1.Phishing

***Phishing* é um método utilizado em engenharia social envolvendo o envio de mensagens fraudulentas ou a criação de sites falsos**. Visa enganar as pessoas e fazê-las divulgar informações confidenciais, como senhas, informações de cartão de crédito, números de seguro social e outros dados pessoais. O phishing pode variar em complexidade, desde ataques simples que visam um grande número de pessoas até ataques altamente direcionados. Para evitar cair em golpes de phishing, é importante que as pessoas estejam cientes das características de mensagens e sites falsos. Elas devem verificar a autenticidade das fontes, não clicar em links suspeitos ou baixar anexos desconhecidos e estar atentas a sinais de alerta, como erros de gramática ou ortografia em mensagens.

1.1 Mensagem falsa

O atacante envia mensagens de e-mail, mensagens de texto ou até mesmo mensagens em redes sociais que parecem ser de fontes legítimas. Essas mensagens geralmente alertam a vítima sobre uma suposta situação urgente, como uma conta bloqueada, uma compra não autorizada, ou a necessidade de atualizar informações de login.

1.2 Isca e página falsa

A mensagem contém um link ou um botão que leva a uma página falsa que imita um site legítimo, como um banco, uma rede social, ou um serviço de e-mail. Essa página solicita que a vítima insira informações confidenciais, como nome de usuário e senha.

1.3 Roubo de informações

Quando a vítima insere suas informações na página falsa, o atacante obtém acesso às credenciais da vítima. Essas informações podem ser usadas para cometer fraudes, acessar contas pessoais ou realizar atividades maliciosas em nome da vítima.

2.Spear phishing

O ***spear phishing*** é uma forma mais direcionada de phishing. **Nesse caso, os atacantes escolhem alvos específicos, como funcionários de uma empresa, executivos ou indivíduos com acesso a informações sensíveis**. Os atacantes coletam informações detalhadas sobre as vítimas, como seus nomes, cargos, interesses, colegas de trabalho e outras informações pessoais. Com base nesses detalhes, eles personalizam mensagens de phishing para parecerem legítimas e confiáveis. Isso aumenta a probabilidade de que as vítimas acreditem nas mensagens e sigam as instruções para divulgar informações confidenciais ou executar ações específicas.

3.Vishing

***Vishing* é o phishing que usa tecnologia de comunicação de voz**. Os criminosos podem falsificar as chamadas de origens legítimas usando a tecnologia VoIP. As vítimas também podem receber uma mensagem gravada que pareça legítima, podendo obter números de cartão de crédito ou outras informações para roubar a identidade da vítima.

4.Pharming

É a representação de um site legítimo na tentativa de enganar os usuários para inserir as credenciais. O pharming leva os usuários para um site falso que parece ser oficial, então as vítimas digitam as informações pessoais achando que estão conectadas a um site legítimo.

5.Smishing

***Short Message Service Phishing* é o que usa mensagens de texto em celulares**. Os criminosos se passam por uma fonte legítima na tentativa de ganhar a confiança da vítima. Quando a vítima visita o site, o malware é instalado no telefone celular.

6.Whaling

É um ataque de phishing que busca vítimas de alto perfil em uma empresa, como executivos ou seniores. Outras vítimas incluem políticos ou celebridades. As violações de segurança podem afetar os navegadores da Web, exibindo anúncios de pop-up, coletando informações pessoais identificáveis ou instalando adware, vírus ou spyware. Um criminoso pode invadir um arquivo executável, os componentes ou plugins do navegador. Os atacantes podem se passar por colegas de trabalho, parceiros de negócios ou autoridades para ganhar a confiança do alvo

7.Spam

Refere-se ao envio em massa de mensagens não solicitadas, geralmente por e-mail, para um grande número de destinatários. Essas mensagens podem conter anúncios, links maliciosos, conteúdo enganoso ou até mesmo tentativas de phishing. Os spammers enviam grandes volumes de e-mails para endereços de e-mail obtidos de diversas fontes, como listas de e-mails compradas, roubadas ou coletadas na web. O objetivo do spam pode variar, desde promover produtos ou serviços ilegítimos até tentar induzir os destinatários a clicarem em links maliciosos para distribuir malware ou phishing.