



Manual para você ter na sua empresa:

COMO PROTEGER SEUS DADOS E SISTEMAS CONTRA AMEAÇAS DIGITAIS


BR2T

Índice

- 1..... Introdução
- 2..... O que é Segurança Cibernética?
- 3..... As Ameaças Mais Comuns
- 4..... Principais Ameaças Cibernéticas
- 5..... Phishing e Engenharia Social
- 6..... Ransomware
- 7..... Roubo de Credenciais
- 8..... Como Criar Senhas Fortes e Seguras
- 9..... Protegendo Seus Dispositivos e Redes
- 10..... Protegendo Seus E-mails e Redes Sociais
- 11..... Backup e Recuperação de Dados
- 12..... Boas Práticas para Empresas

O que é Segurança Cibernética?

Quando falamos sobre segurança cibernética, estamos falando sobre tudo o que você pode fazer para proteger sua empresa de ataques digitais. Isso inclui proteger suas redes, sistemas e dados contra ações maliciosas, como roubo de informações e danos aos seus recursos tecnológicos.

De acordo com o relatório da IBM sobre os custos de violações de dados, o custo médio de uma violação de dados é de cerca de US\$ 4,45 milhões! Além do impacto financeiro, uma violação pode afetar seriamente a reputação da sua empresa, fazendo com que clientes e parceiros percam a confiança no seu negócio.



As Ameaças Mais Comuns

Malware: São softwares maliciosos que têm como objetivo danificar, invadir ou roubar dados do seu sistema. Pode ser vírus, trojans, spyware... enfim, há várias formas de malwares.

Phishing: Já recebeu um e-mail dizendo que sua conta foi hackeada e pedindo para você clicar em um link? Isso é phishing! Trata-se de uma tática usada para enganar você e roubar suas informações pessoais.

Ransomware: Esse é um tipo de malware que criptografa seus arquivos e pede um resgate para liberar os dados. Ele pode paralisar uma empresa inteira.

Roubo de Credenciais: Hackers tentam adivinhar suas senhas e obter acesso a sistemas sensíveis, usando diversas ferramentas para descobrir essas credenciais.

Essas ameaças podem afetar tanto grandes corporações quanto pequenas empresas. E não se engane, qualquer empresa pode ser alvo de ataques, independentemente do seu tamanho.

Principais Ameaças Cibernéticas

Agora que sabemos o que é segurança cibernética, vamos detalhar algumas das ameaças mais comuns que você precisa ficar atento.

Malware, Ransomware e Vírus

Como Funcionam? Esses ataques geralmente começam quando você clica em algo que não devia, como um link em um e-mail suspeito ou baixa um arquivo de uma fonte não confiável.

Uma vez no seu sistema, o malware pode roubar dados, corromper arquivos ou até mesmo destruir os sistemas operacionais.

Como se Proteger?

Mantenha seu antivírus sempre atualizado: Ele vai monitorar sua rede e detectar qualquer software suspeito.

Nunca abra anexos ou links de fontes

desconhecidas: Se você receber um e-mail de uma pessoa desconhecida, especialmente com um link ou arquivo em anexo, fique atento.

Faça backups regularmente:

Assim, caso o pior aconteça, você terá uma cópia segura de todos os seus dados.

Phishing e Engenharia Social

Como Funcionam?

O phishing é uma tentativa de enganar você para que forneça suas informações pessoais ou clique em links maliciosos. A engenharia social, por sua vez, utiliza o comportamento humano para induzir os usuários a cometerem erros, como divulgar senhas ou acessar sites comprometidos.

Como se Proteger?

Desconfie sempre de e-mails suspeitos: verifique o remetente, o conteúdo do e-mail e qualquer link antes de clicar.

Educando sua equipe: Uma das melhores formas de combater o phishing é educar seus funcionários para que eles saibam como identificar essas tentativas de fraude.



Ransomware

Como Funciona?

Um ataque de ransomware pode paralisar sua empresa, criptografando arquivos importantes e exigindo um resgate para liberá-los. Imagine ter toda a sua base de dados ou documentos financeiros bloqueados e a única forma de recuperar é pagando o criminoso.

Como se Proteger?

Tenha backups regulares: Isso é a chave para não pagar resgates. Se você perder dados devido a um ataque de ransomware, poderá restaurá-los a partir de um backup seguro.

Evite clicar em links desconhecidos:

Mantenha um controle rigoroso sobre o que é acessado dentro da sua rede.



Roubo de Credenciais

Como Funciona?

Os hackers podem tentar adivinhar suas senhas e acessar suas contas e sistemas importantes, como o e-mail corporativo, sistemas financeiros ou ferramentas de trabalho.

Como se Proteger?

Crie senhas fortes: Senhas como "123456" ou "senha123" são as primeiras que os hackers tentam. Use combinações de letras, números e caracteres especiais.

Autenticação de dois fatores (2FA): Isso adiciona uma camada extra de proteção. Mesmo que alguém descubra sua senha, ainda precisará do seu celular para concluir o login.



Como Criar Senhas Fortes e Seguras



Agora, vamos falar sobre a primeira linha de defesa contra as ameaças cibernéticas: as senhas.

Como Criar Senhas Fortes:

Misture letras maiúsculas e minúsculas, números e símbolos.

Isso cria combinações difíceis de adivinhar. Por exemplo: **Bv8#sX2a!1**

Evite usar informações pessoais.

Nada de datas de nascimento ou nomes de familiares.

Use um gerenciador de senhas.

Esses aplicativos ajudam você a criar e armazenar senhas complexas sem precisar memorizá-las.

Ative a Autenticação de Dois Fatores (2FA): Sempre que possível, ative a autenticação de dois fatores.

Isso vai proteger suas contas, pois, além da senha, será necessário confirmar a identidade por meio de um código enviado para o seu celular.

Protegendo Seus Dispositivos e Redes

1. Mantenha seus sistemas atualizados:
Quando você não atualiza seus sistemas, fica vulnerável a ataques conhecidos.

Os fabricantes de software lançam atualizações regularmente para corrigir falhas de segurança. Não adie essas atualizações!

2. Use VPNs em redes públicas:

Nunca confie em redes Wi-Fi públicas, como aquelas encontradas em cafeterias e aeroportos. Elas são um prato cheio para hackers. Use uma VPN para proteger sua conexão e garantir que seus dados estejam criptografados.

3. Instale um firewall:

O firewall atua como uma barreira entre sua rede interna e as ameaças externas. Ele ajuda a impedir que acessos não autorizados entrem no seu sistema.



Protegendo Seus E-mails e Redes Sociais

Os e-mails e as redes sociais são grandes alvos para ataques cibernéticos. Por isso, é essencial tomar medidas extras para proteger suas contas.

1. Como Identificar E-mails Suspeitos:

Se você receber um e-mail de alguém que você não conhece ou que parece fora do normal, desconfie. Verifique o endereço do remetente, procure por erros de gramática ou links suspeitos.

2. Segurança em Redes Sociais:

Sempre utilize senhas fortes e ative a autenticação de dois fatores. Além disso, revise suas configurações de privacidade para garantir que você não esteja compartilhando mais informações do que o necessário.



Backup e Recuperação de Dados

1. Faça Backups Regulares:

Não espere perder seus dados para perceber a importância de backups. Realize cópias de segurança regularmente e armazene-as de forma segura, seja em servidores locais ou na nuvem.

2. Teste Seu Plano de Recuperação:

Não basta fazer backups, você também precisa testar se pode restaurar seus dados rapidamente em caso de emergência.



Boas Práticas para Empresas

1. Políticas de Segurança Cibernética:

Crie políticas claras sobre como seus colaboradores devem usar os sistemas e redes da empresa. Isso ajuda a reduzir os riscos de ataques.

2. Treinamentos Regulares:

Realizar treinamentos sobre segurança cibernética é essencial para que todos na sua empresa saibam como identificar e agir diante de ameaças.



Agora que você tem um guia completo sobre como proteger sua empresa contra as ameaças cibernéticas mais comuns, é hora de agir.


A segurança cibernética é uma responsabilidade de todos, e as medidas que você adotar agora podem evitar grandes danos no futuro.

Espero que você tenha conseguido esclarecer suas dúvidas e caso queira aprender ainda mais recomendo que você participe da nossa Master Class!


Lembre-se: um ambiente digital seguro começa com boas práticas, educação constante e ferramentas de proteção adequadas.

Vamos juntos proteger o que é mais importante para a sua empresa!



 [br2t.oficial](https://www.instagram.com/br2t.oficial)

 [BR2T - TI](https://www.facebook.com/BR2T-TI)

 [br2tofficial](https://www.youtube.com/br2tofficial)

 [BR2T](https://www.linkedin.com/company/BR2T)

 11 4613-1190