PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO - 13ª REGIÃO

Cartilha de Segurança da Informação
Correio Eletrônico

Tribunal Regional do Trabalho – 13ª Região
Setor de Segurança da Informação
ssi@trt13.jus.br

Versão 2.0
Autor: Rodrigo Mafra
Maio/2017

Resumo

Este documento tem por objetivo divulgar, no ambiente interno do TRT 13, procedimentos e dicas que orientem os usuários na identificação e tratamento de ameaças à Segurança da Informação, presentes na utilização do correio eletrônico institucional (*e-mail*).

1. Tipos de ameaças via *e-mail*

O correio eletrônico é atualmente um dos principais meios de comunicação, suplantando a muito em utilização o correio tradicional, tornando-se uma ferramenta de trabalho indispensável. Porém, a utilização do *e-mail* é explorada por alguns como forma de disseminação de propagandas e fraudes eletrônicas. Basicamente, as ameaças relacionadas a utilização indevida do correio eletrônico são:

- **Spam:** Mensagem indesejada e não solicitada, geralmente enviada para um grande número de destinatário com objetivo de propaganda comercial ou pornográfica;
- **Hoax:** Tipo de *spam* disseminado com o objetivo de propagar um boato, corrente ou golpe, estimulando o usuário a repassar a mensagem para terceiros;
- **Phishing scam:** Ou simplesmente *scam*. Mensagem disseminada com o objetivo de induzir o usuário a acessar um *link* que aponta para um *site* falso ou para um código malicioso;
- **Vírus mail:** Mensagem cujo anexo está contaminado por um código malicioso, com o objetivo de disseminar uma contaminação.

De uma forma geral, a utilização indevida do correio eletrônico causa transtornos como:

- **Não recebimento de *e-mails*** devido ao "estouro" do limite da caixa postal do usuário, causado pelo recebimento de um grande número de mensagens não solicitadas;
- **Perda de produtividade** em decorrência do tempo extra necessário para a leitura de *e-mails* não solicitados;
- **Consumo desnecessário de recursos computacionais** em virtude do aumento do tráfego na rede, da utilização indevida do espaço de armazenamento nos servidores de correio, etc;
- **Contaminação das estações de trabalho** através da disseminação de códigos maliciosos;
- **Roubo de informações sigilosas**, como senhas, números de cartões de créditos, etc.

2. Identificando *e-mails* suspeitos

Sempre que receber um *e-mail*, realize a seqüência de passos a seguir:

- **Verifique o remetente:** Caso o remetente da mensagem seja desconhecido ou esteja em branco, considere o *e-mail* como suspeito. Mensagens não solicitadas geralmente utilizam remetentes falsos ou em branco. Exs.: mailer@hotmail.com, zblgwwhekbs@yahoo.com;
- **Verifique os destinatários:** Caso a mensagem possua vários destinatários desconhecidos, considere o *e-mail* como suspeito. Mensagens não solicitadas costumam ser enviadas para um grande número de pessoas;
- **Verifique o assunto:** Caso ache o assunto da mensagem estranho, considere o *e-mail* como suspeito;
- **Verifique os anexos:** Caso a mensagem possua anexos não solicitados, de procedência duvidosa ou extensão potencialmente perigosa (SCR, CPL, PIF, CMD, COM, EXE), considere o *e-mail* como suspeito. Mensagens contaminadas por vírus geralmente possuem anexos dessa natureza. Jamais clique, abra ou execute um anexo considerado suspeito. Exs.: robo.zip, sexy.zip, foto.scr, atualização.exe, cartão.exe;
- **Verifique o conteúdo:** Caso o conteúdo da mensagem esteja enquadrado em um dos itens abaixo, considere a mesma como suspeita:
    - **Teor pornográfico**, como propaganda de *sites* pornográficos, fotos, texto erótico, etc;

- **Teor comercial,** como propaganda de *sites*, oferta de produtos, venda de medicamentos, etc;
- **Informações financeiras.** Mensagens, geralmente em nome de bancos, financeiras ou operadoras de cartão de crédito, solicitando ao usuário o recadastramento de informações ou atualização de aplicativos. Instituições financeiras não enviam e-mails desta natureza;
- **Convites,** como solicitação para participação em *sites* de relacionamento ou redes sociais, aviso de recebimento de cartões festivos e mensagens *on-line*, etc;
- **Notificações,** como pendência de débitos, regularização e cancelamento de documentos (CPF, título de eleitor, entre outros). Órgãos públicos e instituições financeiras não enviam notificações desta natureza por *e-mail*;
- **Promoções,** como concursos, premiações, etc;
- **Oferta de downloads**, como atualizações de aplicativos, de antivírus, do Windows, etc;
- **Texto com muitos erros ortográficos,** pois geralmente as mensagens falsas possuem tal característica;
- **Texto em outro idioma**, pois a maior parte das mensagens recebidas escritas em idioma diferente do português é *spam*;

3. Tratando *e-mails* suspeitos

Uma vez identificado um *e-mail* como suspeito, proceda da seguinte forma:

- **Não clique, abra ou execute anexos** existentes na mensagem, pois os mesmos podem conter vírus;
- **Não clique, abra ou acesse *links* (*sites*)** existentes na mensagem, pois os mesmos podem instalar códigos maliciosos em sua estação;
- **Encaminhe o *e-mail* suspeito para o SSI** - Setor de Segurança da Informação - (ssi@trt13.jus.br). A mensagem encaminhada será então analisada, e caso seja confirmada como uma ameaça, o recebimento da mesma será bloqueado;
- **Apague o *e-mail* suspeito de sua caixa postal,** evitando assim que a segurança de sua estação e da rede seja comprometida.

4. Segurança do *e-mail* corporativo

O correio eletrônico institucional do TRT 13 possui defesas contra as ameaças citadas neste documento. Porém, novas ameaças surgem diariamente, sendo impossível garantir 100% de eficiência para todos os casos existentes. A Secretaria de Tecnologia da Informação e Comunicação está constantemente aprimorando os recursos de TI, buscando sempre uma maior segurança na utilização dos serviços disponibilizados.

Sendo assim, é fundamental a colaboração dos usuários, no sentido de proceder conforme as orientações contidas nesta **Cartilha**.

O TRT 13 possui as seguintes proteções contra as ameaças descritas:

- **Filtros anti-spam:** Todo *e-mail* recebido e enviado é verificado automaticamente por *softwares* especializados, os quais efetuam a detecção e bloqueio de mensagens identificadas como ameaças;

- **Filtros antivírus:** Todo *e-mail* recebido e enviado é verificado automaticamente por *softwares* especializados, os quais efetuam a detecção e bloqueio de mensagens cujos anexos estejam contaminados por códigos maliciosos;
- **Clientes antivírus**: Os servidores e estações da rede possuem instalado *software* antivírus, o qual efetua a detecção e remoção de códigos maliciosos.

5. Maiores informações

- *Cartilha de Segurança para a Internet - Spam*
  https://cartilha.cert.br/spam/

- *Scam - A fraude inunda o correio eletrônico*
  http://www.mhavila.com.br/topicos/seguranca/scam.html