Guia prático de **cibersegurança**

Dicas e estratégias para manter sua **vida digital segura**

Novembro/2024

A segurança cibernética é uma ferramenta fundamental e importante no nosso cotidiano digital, porque além proteger nossos dados, também ajuda a manter confiança e integridade da Internet.

Cibersegurança não precisa ser um bicho de sete cabeças. Com as dicas certas, você pode proteger seus dados sem complicação!

O que é cibersegurança?

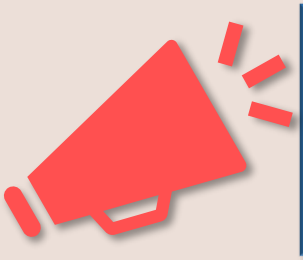
Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos.

Por que proteger seus dados é tão importante?

Esse grande volume de informação administrado por empresas está vulnerável a invasores de sistemas, por isso a proteção de dados pessoais é tão importante. Para as instituições, ter as informações dos clientes invadidas representa dano de imagem e prejuízo financeiro. Para os usuários, pode significar o vazamento de dados privados e importantes, como registros médicos ou informações bancárias, por exemplo. Além da privacidade invadida, o vazamento de dados pessoais na internet também pode trazer aos usuários grandes prejuízos. Esses dados nas mãos de cibercriminosos podem ser usados contra o indivíduo, como nos casos de fraude de identidade ou aplicação de golpes financeiros.

Principais ameaças no mundo digital:

Entre os crimes mais comuns que são cometidos por cibercriminosos estão ataques de *ransomware* e golpes de *phishing* que induzem as pessoas a fazer transferências de dinheiro ou divulgar informações de cartão de crédito, credenciais de login, propriedade intelectual ou outras informações privadas ou sensíveis.



Dica prática: Use senhas longas e únicas, combinando letras, números e símbolos.

Proteção de dispositivos:

Atualize seus dispositivos regularmente

Instale antivírus e *firewalls* confiáveis

Configure backups automáticos

Dica prática: Evite redes Wi-Fi públicas ou use VPN ao acessá-las.

Cuidado com e-mails e sites suspeitos.

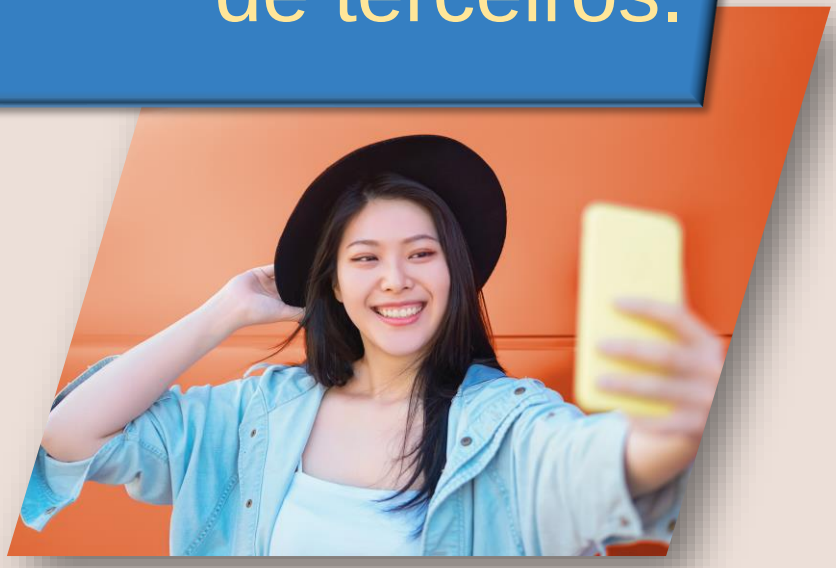
Nunca clique em links desconhecidos.

Dica prática: Se parecer bom demais para ser verdade, provavelmente é golpe.

Limite as informações compartilhadas online.

Revise as configurações de privacidade regularmente.

Cuidado com aplicativos de terceiros.



Dica prática: Não publique dados pessoais, como endereço ou telefone

A cibersegurança começa com pequenos passos. Juntos, podemos tornar o ambiente digital mais seguro!

Glossário de termos básicos de cibersegurança:

- Antivírus: Programa que identifica, bloqueia e remove malwares (software mal-intencionado). É essencial para proteger dispositivos contra vírus e outras ameaças.
- *Backup*: Cópia de segurança dos seus dados armazenada em outro local, como um HD externo ou na nuvem, para evitar perda em caso de ataques ou falhas.
- *Firewall*: Sistema de segurança que monitora e controla o tráfego de dados entre uma rede confiável (como a sua casa) e redes externas (como a internet).
- *Malware*: Termo genérico para softwares maliciosos, incluindo vírus, *worms, ransomware* e *spyware*.
- *Phishing*: Método de enganar pessoas para que forneçam informações confidenciais, como senhas ou números de cartão, por meio de e-mails ou sites falsos.
- VPN (*Virtual Private Network*): Rede privada que cria uma conexão segura entre seu dispositivo e a internet, protegendo sua navegação de bisbilhoteiros.
- Autenticação de Dois Fatores (2FA): Mecanismo de segurança que exige dois tipos de identificação para acessar uma conta (por exemplo, senha e um código enviado ao celular).
- Criptografia: Técnica que transforma dados em um formato ilegível para quem não tem a chave de acesso, garantindo a segurança da informação.
- *Spyware*: Programa espião que coleta informações pessoais sem o conhecimento do usuário.
- *Ransomware*: Tipo de malware que bloqueia o acesso aos seus dados ou dispositivos e exige pagamento de um "resgate" para liberá-los.
- *Trojan* (Cavalo de Troia): Malware disfarçado como um programa legítimo, que engana o usuário para ser instalado e causar danos.
- *Zero-Day* (Dia Zero): Vulnerabilidade em um software desconhecida pelos desenvolvedores, que pode ser explorada por hackers antes de ser corrigida.
- *Keylogger*: Software ou hardware que registra as teclas digitadas para capturar informações confidenciais, como senhas e dados bancários.

Joseana Ziegler