey was conducted on the basis of various databases in 2018. Articles were consulted, blogs and e-books, for a total of 8 documents. Social engineering (SE) has a great importance in the fighting against digital attacks, the challenge today. Hackers (social engineers) through methods of the SE creates flaws or take advantage of the existing flaws in a system to hack it, with the objective to show vulnerabilities. Of course show users how invasions or attacks work and how to avoid such risks is very important, because it is extremely difficult to ensure the total security in the digital world, but consciously you can minimize it. There is no doubt that the awareness is a factor of extreme relevance to the management of risks.

**Key Words:** Digital world, social engineering, digital risks, awareness.

# INTRODUÇÃO

Segurança Digital (SI) é 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 mundo digital, Benefícios e Riscos

O mundo atual está em constantes mudanças, e com a tecnologia não é diferente. Hoje em dia em qualquer lugar que você está, tem uma pessoa usando um celular para se comunicar com outra, podendo ser de uma criança a um idoso. A internet não serve apenas para conversar, mas também para fazer compras sem precisar sair de casa, fazer cursos, entre outras inúmeras coisas. As possibilidades de tecnologia são inúmeras e os limites inimagináveis fazendo com que a pessoa possa usufruir de modo que consiga se juntar com a tecnologia para crescer em seu trabalho e se tornar um profissional cada vez mais capacitado (ANUNCIAÇÃO, 2015).

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 para 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 (KAMANSKI, 2012).

E ainda segundo KAMANSKI, 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.

A gestão de riscos é relevante para a SI 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 roube a sua identidade (CERT, 2017).

**CONSIDERAÇOES FINAIS**

Constata-se que informações sigilosas como senhas devem ser sempre bem elaboradas, utilizando sempre diversos caracteres como letras em caixa alta e baixa, e contendo números aleatórios, assim dificultando a sua descoberta, evitar a utilização da mesma senha para diversas finalidades também pode ajudar, como senha de um e-mail ser diferente de uma senha de uma rede social, mesmo sendo a mesma conta.

Percebe-se que a conscientização da era digital e fundamental no cotidiano dos seres humanos, sendo que se deve sempre estar ciente que na rede contem vários tipos de riscos digitais, podendo comprometer os dados pessoais de uma pessoa ou ate mesmo de uma empresa e também podendo comprometer hardwares (Máquinas), por isso e importante sempre estarmos conscientizados sobre tais riscos.

As falhas humanas são o maior desafio para garantir que um sistema esteja a salvo dos riscos, as informações sejam integras e confidenciais. Ao invés de usar ferramentas poderosas, com grande capacidade de processamento para atacar sistemas, que precisa um custo significativa para o seu desenvolvimento, os hackers optam por manipular usuários (pessoas) para conseguir acesso a sistemas, para eles é mais simples, mais fácil e mais prático. Em virtude disso, não há dúvida alguma que a conscientização é um fator de extrema relevância para a gestão dos riscos digitais.

**RFERENCIAS BIBLIOGRFICAS**

ANUNCIAÇÃO, F. E. **O mundo digital e sua importância no cotidiano.** Disponível em: http://www.direitonet.com.br/artigos/exibir/8962/O-mundo-digital-e-sua-importancia-no-cotidiano. Acessado em: 25/04/2018.

BATISTA, F. L. **Métodos e práticas utilizadas em engenharia social com o intuito de obstar o roubo de informações sensíveis.** Disponível em: <http://repositorio.uniceub.br/bitstream/235/8155/1/51306378.pdf>. Acessado em: 21/03/2018.

BENTO, N. M. B. **Gestão Integrada da Segurança Lógica e Física nas Organizações.** Disponível em: https://repositorio.utad.pt/bitstream/10348/3066/1/msc\_nmbbento.pdf. Acessado em: 20/03/2018.

CABRAL, C.; CAPRINO, W. **Trilhas em segurança da informação.** Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=CeInBgAAQBAJ&oi=fnd&pg=PA1&dq=seguran%C3%A7a+digital%22&ots=twm6LPd80O&sig=opHnIYGDN_MngobooUZ7I_FPFXA#v=onepage&q=seguran%C3%A7a%20digital%22&f=false>. Acessado em: 21/03/2018.

CAMPOS, F. M. **Informação digital: um novo património a preservar.** Disponível em: <https://www.bad.pt/publicacoes/index.php/cadernos/article/view/861/860>. Acessado em: 20/03/2018.

CERT. **Fascículo Senhas**. Disponível em: <https://cartilha.cert.br/fasciculos/>. Acessado em: 27/03/2018.

KAMANSKI, M. P. **Estratégias para prevenção de ataques de engenharia social aplicado a Segurança da Informação.** Disponível em: http://www.pb.utfpr.edu.br/redes/1esprc/tccs/MonografiaFinal-MarceloPedroKamanski.pdf. Acessado em: 27/03/2018.

PEREIRA, P.J.F. **Segurança da Informação Digital**. Disponível em: https://www.bad.pt/publicacoes/index.php/cadernos/article/view/822/821. Acessado em: 20/03/2018.