Treinamento de conscientização de Engenharia Social

Bem vindo ao treinamento de conscientização de Engenharia Social, caro colaborador.

Neste material, abordaremos conceitos e práticas de engenharia social, termo que se refere a um tipo de ataque cibernético que explora a psicologia humana para obter acesso a informações confidenciais ou sistemas protegidos.

Antes de tudo, precisamos entender como o ser humano está sujeito a cair nesse tipo de armadilha. Uma das formas que os hackers, sejam honestos ou não, conseguem invadir sistemas de informação, é valendo-se de fragilidades inerentes à mente de qualquer pessoa, principalmente daquelas que não estão familiarizadas com o nível de sofisticação das técnicas alcançado atualmente.

O medo, a curiosidade, a pressa, a falta de atenção, a confiança em impostores, a ganância, são algumas dessas fragilidades que tornam as pessoas alvos fáceis desse tipo de ataque.

Alguns exemplos que servem de alerta são:

E-mails ou mensagens que alertam sobre atividades suspeitas em contas bancárias, ameaças de bloqueio de serviços ou avisos de vírus podem gerar pânico, levando as pessoas a clicar em links sem pensar.

Conteúdo sensacionalista, promessas de prêmios ou ofertas irresistíveis despertam a curiosidade e podem levar as pessoas a clicar em links para satisfazer seu interesse.

Mensagens que exigem ação imediata, como "sua conta será bloqueada em 2 horas" ou "última chance de aproveitar esta oferta", pressionam as vítimas a agir impulsivamente.

Perfis falsos, mensagens diretas ou postagens enganosas em redes sociais podem levar as vítimas a clicar em links maliciosos.

Falsos técnicos de suporte entram em contato com as vítimas, alegando problemas em seus dispositivos e solicitando acesso remoto ou informações confidenciais.

Oferecimento de serviços ou benefícios em troca de informações confidenciais ou acesso a sistemas.

Na terminologia da cibersegurança, existem vários tipos de ataques cibernéticos. Conheça alguns deles:

Phishing: Envio de e-mails, mensagens ou ligações fraudulentas que se passam por entidades confiáveis (bancos, empresas, etc.) para induzir a vítima a revelar dados pessoais, senhas ou informações financeiras. [

Spear Phishing: Um tipo de phishing mais direcionado, onde o atacante personaliza a mensagem para uma vítima específica, aumentando a credibilidade e a probabilidade de sucesso.

Baiting (Isca): Oferecimento de algo atraente (como um pen drive infectado ou um download gratuito) para atrair a vítima e infectar seu dispositivo com malware.

Pretexting (Pretexto): Criação de um cenário fictício para ganhar a confiança da vítima e obter informações confidenciais.

Quid Pro Quo: Oferecimento de um serviço ou benefício em troca de informações confidenciais.

Tailgating (Carona): Obtenção de acesso físico a áreas restritas seguindo pessoas autorizadas.

Neste treinamento vamos nos focar na técnica conhecida como Phishing, cujo nome deriva da palavra fishing (pesca) com o termo hacker phreaking, em referência aos primórdios do hacking feito pela rede telefônica.

O phishing busca obter o acesso às credenciais das vítimas através do envio de e-mails, mensagens ou ligações fraudulentas que se passam por entidades confiáveis (bancos, empresas, etc.) para induzir a vítima a revelar dados pessoais, senhas ou informações financeiras.

O fato de tantas pessoas serem vítimas desse tipo de ataque, faz com que seja preciso promover campanhas de conscientização abrangentes, indo desde o familiar do colaborador, até os executivos mais importantes da organização.

Em se tratando de phishing por meio de mensagem eletrônica, os usuários devem ficar atentos às seguintes recomendações:

Não abra a mensagem se desconfiar do nome do remetente.

Verifique se o endereço do remetente é legítimo. Verifique se depois do nome do remetente, após o @, o domínio é confiável.

O uso de ferramentas de verificação é mais uma camada de proteção para a organização.

Desconecte o dispositivo da internet após clicar em um link suspeito.

Tenha cuidado com mensagens de e-mail com linguagem urgente ou ameaçadora,
com erros de ortografia ou gramática, com logomarcas desatualizadas ou distorcidas,
com nomes falsos ou endereços de e-mail suspeitos, ou que se passam por comunicações oficiais de instituições conhecidas.

Mantenha o software antivírus atualizado, seja pessoal ou corporativo.

Use autenticação de 2 fatores – ajuda a impedir a ação do agente malicioso.

Use senhas fortes e únicas – Normalmente a organização estabelece um padrão de senha a ser utilizado. Em certos casos, um cofre de senha deve ser implementado.

Não forneça informações pessoais por e-mail, pois pode ser utilizado por um impostor para aplicar golpes em seu nome.

Desconecte o dispositivo da internet após clicar em um link suspeito.

Quais medidas deve-se tomar se acidentalmente você constatou ser vítima de phishing?

- Avise imediatamente o setor de segurança da informação. Relate a ocorrência com urgência, para minimizar o tempo de ação do agente suspeito.
- Se possível, altere a senha imediatamente.
- Colete as evidências de atividade suspeita e comunique ao setor de segurança da informação. Não forneça acesso aos seus dados a ninguém.
- Monitore os recursos(consumo de cpu, uso de memória, alteração de arquivos), em horários fora do usual, como por exemplo na hora de almoço.
- Monitore se suas contas de trabalho foram comprometidas. Verifique os arquivos que você utiliza foram realmente alterados por você.
- Acesse a cartilha de política de segurança da informação da empresa para ver se as medidas que está tomando estão compatíveis, sob o risco de sanções disciplinares.

Adotando as práticas mencionadas, você ajuda a fortalecer a segurança, estabilidade e prosperidade da empresa e da sua família.