



# *Info Hacker*

RESUMO QUINZENAL OFICIAL DA ACADEMIA HACKER



## LEMBRETES

- 23/02  
Como ingressar na Carreira de Dados?
- 24/02  
DevOps Experience
- 24/02  
PRIVACIDADE ACIMA DE TUDO: LGPD na Saúde

**01 - Proteção de Dados no Brasil**

**02 - Malwares**

**03 - Conscientização em Segurança da Informação**



# Proteção de Dados no Brasil

por Paloma Lacerda

Em Setembro de 2020 passou a valer a LGPD (Lei de Proteção de Dados) que nada mais é que a versão Brasileira para a GDPR(General Data Protection Regulation) que seria a versão Europeia da lei. Ambas têm por objetivo garantir a proteção e controle dos dados pessoais e sensíveis dos cidadãos, estabelecendo um padrão sobre quais dados são pessoais ou sensíveis e assim mantendo o direito à privacidade de todos. Isso ajuda não apenas a dificultar que furtos de identidade e contas bancárias aconteçam, mas também auxiliam a preservar e fortalecer a confiança dos clientes e empresas.

No dia 10/02/2022, uma quinta-feira, o Congresso Nacional incluiu a proteção de dados pessoais entre os direitos fundamentais do cidadão, ou seja, foi alterado o artigo 5ª da Constituição de 1988 que trata especificamente dos direitos e deveres individuais e coletivos, um novo trecho que assegura o direito a proteção dos dados pessoais incluindo os meios digitais. Essa mudança na Constituição, torna qualquer alteração futura referente a esse tema a ser apenas para ampliar ou resguardar os direitos, sendo estritamente proibido fragilizar a proteção à privacidade do cidadão.

O roubo de dados pessoais é bastante lucrativo para os hackers criminosos. Ao conseguir, por exemplo as suas credenciais, combinação de nome de usuário e senha, eles podem usá-las para ataques diversos em sites de interesses, como bancos, varejos e redes sociais. Muitas pessoas repetem o mesmo login/senha em vários sites e torna a fraude mais fácil e perigosa para a população, esse tipo de ataque é conhecido como *Credential stuffing*. Portanto, ter um trecho específico sobre o tema na Constituição Federal é um passo importantíssimo para que tais crimes possam ser penalizados mais seriamente.





# Malwares

por Ullyanne Freire

*Malware* é um software malicioso criado para infectar dispositivos, servidores ou redes de computadores. O Creeper foi o primeiro vírus criado na história, 1971, sua finalidade era exibir uma mensagem "I'M THE CREPER: CATCH ME IF YOU CAN". E para combater esse vírus foi necessário criar um antivírus, chamado Reaper. Alguns tipos de malwares e suas características:

**Vírus:** Atrelados a arquivos executáveis. É necessária a interação do usuário para sua replicação, para isso é utilizado engenharia social.

**Worms:** Não são atrelados a nada para se espalhar. Não é necessária a interação do usuário para sua replicação. É autônomo. Cria cópias de si mesmo.

**Adware:** Exibem anúncios. Coletam dados. Podem ser instalado a partir de um software malicioso, geralmente em um pacote de programas. Pode redirecionar o tráfego do usuário para sites maliciosos ou para anúncios.

**Trojan:** O famigerado "Cavalo de Troia", inspirado no poema grego "Odisséia". Engana os usuários sobre sua verdadeira intenção. Geralmente a infecção ocorre por meio de downloads de mídia pirata, programas crackeados e anexos de email.

**Spyware:** Destinado a infiltrar em dispositivos, e coletar informações, principalmente as sensíveis de um usuário. Pode rastrear atividade online, rastrear e copiar tudo o que é digitado (keyloggers), baixado e armazenado.

**Ransomware:** Quando infectado, o computador tem seus dados criptografados, impedindo que eles possam ser acessados. Para poder liberar os dados, normalmente os criminosos exigem um resgate (ransom).



# *Conscientização em Segurança da Informação*

por Everton Borges

Vários relatórios apontam um crescimento de ataques cibernéticos no ano de 2021. Segundo o infográfico da Fundação ISACA, as empresas relataram um crescimento de 35% de ciberataques e o ataque de Engenharia Social é o mais frequente com 14%. Nesse tipo de ataque os criminosos vão tentar enganar suas vítimas e fazer com que elas entreguem informações pessoais. Quando o atacante é bem-sucedido em seu ataque cibernético, de acordo com o relatório da Verizon, os dados comprometidos são credenciais (85%), dados pessoais (17%), outros (9%) e dados médicos (4%).

Houve também um crescimento dos e-mails que tinham relação com vacinas ou seguro emergência no Brasil. Houve um crescimento de 28% no volume de ataques de phishing em 2021 e esse número cresce ano após ano, em uma pesquisa realizada pela PhishLabs. Devido ao crescimento de ataques que tem como alvo o ser humano, devem ser criadas maneiras de proteger esses usuários. Logo é preciso realizar a conscientização deles para que sejam menos propício a cair em um desses ataques cibernéticos.



Segundo o relatório da CyberSafe e da National Cybersecurity Alliance, 67% dos participantes se acham preparados para identificar um e-mail malicioso e 38% se sentem como um alvo de cibercriminosos. O relatório também mostrou que cerca de 64% dos participantes não tiveram nenhum tipo de treinamento. E ainda segundo a pesquisa, os participantes que tiveram acesso aos treinamentos, 73% mostraram interesse em aprender mais sobre o assunto quando a informação é disponibilizada a eles.

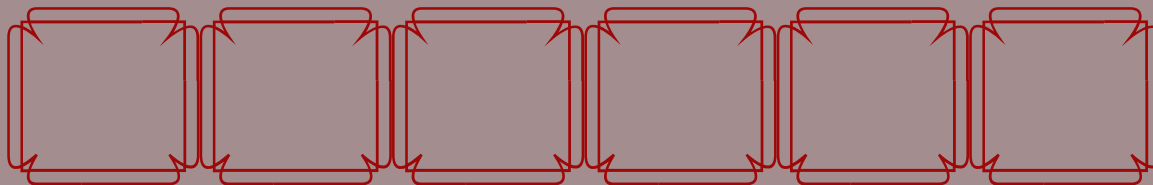
# *Caça Palavras*

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

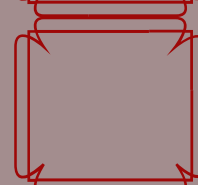
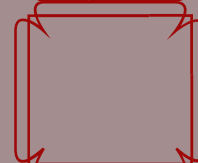
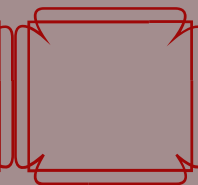
*certificado ssl cifra chave  
mensagem assinatura simetrica hash*

# *Palavras Cruzadas*

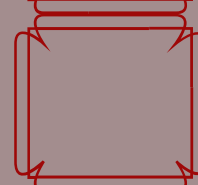
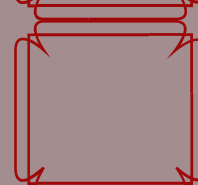
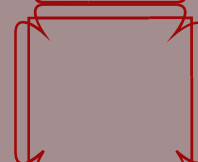
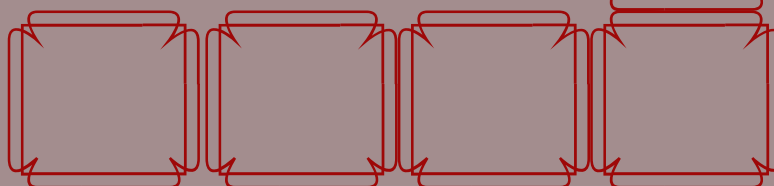
1



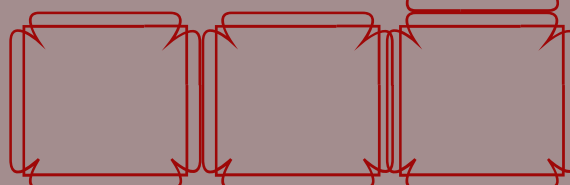
2



3



4

**Vertical**

2- Email contendo links e/ou anexo suspeitos

**Horizontal**

1- Cópia reserva da informação  
3- Ataque de negação de serviço distribuído  
4- Registro de eventos

## Referências

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

<https://www.techtudo.com.br/noticias/2018/07/o-que-acontece-quando-seus-dados-caem-nas-maos-de-hackers.ghtml>

<https://g1.globo.com/politica/noticia/2022/02/10/congresso-promulga-pec-que-transforma-protecao-de-dados-pessoais-em-direito-fundamental.ghtml>

<https://www.isaca.org/resources/infographics/state-of-cybersecurity-2021-part-2>

<https://www.verizon.com/business/resources/reports/dbir/>

<https://www.phishlabs.com/news/social-media-attacks-doubled-in-2021-according-to-latest-phishlabs-report/>

<https://www.cybsafe.com/research-papers/cybersecurity-attitudes-and-behaviors-report-2021/>

---

## Info Hacker - Edição 001 22/02/2022



### **Autores:**

Paloma Lacerda  
Uliyanne Freire  
Everton Borges

### **Revisão**

Bruno Severo

