



# Info Hacker

RESUMO QUINZENAL OFICIAL DA ACADEMIA HACKER



## LEMBRETES

**01 - Quem poderia me ajudar?**

**02 - O que é Threat Intelligence?**

**03 - Edital Novos Membros**



# Quem poderia me ajudar?

por Priscila Teodorio

Imagine a seguinte situação: Você quer aprender uma nova habilidade ou está em busca de emprego, então decide comprar um curso online para te ajudar. Felizmente, você encontra uma escola com aulas remotas e preço acessível, compra com seu cartão de crédito e começa a estudar imediatamente. Dias depois você percebe que seu cartão de crédito está sendo usado para compras caríssimas que você não fez.

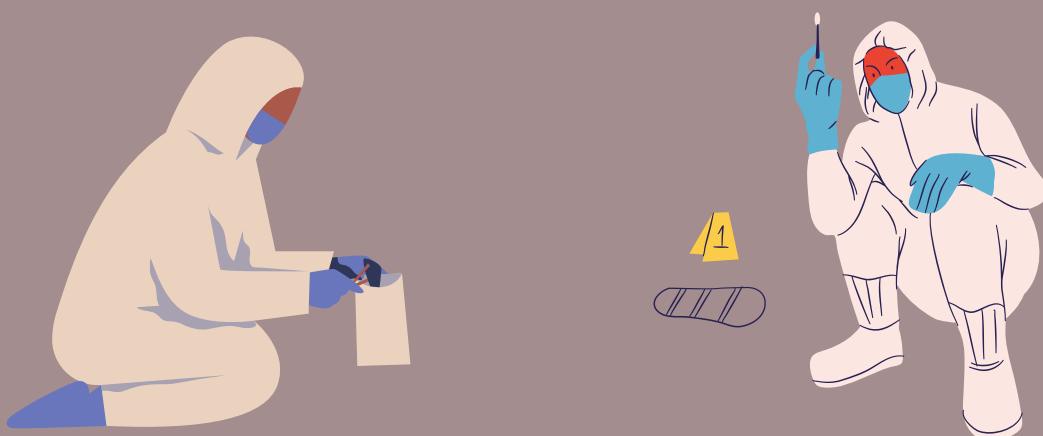
Esse é um tipo de crime cibernético muito comum chamado phishing. Basicamente, é a tentativa de “fisgar” usuários por meio de links, e-mails, aplicativos ou sites construídos especificamente para roubar dados, como senhas, números e cartões, entre outros dados.

Segundo definição encontrada em Brooks (2014), computação forense é uma disciplina que combina elementos do direito e da computação com objetivo de coletar e analisar dados de sistemas computacionais, redes de computadores, comunicações sem fio e sistemas de armazenamento digitais de tal forma que esses dados sejam válidos na justiça.

Um perito forense digital é o profissional responsável por averiguar a autoria de um crime virtual. Para isso, ele vai precisar coletar e analisar imagens e demais dados de computadores e outros dispositivos para levar informações suficientes sobre o ocorrido. E não basta apenas procurar as evidências. Tudo precisa ser preservado a fim de que as informações possam ser utilizadas no processo. Para isso, o trabalho de investigação segue algumas etapas bem sistematizadas:

1. Preservação e coleta dos dados
2. Integridade e cadeia de custódia
3. Análise e apresentação dos resultados

Sendo assim, o perito forense seria o profissional que te ajudaria a encontrar o responsável pelo crime cibernético na situação hipotética no início desse texto.



# O que é Threat Intelligence?

por Leonardo Zaia

Que vários ataques cibernéticos ocorrem todos os dias vocês claramente já devem saber, alguns *DDoS*, *ransomwares*, *CVEs* novas, *zero-days*, etc. Mitigar esses problemas de forma a resolver o problema apenas quando ele aparece, é a mesma coisa que enxugar gelo. Falhas novas vão ser descobertas, abusadas e compartilhadas em fóruns onde diversas pessoas tem acesso. Se defender desses problemas não é apenas consertar um *bug*, até porque é possível haver diversos outros por aí, é também mapear e acompanhar tudo o que está sendo compartilhado na rede.



A melhor forma de se proteger não é esperando algum ataque, mas sim ficar por dentro de tudo que é compartilhado e está rolando pela internet. Foi aí que surgiu o que é chamado de *Threat Intelligence* (O nome já diz bastante sobre o que é, algo como "inteligência de ameaças" em português), que usa conhecimento com base na evidência, incluindo contextos, mecanismos, indicadores, conselhos e implicações sobre os riscos existentes ou emergentes. Esse monitoramento é feito se infiltrando em fóruns, redes sociais, portais, blogs, matérias de jornais, etc. Desta forma, mapeando os agentes, ataques e técnicas utilizadas, torna-se mais fácil de identificar os problemas, ou quem causam, antes deles chegarem até a sua empresa, e possibilita que você consiga corrigir as falhas que sequer começaram a ser explorada por criminosos.

# Edital Novos Membros

por Everton Borges

Será lançado o primeiro edital de 2022 para a adição de novos membros da Academia Hacker (AcHa). Qualquer estudante matriculado nos cursos de Ciências e Engenharia da Computação da Universidade Federal de Alagoas (UFAL) poderá participar do processo seletivo, esse será um pré-requisito. A ideia é que esses novos membros participem de atividades semanais para conhecerem e se aprofundarem mais na área de segurança da informação. Mais detalhes nos próximos dias. Fiquem atentos e vigilantes!!



# Caça Palavras

D	P	Q	U	G	T	H	S	K	A	B
E	I	F	H	R	Z	H	Y	A	G	M
V	L	G	O	M	M	Z	U	K	L	U
I	A	N	I	R	O	F	S	V	Q	C
D	U	E	P	T	E	Z	I	E	O	O
E	D	G	X	J	A	N	Y	O	Z	L
N	O	X	C	Q	A	L	S	F	F	E
C	M	D	A	C	T	P	R	E	Y	T
I	T	T	O	B	H	C	O	F	C	A
A	C	S	O	P	E	R	I	T	O	H
I	L	D	R	V	K	Y	C	O	A	F

evidência    coleta    perito  
 forense    digital    laudo

## Referências

[https://www.canva.com/pt\\_br/](https://www.canva.com/pt_br/)

## Edições Anteriores

<https://github.com/Academia-Hacker/Info-Hacker>

---

**Info Hacker - Edição 005**  
**19/04/2022**



**Autores:**

Priscila Teodorio  
Leonardo Zaia  
Everton Borges

**Revisão**

Bruno Severo