SALVADOR
PREFEITURA

COGEL
Companhia de Governança Eletrônica de Salvador

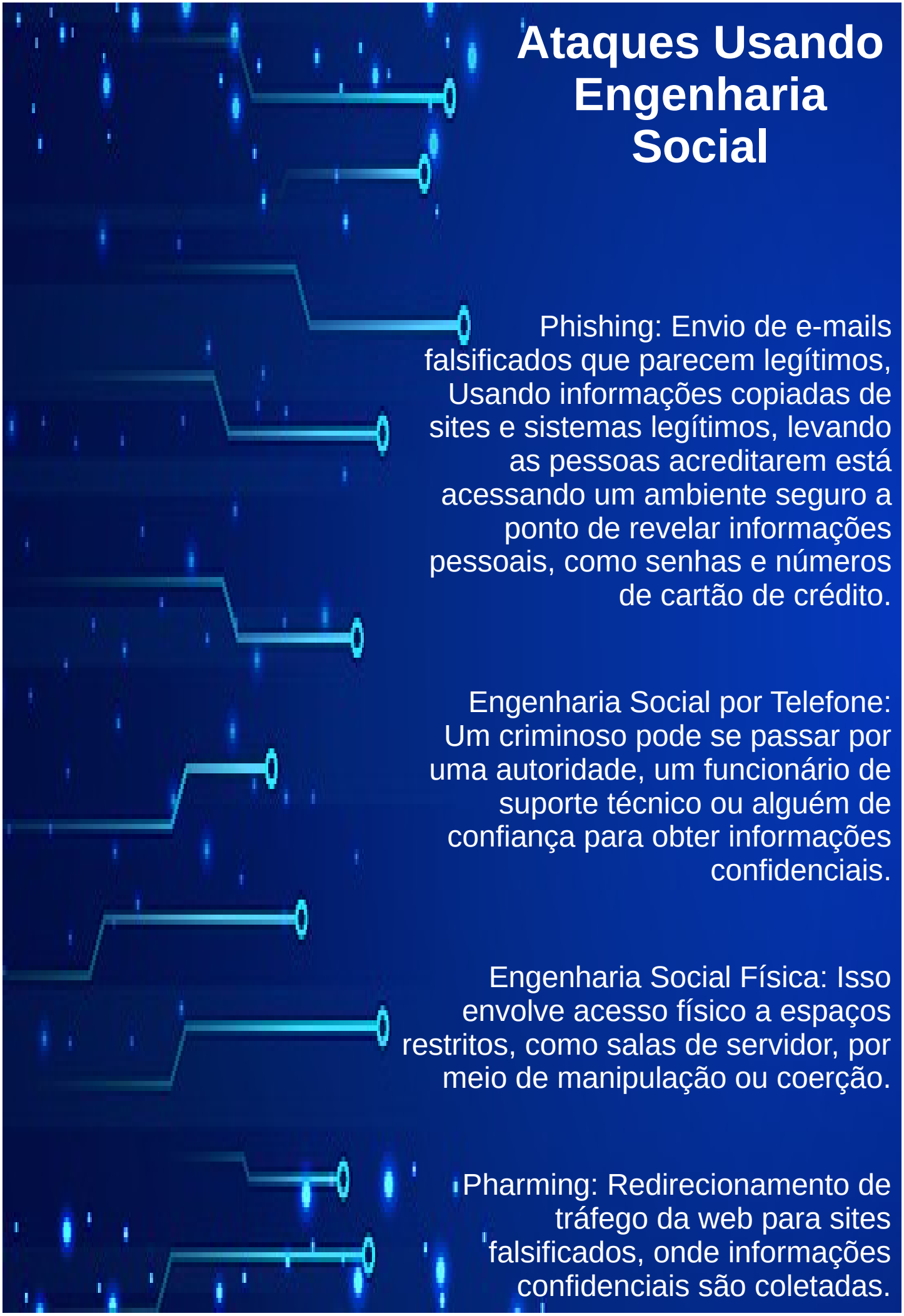
GESIC
Gerência de segurança da Informação e comunicação

Cartilha sobre Engenharia Social e Crime Cibernéticos

Engenharia Social e Crimes Cibernéticos...

Engenharia Social, a arte de enganar para roubar…

A Engenharia social, refere-se à manipulação psicológica de pessoas para obter informações confidenciais, acesso a sistemas ou realizar determinadas ações de comprometimento da segurança, para a realização de um ataque cibernético. O atacante busca informações, na própria internet, como por exemplo redes sociais para estabelecer contato com swua vítima, para facilmente enganá-la e executar seu ataque. Outra fonte importante de informações é o seu lixo, pois ele diz muito sobre quem você é. A manipulação do lixo é muito importante, pois muito do que é descartado, é informação valiosa para o atacante. A seguir algumas técnicas usadas para manipulação de usuários com o intuito de realização de ataque cibernético.



Ataques Usando Engenharia Social

Phishing: Envio de e-mails falsificados que parecem legítimos, Usando informações copiadas de sites e sistemas legítimos, levando as pessoas acreditarem está acessando um ambiente seguro a ponto de revelar informações pessoais, como senhas e números de cartão de crédito.

Engenharia Social por Telefone: Um criminoso pode se passar por uma autoridade, um funcionário de suporte técnico ou alguém de confiança para obter informações confidenciais.

Engenharia Social Física: Isso envolve acesso físico a espaços restritos, como salas de servidor, por meio de manipulação ou coerção.

Pharming: Redirecionamento de tráfego da web para sites falsificados, onde informações confidenciais são coletadas.

Cuidado!!!

A falta de conscientização ds usuários e colaboradores, torna o emprego da Engenharia Social eficaz, pois a vitima está criando brechas na realização de ataques cibernéticos. Entenda, ter equipamentos de segurança e sistemas avançados não coibem os atacantes cibernéticos, pois os mesmos estão estudando todos os pontos vulnaráveis para realização de seus ataques.

Crimes cibernéticos como:

Hacking: Acesso não autorizado a sistemas de computador ou redes.

Malware: Programas maliciosos projetados para danificar, controlar ou obter acesso não autorizado a sistemas de computador.

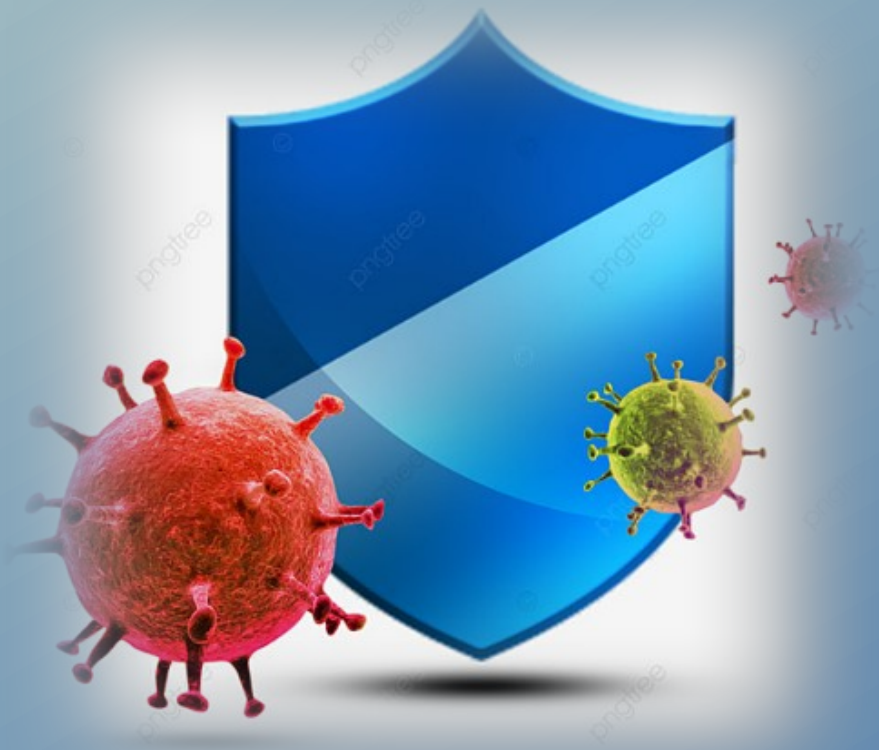
Roubo de Identidade: Obtendo informações pessoais para se passar por outra pessoa, geralmente para fins fraudulentos.

Fraude Online: Enganar pessoas para obter dinheiro, informações pessoais ou outros benefícios através da internet.

Sempre surtirão efeito, sem a devida CONSCIENTIZAÇÃO SOBRE SEGURANÇA. O conhecimento nos torna mais seguros.

Fique atento!!!

A prevenção contra esses crimes cibernéticos e a engenharia social envolve educação, conscientização e medidas de segurança rigorosas, como o uso de autenticação em dois fatores, manutenção de softwares atualizados, desconfiança de solicitações de informações pessoais por canais não seguros e uso de senhas fortes e únicas para cada conta. Organizações também devem implementar políticas de segurança robustas e treinar funcionários para reconhecer e lidar com tentativas de engenharia social.



Seja SEGURO

GESIC

Gerência de segurança da Informação e comunicação