DICAS DE SEGURANÇA DE PHISHING

É importante proteger a si mesmo e outras pessoas contra todos os ataques de phishing e não causar danos a outras pessoas acidentalmente. Aqui estão algumas das melhores práticas que irão ajudar você a alcançá-las:

O QUE VOCÊ PRECISA FAZER

- Só abra anexos se forem de uma fonte conhecida e se você estiver esperando.
  - Se você estiver esperando, contate a parte interessada e verifique a correspondência antes de abrir.
- Se um e-mail aparenta oferecer algum risco, não abra nenhum link ou anexo relacionado a ele.
- Antes de clicar em qualquer link, passe o mouse sobre o link e leia a URL completa para verificar se o link é autêntico.
- Digite os links diretamente no navegador em vez de clicar neles.
- Confira o remetente dos e-mails suspeitos, mesmo se o e-mail for de uma pessoa conhecida.
  - O domínio desses e-mails não seria confiável.

O QUE VOCÊ DEVE EVITAR

- Evite abrir e-mails com anexos desconhecidos, links clicáveis, e-mails de recompensa, e-mails pavorosos e e-mails ameaçadores.
  - A recompensa mais atraente = é a maior possibilidade de um ataque.
  - Ignore tais e-mails, a menos que você esteja esperando uma recompensa.
- Evite visitar sites de aparência suspeita.
- Não use, distribua, crie vírus, warms ou outros softwares maliciosos intencionalmente.
- Não interrompa ou altere as configurações da programação de varredura automática programada em seu desktop ou laptop.

- Cuidado com e-mails desconhecidos que indicam urgência ou ações imediatas.
  - Verifique esses e-mails com as equipes de segurança de TI.
- Fique atento no seguinte:
  - péssimo formato do e-mail
  - banner péssimo ou com pouca qualidade
  - Erros de ortografia e gramática
  - Saudações e mensagens genéricas

- Evite compartilhar informações pessoais ou confidenciais relacionadas à ABI em e-mails ou formulários da web.
- Evite abrir e-mails assinalados como spam.
  - A ABI tem ferramentas para filtrar e assinalar a comunicação como spam.

Lembre-se sempre de relatar imediatamente o seguinte:

- e-mails suspeitos
- Vírus de incidente de malware

Sempre denuncie qualquer atividade de roubo de identidade

abuse@ambevtech.com.br