

SEGGEST lança campanha “6 Dicas para Reconhecer E-mails de Phishing”

Objetivo é conscientizar magistrados, servidores e jurisdicionados sobre o tema

publicado: 30/09/2022 08h11 última modificação: 30/09/2022 08h13

Em um ataque de mail *phishing*, e-mail falsos são enviados em nome de uma empresa, serviço ou instituição, solicitando ao destinatário para clicar em um link no texto da mensagem. No entanto, o link não aponta para o que a mensagem oferece, mas sim para um site falso ou arquivo contaminado, visando capturar informações da vítima para utilização em fraudes.

Com o objetivo de conscientizar magistrados, servidores e jurisdicionados sobre a ameaça representada por e-mails de phishing, a Secretaria de Governança e Gestão Estratégica (SEGGEST) lançou esta semana a campanha intitulada “6 Dicas para Reconhecer E-mails de Phishing”. O conteúdo da campanha foi elaborado pela Assessoria de Governança de Segurança da Informação da SEGGEST, com o apoio da Assessoria de Comunicação Social na arte e divulgação, e da Coordenadoria de Material e Patrimônio na impressão do material utilizado na campanha.

Segundo o Secretário de Governança e Gestão Estratégica, Max Frederico, foi elaborado para a campanha um infográfico contendo dicas básicas sobre como identificar um e-mail de *phishing*, o qual será fixado nos murais existentes nos prédios da instituição, assim como divulgado em formato digital por e-mail e nos sites do TRT 13.

A campanha teve como principal motivação os resultados obtidos com a recente simulação de *phishing* realizada na instituição pela SEGGEST, onde 17% dos servidores e magistrados teriam suas senhas comprometidas se o ataque fosse real.

Rodrigo Mafra, Assessor de Governança de Segurança da Informação da SEGGEST, destaca que a maioria dos incidentes cibernéticos tem início com o comprometimento de credenciais de

acesso (login e senha) obtidas por meio de *phishing*, sendo a conscientização a principal ferramenta de proteção contra este tipo de ameaça.

6 Dicas para Reconhecer E-mails de Phishing

Quanto mais precavido seja, quanto mais informado esteja e quanto mais pense antes de dar um clique, estará bem mais prevenido contra o phishing.

- 1. CHEQUE O REMETENTE**
 - DESCONFIE DE E-MAILS COM REMETENTES DESCONHECIDOS OU ESTRANHOS.
 - NÃO ESQUEÇA DE QUE O REMETENTE DE E-MAILS ENVIADOS NO ÂMBITO DO TRT 13 SERÁ SEMPRE @TRT13.JUS.BR.
- 2. DESCONFIE DE TEXTOS MAL ELABORADOS**
 - GERALMENTE E-MAIL FALSOS POSSUEM UMA REDAÇÃO MAL ELABORADA, COM ERROS GRAMATICAIS, INFORMAÇÕES DESENCONTRADAS OU TEXTO DE TEOR INFORMAL.
 - E-MAILS ENVIADOS POR INSTITUIÇÕES POSSUEM UMA REDAÇÃO MAIS FORMAL.
- 3. VERIFIQUE OS LINKS**
 - LINKS EM E-MAILS FALSOS COSTUMAM APONTAR PARA SITES DESCONHECIDOS OU DIFERENTES DO CONTIDO NO TEXTO.
 - LEMBRE-SE QUE OS SITES INSTITUCIONAIS DO TRT 13 SERÃO SEMPRE TRT13.JUS.BR. POR EXEMPLO: PJE.TRT13.JUS.BR, WWW.TRT13.JUS.BR, ETC.
- 4. OBSERVE SE O E-MAIL SOLICITA DADOS SENSÍVEIS**
 - DESCONFIE DE E-MAILS QUE SOLICITEM DADOS SENSÍVEIS OU PESSOAIS, COMO CPF, RG, INFORMAÇÕES BANCÁRIAS OU CREDENCIAIS DE ACESSO (LOGIN E SENHA).
 - NENHUMA INSTITUIÇÃO SÉRIA COSTUMA SOLICITAR TAIS DADOS POR E-MAIL, MUITO MENOS O TRT 13!
- 5. DESCONFIE DE E-MAILS COM TEOR DE URGÊNCIA**
 - E-MAILS FALSOS COSTUMAM TER SENSO DE URGÊNCIA, COMO AMEAÇAS DE BLOQUEIO DE ACESSO, DE MULTAS OU DE CANCELAMENTO DE CADASTRO.
 - NA DÚVIDA, ENTRE EM CONTATO COM O CANAL OFICIAL DE ATENDIMENTO DA INSTITUIÇÃO REMETENTE. NO TRT 13, O CANAL OFICIAL DE CONTATO COM A SOCIEDADE É A OUVIDORIA. WWW.TRT13.JUS.BR/INSTITUCIONAL/OUVIDORIA
- 6. NÃO SE ENTUSIASME COM OS CLIQUES**
 - NÃO ESQUEÇA QUE, MESMO TENDO INSTALADO UM ANTIVÍRUS OU OUTROS PROGRAMAS DE SEGURANÇA NÃO É ACONSELHÁVEL CLICAR INDISCRIMINADAMENTE, PRESUMINDO QUE SEU SOFTWARE IRÁ DETECTAR TODOS OS CÓDIGOS E SITES MALICIOSOS.

TRT-13ª REGIÃO
Paralíba

Secretaria de Governança e Gestão Estratégica
Assessoria de Governança de Segurança da Informação

SEJA SEMPRE CAUTELOSO!

Assessoria de Comunicação Social TRT-13 com informações da Seggest

31 visualizações desde a data de publicação