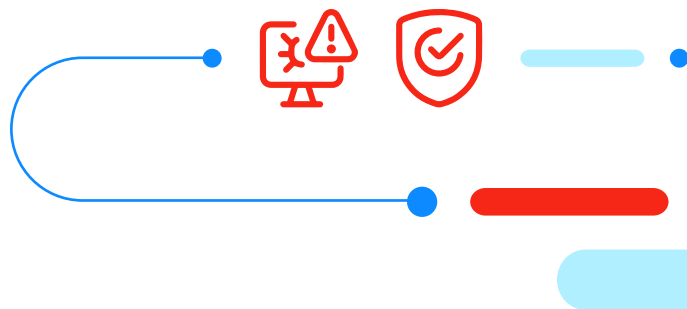


● Prevenção contra ameaças cibernéticas





Sumário

1. INTRODUÇÃO	3
2. DICAS GERAIS	4
2.1. Conheça as ameaças mais comuns	4
2.2. Faça backup e sincronize seus arquivos	4
2.3. Software de segurança habilitado	5
2.4. Hábitos de navegação segura	5
2.5. Mantenha os seus dispositivos atualizados	6
2.6. Finalmente... Em caso de dúvida, jogue fora:	6
3. DICAS PARA EVITAR ATAQUES CIBERNÉTICOS POR E-MAIL	7



1. Introdução



Este documento tem como objetivo dar insumos para evitar que hackers ou softwares maliciosos infectem o seu computador, seja você um colaborador, cliente ou parceiro da Edenred Brasil.

As dicas abaixo foram produzidas pela Edenred Security Awareness, área Global de Segurança da Edenred, a fim de reduzir riscos relacionados a segurança da informação.





2. Dicas Gerais

2.1 Conheça as ameaças mais comuns

Trojans, ransomware, keyloggers, phishing, vazamento de dados e malware.

Isso é o mínimo que você pode fazer para se manter seguro online. Você deve sempre saber as últimas ameaças cibernéticas que se escondem na web. Isso ajudará você a tomar ações imediatas em caso de ataques cibernéticos

2.2 Faça backup e sincronize seus arquivos

Os backups em nuvem são os mais recomendados

É a próxima etapa mais básica na era digital que os usuários devem seguir. Um backup seguro sempre dá um sinal de alívio, pois ajuda a lidar com ameaças cibernéticas em potencial, como o ransomware.



2.3

Software de segurança habilitado

Antivirus, antimalware e etc.

Um programa de segurança ativo pode ser o primeiro a informá-lo sobre qualquer risco em seu computador pessoal ou dispositivo. Portanto, não hesite em investir um pouco, em vez de perder seus valiosos dados sendo usados indevidamente por cibercriminosos.

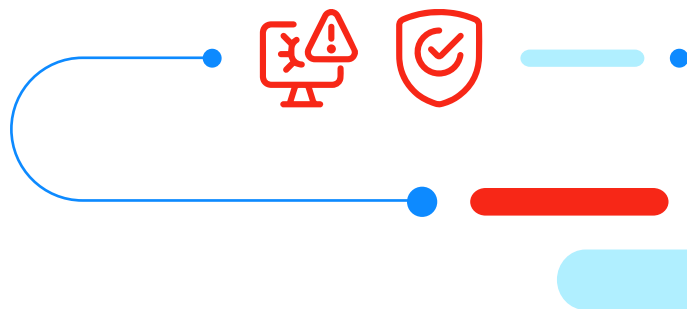
2.4

Hábitos de navegação segura

Ameaças potenciais facilmente atacam por meio de atividades de navegação não segura.

Nossos hábitos de navegação falam sobre nós, o que atrai os cibercriminosos em busca de brechas. Portanto, praticar hábitos de navegação seguros em qualquer lugar é um passo importante para o entendimento básico de segurança cibernética.





2.5

Mantenha os seus dispositivos atualizados

Aplicativos, software, versões do sistema operacional e antivírus.

Seus dispositivos, sejam PC, mobile ou tablets, são vulneráveis. Quanto mais você mantém seus dispositivos e aplicativos atualizados, mais seguro você fica contra vírus, malware ou outras ameaças.

2.6

Finalmente... Em caso de dúvida, jogue fora:

Nunca tenha pressa em clicar em qualquer link ou e-mail que receber. Como links dentro de e-mails, sites não oficiais, plataformas de compartilhamento de mídia social podem conter cargas de ameaças cibernéticas. Esta é a maneira mais comum de os criminosos cibernéticos roubarem suas informações pessoais. Se você encontrar qualquer coisa suspeita, não tente clicar nela.

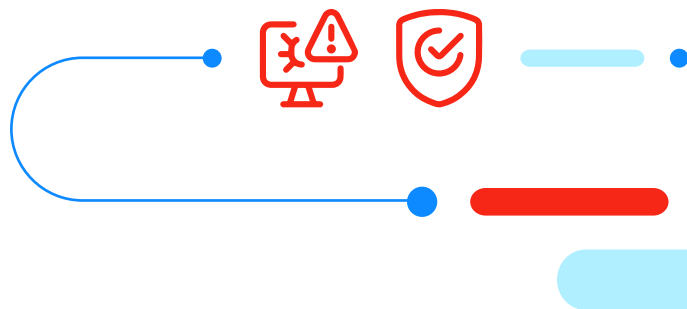




● 3. Dicas para evitar ataques cibernéticos por e-mail



- Certifique-se de abrir anexos com extremo cuidado. Verifique a extensão do arquivo. Nunca abra o anexo com as extensões "pif", "exe", "bat", "vbs";
- Ao navegar, visite apenas sites oficiais. Evite páginas suspeitas e nunca clique em links fornecidos nesses sites;
- Os e-mails de phishing são projetados para serem enviados a uma grande quantidade de pessoas. Portanto, eles precisam ser o mais impessoal possível. Você deve verificar se a mensagem contém um assunto genérico e uma saudação (o Ministério da Saúde, outras autoridades, a identidade do suporte técnico ...);
- Ao utilizar o e-mail corporativo, nunca clique em links contidos em e-mails de remetentes desconhecidos, para evitar ser redirecionado para sites maliciosos que geralmente parecem legítimos;
- Fique atento aos erros gramaticais e ortográficos. Empresas sérias costumam empregar revisores e editores, que garantem que os materiais enviados estejam sempre corretos;



- Verifique se seus equipamentos corporativos são usados apenas para atividades profissionais. Não abra correspondências ou contas pessoais em equipamentos que contenham informações sensíveis da Edenred;
- Atenção ao endereço de e-mail para checar se o remetente é legítimo. Frequentemente, as tentativas de phishing parecem pertencer a uma entidade conhecida. Dê uma olhada no endereço de e-mail do remetente. Você pode verificar o endereço do domínio (exemplos: edenred.com e edenred.consulting-for.com, etc.). Cuidado se o domínio do e-mail não lhe parecer familiar;
- Ao clicar em links, sempre preste atenção nos URLs. Aponte o cursor na URL suspeita. Se ela passar por um link reduzido (bit.ly, goo.gl, tinyurl ...), nunca clique. O principal perigo vem do fato de você não saber para onde será redirecionado.



The logo features a large, white, rounded rectangular shape centered on a solid red background. Inside the left portion of this white shape is a solid red circle. The word "Edenred" is written across the center of the logo. The letters "Eden" are white and positioned over the red circle, while the letters "red" are red and positioned to the right of the circle.

Edenred