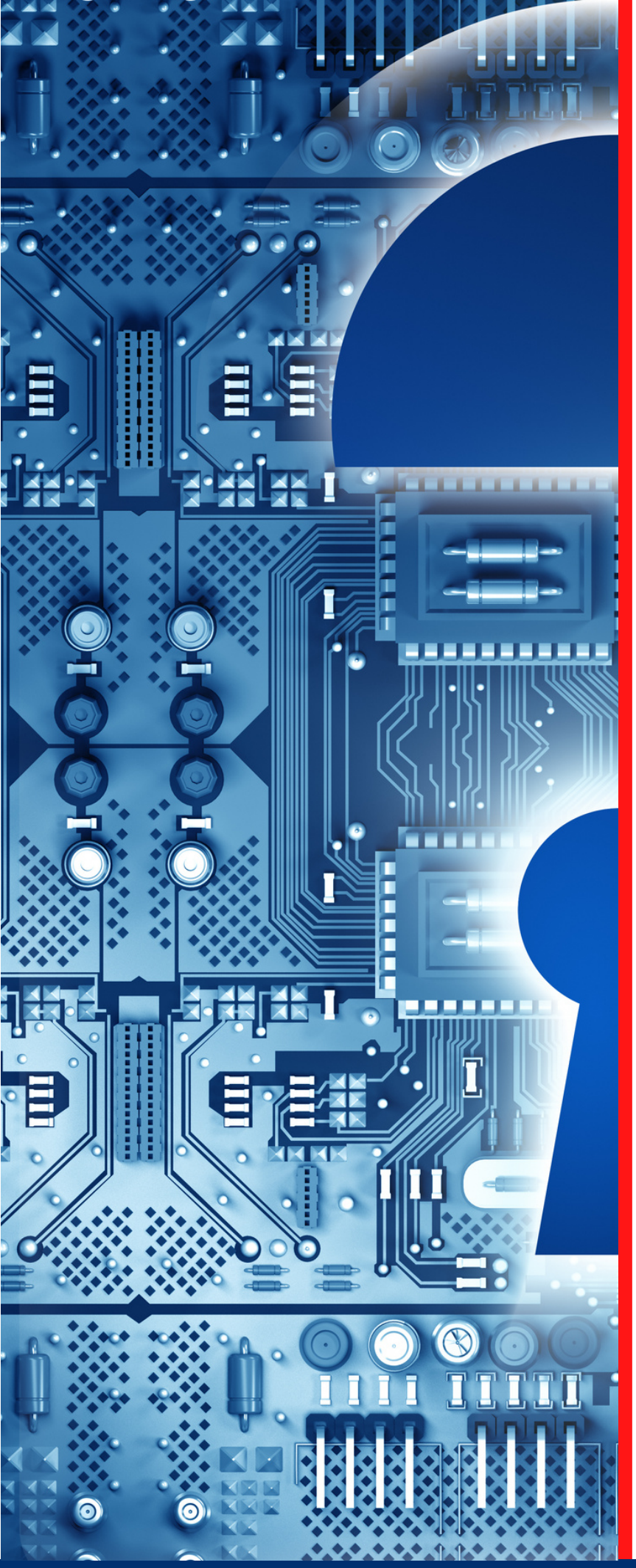


OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

01/2023

Engenharia social como vetor de incidentes cibernéticos às infraestruturas de Governo.

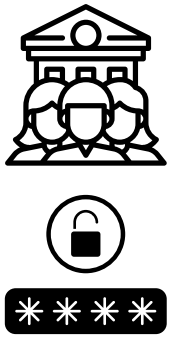
Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.

TLP:CLEAR

O que é Engenharia Social?

A engenharia social é uma técnica de manipulação que explora o erro humano para aplicar golpes, ludibriar ou obter de forma indevida dados pessoais ou sensíveis. Estas ações envolvem expor dados, execução de malware ou acesso indevido a infraestruturas.

A engenharia social é baseada na interação humana e é conduzida por ameaças que usam o engano, para violar os procedimentos de segurança que normalmente deveriam ser seguidos.



Essa forma de ataque pode ser utilizada para obtenção de credenciais de acesso às redes governamentais para obter, por exemplo, nomes de usuários, *e-mails* e senhas correspondentes. Essa é uma forma de violação de dados que é agravada quando a vítima utiliza a mesma combinação de usuário e senha em diferentes plataformas, sítios eletrônicos (*sites*) ou serviços.

Phishing

A técnica de engenharia social mais utilizada é o *phishing*, em que o atacante envia mensagens fraudulentas para induzir a vítima a executar um *malware* ou clicar em um *link* para um *site* falso ou malicioso.

O *phishing* apresenta variações que merecem atenção. Entre elas, destacam-se:

- ***smishing*** é uma combinação do termo "SMS" (*short message services*, ou mensagens de texto) com o termo *phishing*; e

- ***vishing*** é uma forma de ataque de *phishing* que ocorre por voz, por meio de ligações telefônicas.

As mensagens utilizadas costumam expressar urgência, oportunidade ou autoridade para facilitar o convencimento à vítima.

Recomendações

O Departamento de Segurança da Informação (DSI) recomenda a realização de campanhas de conscientização para que o usuário de redes governamentais:

- não abra mensagem de origem desconhecida, remetente suspeito ou com texto incomum;
- não acesse *links* suspeitos ou de origem desconhecida;
- não se ausente da estação de trabalho sem bloquear a tela do dispositivo;
- ative, sempre que disponível, o Múltiplo Fator de Autenticação[1] (MFA) em seus sistemas;
- evite utilizar redes sem fio, *wi-fi*, não confiáveis (bares, restaurantes, aeroportos, etc);
- não preencha suas informações em formulários de *sites* desconhecidos ou inseguros;
- verifique se o endereço do site da página apresenta “HTTPS” e não apenas “HTTP.” O \"S\" significa \"seguro\". Os sites HTTP, mesmo que sejam legítimos, são geralmente mais vulneráveis;
- não informe seus dados por telefone, principalmente senhas;
- não envie fotos de documentos ou os publique em redes sociais;
- controle e mantenha atualizados os aplicativos e os sistemas em seu dispositivo;
- não autorize, se possível acessos remotos ao seu dispositivo;
- não repasse códigos recebidos para supostos atendentes;
- desconfie de ofertas, promessas ou ameaças que exigem o fornecimento de dados; e
- **informe a Equipe de Prevenção, Tratamento e Resposta a Incidentes (ETIR) de seu órgão sempre que receber mensagens falsas ou suspeitas.**

Para os responsáveis pela infraestrutura de rede, recomendamos atenção na correta configuração do servidor *proxy*[2], particularmente com o objetivo de garantir a segurança dos dados. Os servidores *proxy* atuam como um *firewall*[3] e filtro da *web*. Um servidor *proxy* adequadamente configurado mantém os usuários e a rede interna protegidos. Além disso, permite bons níveis de privacidade.

Outra medida eficaz é aplicar o princípio do menor privilégio[4] na definição dos perfis das contas de usuários, limitando os privilégios de administrador àqueles que realmente necessitam. Além disso, é importante que as contas com esse perfil não sejam utilizadas para verificar *e-mails* ou navegar na *Web*. Com essas ações, evita-se que usuários instalem acidentalmente *malwares*[5].

Por fim, recomenda-se ainda a leitura das orientações contidas nos *sites* abaixo:

https://www.gov.br/gsi/pt-br/assuntos/dsi/boletim-informativo-mensal-1

https://www.cisa.gov/phishing-infographic

https://www.ncsc.gov.uk/guidance/phishing

Outros conceitos podem ser verificados no glossário do DSI do Gabinete de Segurança Institucional da Presidência da República, disponível em:

https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1

TLP:CLEAR

Informações complementares

1. **Múltiplo Fator de Autenticação (MFA):** é um componente de gestão de acesso que requer que os utilizadores provem a sua identidade utilizando pelo menos dois fatores de verificação diferentes antes de terem acesso a um website, aplicação móvel ou outro recurso online, Em contraste, a autenticação por fator único (ou simplesmente "autenticação") usa uma única tecnologia para provar a autenticidade do usuário.
2. **Servidor *proxy*:** um servidor *proxy* é um aplicativo de servidor que atua como intermediário entre um cliente que solicita um recurso e o servidor que fornece esse recurso.
3. ***Firewall:*** é um dispositivo de uma rede de computadores, na forma de um programa ou de equipamento físico, que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP.
4. **Princípio do menor privilégio:** O princípio do menor privilégio é uma estratégia de segurança, aplicável a diferentes áreas, que se baseia na ideia de conceder autorizações apenas quando realmente sejam necessárias para o desempenho de uma atividade específica.
5. ***Malware:*** *malware* é qualquer *software* intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores.