Coordenação de Gestão de Tecnologia da Informação CGTI

INSTITUTO FEDERAL
Rondônia

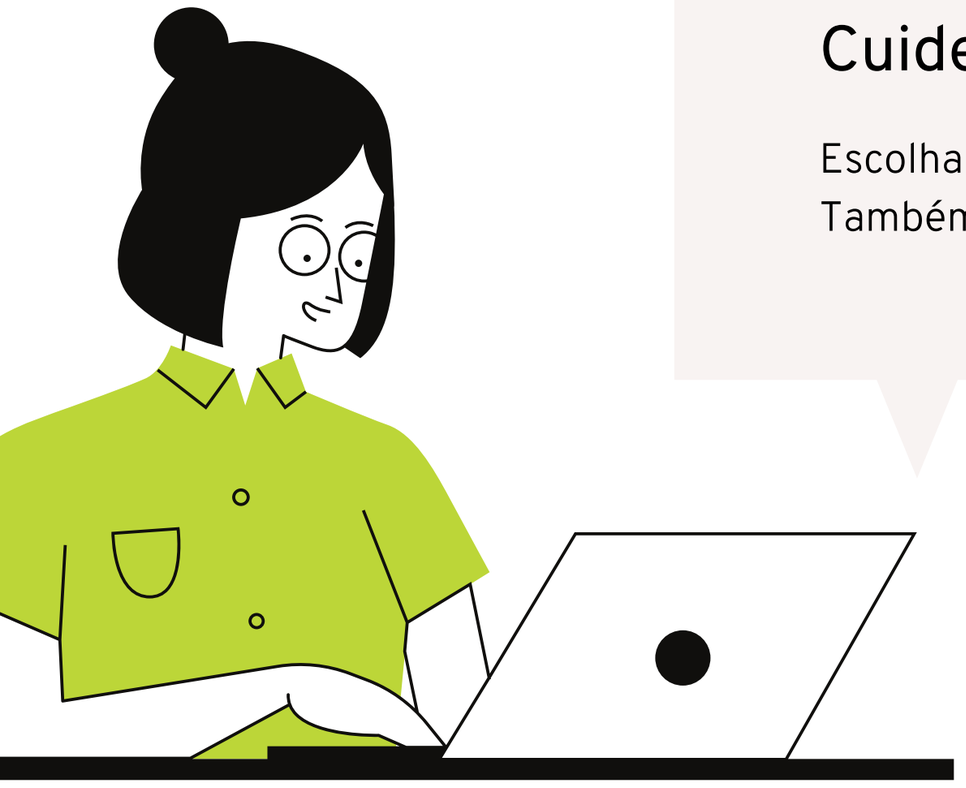
Campus Avançado São Miguel do Guaporé

SEGURANÇA DA INFORMAÇÃO

SEGURANÇA
DA INFORMAÇÃO

Cuide das suas senhas.

Escolha senhas fortes e nunca compartilhe-as com outra pessoa. Também verifique regularmente suas configurações de privacidade.



Tenha atenção com aquilo que você baixa.

Alguns programas e aplicativos carregam malware e tentam roubar suas informações. Faça download de conteúdos apenas em sites de confiança.

Seja cauteloso com sua vida social online.

Exercite a precaução com cada interação online, para que você esteja a salvo de hackers e usuários fake. Não dê informações pessoais ou envie fotos particulares.

Faça compras com segurança.

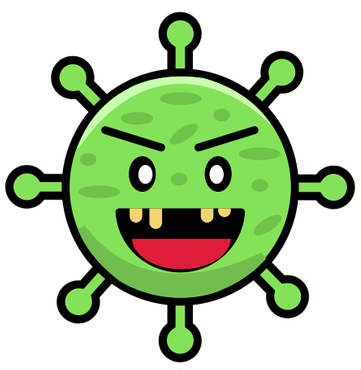
Faça compras em sites seguros, e evite salvar suas informações do cartão de crédito. Gaste tempo lendo os reviews e perguntas feitas por usuários quando for fazer alguma compra.

Reflita antes de postar.

Fique atento a cada post que você cria. Não publique conteúdo que você não queira que sua família, amigos e potenciais empregadores vejam.

SEGURANÇA DA INFORMAÇÃO

Você conhece os principais tipos de malwares? Vamos listar alguns abaixo!

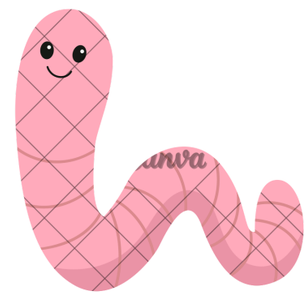


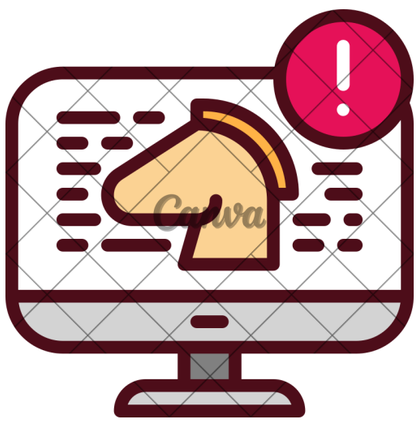
Vírus

Em informática, um vírus de computador é um software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática

Worm

Worm ou computer worm é um programa independente, do tipo malware, que se replica com o objetivo de se espalhar para outros computadores. Geralmente, usa uma rede de computadores para se espalhar, ou mesmo unidades USB, contando com falhas de segurança no computador de destino para acessá-lo





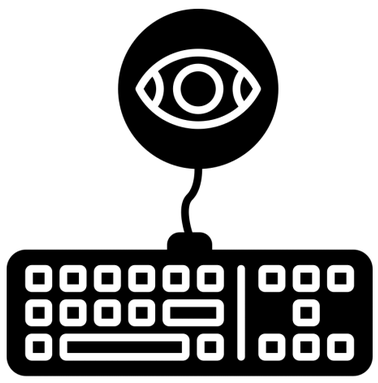
Cavalo de Tróia(Trojan)

Diferentemente dos vírus, Cavalos de Troia não se replicam automaticamente para infectar outros arquivos e computadores. Ao invés disso, ele é o “cavalo de madeira” que leva outros softwares maliciosos (malwares) escondidos para disfarçar seu objetivo nefasto.

SEGURANÇA DA INFORMAÇÃO

Spyware

Spyware é um malware projetado para espionagem. Ele se oculta em segundo plano e coleta seus dados, como senhas, localização GPS e informações financeiras.

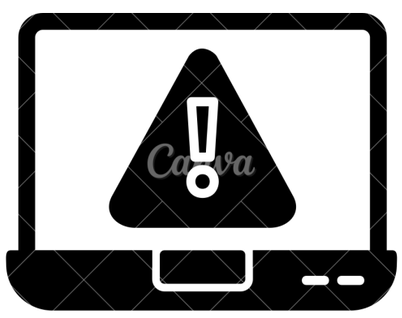


Keylogger

Keyloggers são um tipo de spyware que se oculta no dispositivo para registrar a digitação do usuário. Eles podem capturar credenciais de login, números de cartão de crédito e muito mais.

Adware

Adware é um software maligno que envia spam com anúncios para gerar receita aos cibercriminosos. O adware prejudica sua segurança para veicular anúncios, o que pode facilitar a entrada de outros malwares.



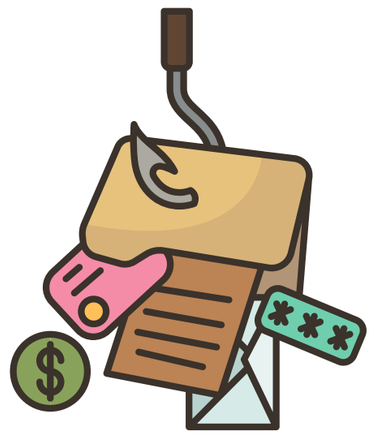
Ransomware

Ransomware trava o computador e os arquivos, ameaçando apagar tudo caso não receba um resgate. É uma das ameaças de malware mais urgentes atualmente.

SEGURANÇA DA INFORMAÇÃO

Phishing

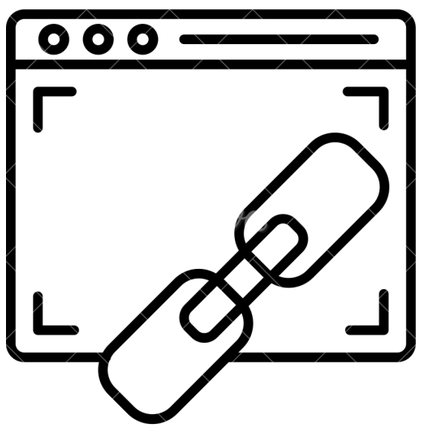
Não se trata de um malware, mas sim uma técnica criminosa. Phishing (pronunciado: fishing) é um ataque que tenta roubar seu dinheiro ou a sua identidade fazendo com que você revele informações pessoais, tais como números de cartão de crédito, informações bancárias ou senhas em sites que fingem ser legítimos.



Além disso, se liga nessas principais dicas de segurança e fique atento!

Não divulgue informações pessoais

Muita atenção no armazenamento e divulgação de dados sensíveis. Não salve informações pessoais em computadores e aparelhos não seguros ou públicos, e cuidado ao repassar esses dados em ligações telefônicas, mensagens ou e-mails a terceiros. Sempre confirme estar falando com contatos oficiais. Na dúvida, não divulgue informações.



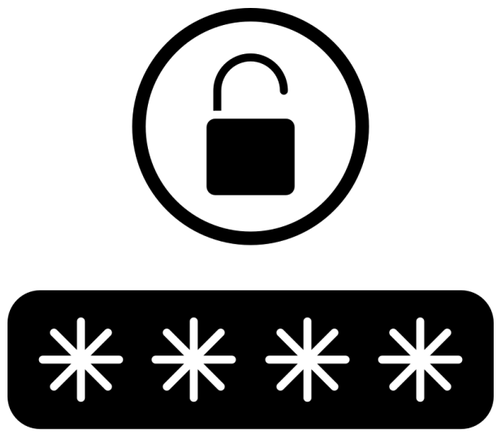
Não clique em links suspeitos

Cuidado ao clicar em links desconhecidos, pois podem levar a sites falsos ou infectar seu dispositivo com apenas um clique, liberando aos criminosos acesso a todas as informações armazenadas na máquina.
Links falsos são facilmente criados e podem ser enviados de diversas plataformas e aplicativos. Portanto, se você não conhece ou desconfia de um link, não clique.

SEGURANÇA DA INFORMAÇÃO

Crie senhas fortes

As senhas são uma excelente forma de proteger suas informações, mas para isso é preciso criar senhas fortes. Nada de usar datas de aniversário, nomes e outras informações que podem ser facilmente descobertas pelos cibercriminosos.
Crie senhas aleatórias, utilizando letras, números e caracteres especiais, e não esqueça de trocar sua senha a cada 90 dias.

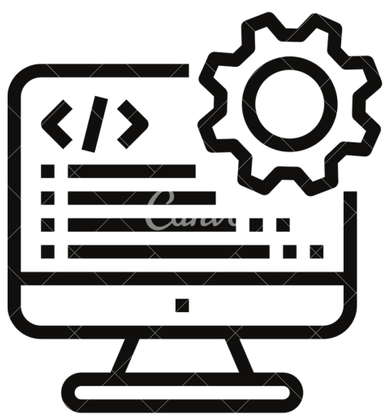


Atenção com emails e mensagens não solicitadas.

Antes de responder uma solicitação, clicar no link ou realizar um pagamento, verifique se você solicitou o serviço ou o contato em questão e se conhece o remetente da mensagem.
Por exemplo, você tem algum vínculo com o banco que está constantemente mandando e-mails para você? Esse é um tipo muito comum de tentativa de ataque cibernético, por isso, atenção sempre.

Cuidado com os downloads

Baixar arquivos da internet é algo comum no nosso cotidiano, no entanto, é preciso cuidado com as fontes desses arquivos e os sites onde estão localizados.
O download de um arquivo mal-intencionado pode dar acesso aos criminosos, apagar informações e causar muitos prejuízos.
Para evitar tudo isso, verifique a procedência dos arquivos antes de fazer download e respeite os avisos do seu antivírus sobre possíveis ameaças.



Mantenha sistemas e aplicativos atualizados

Sistemas operacionais não são tão vulneráveis. Os criminosos se aproveitam e exploram pequenas vulnerabilidades encontradas.
No entanto, as empresas costumam resolver essas vulnerabilidades muito rapidamente e justamente por isso é tão importante você manter seus sistemas sempre atualizados, de preferência de forma automática.
A falta de atualização pode abrir brechas e facilitar os ataques criminosos.

SEGURANÇA DA INFORMAÇÃO

Não abra anexos desconhecidos

Aqui vale a mesma regra dos links e downloads, você conhece a fonte ou quem está enviando os anexos para o seu e-mail? Se a resposta for não, é melhor não abrir o anexo e verificar a procedência antes de tomar qualquer ação.
Atenção também com algumas extensões que podem indicar arquivos maliciosos como .exe, .bat, .rar e .zip.

Faça backup dos seus arquivos.

A intenção de todas essas dicas é que você não caia em nenhum golpe ou tentativa de golpe, mas novos tipos de ataque surgem diariamente, por isso, é importante que você se proteja de todas as maneiras possíveis.
Mantenha um backup atualizado dos seus arquivos e informações em local seguro e diferente dos seus dispositivos principais. Se você não tem conhecimento técnico para isso, vale pensar em contratar um especialista para ajudar.

Na dúvida, consulte um profissional de TI

E se você recebeu um e-mail, mensagem, clicou em um link ou baixou um arquivo que desconfia ser prejudicial, fale com um profissional de tecnologia ou especialista em cibersegurança.
Se o acesso foi feito em um computador corporativo, o possível ataque pode, dependendo do caso, chegar até o servidor da empresa e causar ainda mais prejuízos, por isso, é mais seguro comunicar a área responsável para que as medidas corretas sejam tomadas.
Seguindo essas dicas, você se previne contra alguns tipos de ataque cibernético. O importante é estar sempre atento e evitar se colocar em situações de risco que podem ser evitadas.