# BIM

**Boletim Informativo Mensal**

**Comunicar para Educar**

Nº 22– Novembro/2021


## Você já viu *links* suspeitos em fóruns ou áreas de comentários de *sites*?

Caso a resposta seja sim, você pode ter presenciado um ***Spamdexing*.**

O *Spamdexing*, também conhecido como *Spam* de Busca, é a técnica utilizada por criminosos digitais para melhorar ou aumentar a chance de um *site* "malicioso" ser colocado no topo das páginas de resultados em buscadores da *Internet*.

Para promover os *sites* de seu interesse, pessoas com más intenções abusam de *sites* legítimos, normalmente, de boa reputação, inserindo seus *links* nestes *sites*. Logo, quando o buscador for analisar o *site* alvo da ação intrusiva, encontrará os *links* inseridos e, consequentemente, melhorará o *ranking* do *site* malicioso. Esse golpe hoje em dia é utilizado para promover toda a sorte de lojas *on-line* de produtos, alguns relacionados com pornografia e drogas, entre outros temas ilícitos.

A palavra *Spamdexing* combina as palavras *Spam* (termo em inglês associado a conteúdo indesejado) e *Indexing* (termo em inglês que significa indexar), remetendo à ideia de que o *hacker* conseguirá indexar conteúdo indesejado em uma página na *Web*, ao invés do tradicional envio de *spam* por *e-mail*. Mas, não param por aí as diferenças em relação ao "*Spam*".

Diferente do *spam*, que tem por objetivo fazer propaganda diretamente para o usuário, através do envio de conteúdo indesejado, o *Spamdexing* é uma abordagem que não tem foco direto no usuário. O objetivo do criminoso é não ser percebido, uma vez que ele vai alcançar o usuário, indiretamente, através da melhoria do *ranking* de seus *links* em buscadores da *Web*. Outro ponto de destaque é o meio: o *Spamdexing* é executado contra *sites,* e não contra contas de *e-mail* pessoais.

Este golpe normalmente explora campos de comentários de *sites*. Então, caso perceba um comentário estranho, no *site* de sua organização, fazendo menção a termos fora do tema da página, avise imediatamente ao administrador do *site*; afinal, segurança é responsabilidade de todos.


## Publicada revisão do Glossário de Segurança da Informação

A Portaria GSI/PR Nº 93, de 18 de outubro de 2021, do Gabinete de Segurança Institucional da Presidência da República, foi publicada no Diário Oficial da União. Ela aprova o Glossário de Segurança da Informação, revoga versão anterior deste e entra em vigor no dia 1º de novembro de 2021. Seu inteiro teor pode ser acessado em:
https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao

BIM
Boletim Informativo Mensal
Comunicar para Educar
Nº 22– Novembro/2021

Você sabia?
Desde que observado o seu teor e, em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, uma Informação Sigilosa pode ser classificada como RESERVADA, SECRETA ou ULTRASSECRETA?


## O que são ATIVOS?


Uma questão muito importante para a segurança da informação é a proteção dos ATIVOS. Mas, afinal, o que são ATIVOS?

No contexto de segurança da informação, ATIVO é tudo que tem valor para a organização, material ou não. Os exemplos de ativos são diversos. Eles podem ser pessoas, bens móveis, bens imóveis, computadores, sistemas, documentos digitais, documentos físicos, entre outros.

Mais especificamente, quando se fala em ATIVO DE REDE, estamo-nos referindo a um equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores, permitindo a conectividade entre diversos ativos.
É interessante relembrar, também, o conceito de ATIVOS DE INFORMAÇÃO, que são:

- os meios, os equipamentos e os sistemas utilizados para armazenamento, transmissão e processamento da informação;
- os locais onde se encontram esses meios;
- as pessoas que têm acesso a esses meios; e
- o conhecimento ou o dado que tem valor para um indivíduo ou uma organização.

Esses e outros conceitos relacionados à segurança da informação podem ser encontrados no Glossário de Segurança da Informação, revisado recentemente.

**Fonte:** https://www.gov.br/gsi/dsi/ https://www.ctir.gov.br/
Editorial/redação/diagramação: AssESI Sugestões: asscom.dsi@presidencia.gov.br