

## PHISING NA WEB

**Guilherme Hernandez Hübner**<sup>1</sup>

Anderson santos da silva<sup>2</sup>

João Padilha Moreira<sup>3</sup>

### RESUMO

Este artigo visa falar sobre os perigos que as pessoas podem passar por uma simples ameaça na web, o phishing nada mais é que uma isca lançada para enganar as pessoas e aguardar que alguém caia nela. Este tipo de vulnerabilidade é difícil de combater ou até exterminar, devido a quantidade de pessoas que acessam a internet e sua falta de conhecimento para prevenção.

**Palavras-Chave:** phishing, vulnerabilidade, internet, prevenção, ameaça.

### ABSTRACT

This article aims to talk about the dangers that people can go through a simple threat on the web, phishing is nothing more than one is launched to deceive people and wait for someone to fall into it. This type of vulnerability is difficult to combat or even exterminate, due to the number of people accessing the internet and their lack of knowledge for prevention.

**Keywords:** phishing, vulnerability, internet, prevention, threat.

---

<sup>1</sup> Acadêmico do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. guilherme.hubner@alcidesmaya.edu.br

<sup>2</sup> Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. anderson\_silva@alcidesmaya.edu.br

<sup>3</sup> Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. joao\_moreira@alcidesmaya.edu.br



## EXPLICAÇÃO DA VULNERABILIDADE

**Phishing:** O Phishing foi desenvolvido para roubar dados pessoais dos usuários, como senhas de e-mails, redes sociais, dados de cartão de créditos, entre diversos outros. Atualmente, qualquer empresa que utiliza a internet para comunicação pode sofrer um ataque. Basta um usuário desatento logado em seu e-mail e/ou internet.

De acordo com KLEVERTON. (2019)

*Phishing* é um crime virtual no qual pessoas comuns são contactadas através de email, telefone ou mensagens de texto (SMS) por uma outra pessoa ou empresa. O contato se faz de maneira genuína, para atrair e induzir o contactado a fornecer informações sigilosas dados bancários, cartão de crédito, senhas e outros informações confidenciais.

Os crimes de phishing chegam até os usuários através de falsos anúncios, sempre bem atrativos ao acesso, ou até clonagem de sites bancários, onde o usuário pensa estar em um ambiente seguro de um banco, mas na verdade está acessando um site desprotegido.

## ESTRATÉGIAS DE DETECÇÃO

Algumas formas de detecção dessa ameaça são desconfiar de ofertas deslumbrantes e lucrativas sem precedentes, como alguma premiação. E caráter de urgência, eles pedem que o usuário seja rápido em sua ação e se não for terá consequências graves.

Segundo ALECRIM (2019)

No Brasil, é bastante comum encontrar mensagens do tipo que se passam por comunicados de bancos, operadoras de cartão de crédito, companhias aéreas, serviços de redes sociais, desenvolvedoras de antivírus, entidades judiciais, lojas virtuais e assim por diante.



Algumas formas de detecção desses sites são através de erros gramaticais, links estranhos e confusos, que não tenham ligação com o conteúdo do site, anexos suspeitos.

## **POSSIBILIDADE DE USO FUTURO**

Phishing é o tipo mais simples de ciberataque e, ao mesmo tempo, o mais perigoso e eficiente. Esse tipo de vulnerabilidade ultrapassa a tecnologia e vai de encontro a questões sociais, hoje a internet é utilizada por todos os tipos de pessoas, e sabendo disso esses ataques simples são cada vez mais usados, pela falta de conhecimento das pessoas o phishing se torna o mais eficaz dentre outras ameaças.

### **Segundo ANDRION (2019)**

Um relatório da Cyxtera, o The Fraud Beat 2018, indica que o phishing continua sendo a forma mais comum de ataque virtual. As ameaças têm alcançado alto nível de complexidade e inovação, já que os hackers têm recursos cada vez mais poderosos e difíceis de serem identificados.

O futuro do phishing está nas compras on-line, que só aumentam ao passar dos anos, e as redes sociais que estão começando a incorporar vendas em suas plataformas digitais. Embora o phishing possa ser um problema difícil de se revolver, algumas dicas de prevenção são essenciais para a proteção do seu ambiente virtual.

- Verifique os links que acessa.
- Cuidado onde digita seu usuário e senha.
- Cuidados ao receber avisos e mensagens.
- Bancos e organizações não pedem para alterar senhas.
- Verifique o site que está comprando.
- Evite redes wi-fi públicas.
- Cuidados com arquivos recebidos.
- Antivírus, sempre é bom né?



## REFERÊNCIAS:

ALECRIM, E. O que é phishing? E como evitar golpes do tipo?. 2019. Disponível em:  
< <https://www.infowester.com/phishing.php/>>. Acesso em: 25 Out 2020.

ANDRION, R. Phishing ainda é a forma mais comum de ataque virtual. 2019.  
Disponível em:  
< [https://olhardigital.com.br/fique\\_seguro/noticia/phishing-ainda-e-a-forma-mais-comum-de-ataque-virtual/82278/](https://olhardigital.com.br/fique_seguro/noticia/phishing-ainda-e-a-forma-mais-comum-de-ataque-virtual/82278/)>. Acesso em: 25 Out 2020.

KLEVERTON, K. O que é phishing e como se proteger de golpes na internet. 2019.  
Disponível em:  
<<https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet/>>. Acesso em: 25 Out. 2020.