

Website com BD

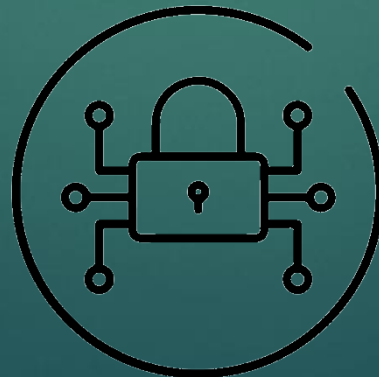


Curso Técnico de
Programação e
Sistemas de Informação
Paulo Teixeira e
Gonçalo Vila Nova
12ºN

2023/2024

Introdução

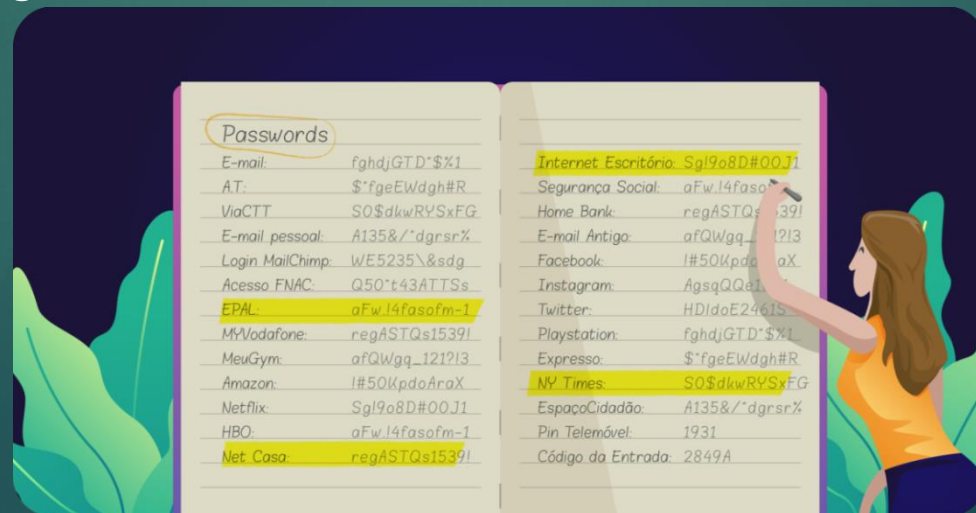
Com o crescimento da internet, a proteção cibernética torna-se crucial para preservar a integridade das informações. A cibersegurança é vital na proteção contra ameaças digitais e designa-se pela proteção de sistemas de computador contra roubos ou danos ao *hardware* ou *software* bem como a interrupção de serviços. É por isso que, neste trabalho, abordaremos não só os seus fundamentos como também os seus desafios e estratégias de defesa.



Segurança de *passwords*

No contexto da segurança, a criação de *passwords* robustas é uma prática essencial. *Passwords* fortes são aquelas que combinam caracteres alfanuméricos e símbolos, evitando informações pessoais.

A utilização de gerenciadores de *passwords* pode contribuir para a criação e armazenamento seguro dessas informações. Ativar a autenticação de dois fatores oferece uma camada extra de segurança, reduzindo significativamente o risco de acesso não autorizado.



Ataque de *phishing*

O *phishing* é uma técnica amplamente utilizada por criminosos na internet, para enganar os utilizadores e obter informações confidenciais, como *passwords* e informações bancárias. Estes ataques ocorrem geralmente através de e-mails fraudulentos, mensagens de texto ou chamadas telefónicas. Os riscos associados ao *phishing*, incluem o roubo de identidade, a instalação de *malware* nos dispositivos do utilizador e o comprometimento da segurança dos dados.



Informações confidenciais

Informações confidenciais são aqueles segredinhos que ninguém quer que as pessoas saibam. Pode ser desde dados pessoais até os planos mirabolantes da empresa. Manter essas coisinhas em segredo é essencial para não dar brecha a malandros. Nas empresas, as pessoas costumam usar truques como senhas fortíssimas, *firewalls* e criptografia para garantir que essas informações fiquem na mão certa.



Tipos de ataques cibernéticos

Os ataques cibernéticos são tipo os vilões do mundo digital, sempre querendo aprontar. Tem uns golpes famosos, tipo o *phishing*, que é tipo quando te mandam mensagem fingindo ser quem não é só pra te tirar informações. Tem também o malware, que é tipo um vírus digital querendo bagunçar tudo. E o DDoS (é um crime cibernético no qual o invasor “inunda” um servidor com tráfego de internet para impedir que os utilizadores acessem sites e serviços *online* conectados.)? Esse é o ataque que quer “encher o saco” e deixar os sistemas indisponíveis. É tipo um ataque de nervos, mas digital.



Criptografia

Criptografia é tipo o escudo mágico do mundo digital. É quando você transforma suas mensagens em algo ilegível, tipo código de espião, só que digital. Tem dois jeitos principais: o fácil, onde usa a mesma chave pra esconder e revelar (como uma senha), e o mais avançado, onde tem um par de chaves, uma pública e outra privada. Isso é tipo magia digital para proteger suas mensagens e dados de curiosos e malandros.



Conclusão

Assim, entendemos que a cibersegurança é uma preocupação constante no mundo digital em constante evolução. Adotar medidas de segurança, compreender os diferentes tipos de ameaças e proteger informações confidenciais são passos essenciais para uma presença online segura. A educação sobre boas práticas de segurança e a implementação de tecnologias de proteção são cruciais para minimizar os riscos associados à segurança cibernética.



Website com BD



Curso Técnico de
Programação e
Sistemas de Informação
Paulo Teixeira e
Gonçalo Vila Nova
12ºN

2023/2024