SALVADOR
PREFEITURA

COGEL
Companhia de Governança
Eletrônica de Salvador

GESIC
Gerência de Segurança da
Informação e Comunicação

Cartilha de uso do E-mail Corporativo @SALVADOR

OBJETIVOS

Conscientizar todos os colaboradores, sobre a importância do uso do e-mail **@SALVADOR** da prefeitura, pois a ferramenta de e-mail adotada o **MS Office 365**, é um ambiente seguro e monitorado, livre de ameaças cibernéticas. Outro motivo para sua utilização é a documentação da comunicação, da prefeitura junto a sociedade.

FINALIDADE

Criar uma cultura orgânica de utilização do e-mail corporativo **@SALVADOR**, dentro da instituição, como forma segura de comunicação documental.

Documentos e afins devem ser recepcionados e transmitidos por este canal, a fim de dar para sociedade, confiabilidade e segurança na comunicação da instituição.

SEGURANÇA

Nosso ambiente de e-mail **@SALVADOR** é provido de políticas de segurança, que garantem a segurança na transmissão das mensagens, protegendo contra a evolução das ameaças cibernéticas.

Além dos recursos de segurança da plataforma do Office 365, nosso ambiente conta com o TM CAS, uma camada a mais de segurança para garantir que ameaças, fraudes e golpes sejam evitados.

Por este motivo, é imprescindível a utilização do e-mail **@SALVADOR**, para transmissão de mensagens, garantindo a segurança na comunicação da prefeitura, com a sociedade.

NÃO USE E-MAIL PESSOAL PARA ASSUNTOS RELACIONADOS À PREFEITURA.

CONFIABILIDADE

A plataforma de e-mail adotada, Office 365 da Microsoft, vem destacando-se no cenário mundial pela sua facilidade e segurança, lembrando que nossa estrutura, conta também redundância de segurança, garantindo a confiabilidade na comunicação da prefeitura com a sociedade. A seguir descreveremos os ataques mais conhecidos, lembrando que nosso ambiente tem uma proteção de quase 100% para os ataques cibernéticos, uma vez que nossas ferramentas usam inteligência artificial, no processo e monitoramento de segurança.

TIPOS DE ATAQUES A E-MAILS

Phishing: geralmente descreve as técnicas de engenharia social que os criminosos usam para roubar informações corporativas ou de usuários por e-mail. Os ataques de phishing são mais eficazes quando os usuários não sabem que isso está acontecendo.

Fraude: esse tipo de ataque pode assumir várias formas, desde os clássicos golpes de taxa antecipada direcionados a pessoas comuns até mensagens de comprometimento de e-mail corporativo (BEC) que que visam induzir os departamentos de contabilidade de grandes empresas a transferir dinheiro para contas ilegítimas. Muitas vezes, o invasor usará falsificação de domínio para fazer com que a solicitação de fundos pareça ter vindo de uma fonte legítima.

Malware: os tipos de malware distribuídos por e-mail incluem spyware, scareware, adware e ransomware, entre outros. Há diversas formas de um invasor distribuir malware por e-mail. Uma das mais comuns é incluir um anexo com código malicioso.

Invasão de contas: os invasores invadem as caixas de entrada de usuários legítimos por uma variedade de motivos, como monitorar suas mensagens, roubar informações ou usar endereços de e-mail legítimos para

encaminhar ataques de malware e spam para seus contatos.

Interceptação de e-mail: os invasores podem interceptar e-mails para roubar informações contidas neles ou realizar ataques de invasores intermediários, em que eles se passam por ambos os lados de uma conversa. A forma mais comum de realizar esse ataque é monitorar os pacotes de dados em redes locais (LANs) sem fio, já que interceptar um e-mail em trânsito pela internet é extremamente difícil.

A segurança não é um produto pronto, é um processo diário que fazemos para manter nossas informações seguras, livres de ataques e ameaças, por tanto é imprescindível que facçamos nossa parte, mantendo nossas senhas em segurança, não informando seu email em sites suspeitos, atentando-se sempre para as observções de segurança, disponibilizadas por nossos analistas.

SEJA SEGURO

Fonte: Google busca e imagens